Perfiles de las Ciencias Sociales, Nueva Época,
Vol. 13, Núm. 26, Julio – Diciembre 2026, ISSN: 2007-9362
DOI: 10.19136/pcs.a13n26.6697
Sección: Interdisciplinariedad en las Ciencias Sociales.

# NUEVAS DIMENSIONES DEL DERECHO A LA PRIVACIDAD Y DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES ANTE LAS TECNOLOGÍAS EMERGENTES: INTERNET, BIOMETRÍA Y DRONES*

# NEW DIMENSIONS OF THE RIGHT TO PRIVACY AND THE RIGHT TO THE PROTECTION OF PERSONAL DATA IN THE FACE OF EMERGING TECHNOLOGIES: INTERNET, BIOMETRICS AND DRONES

Eduardo Kanahuati Fares[1]
Oscar Rafael Hernández Meneses[2]

**Resumen:** El artículo analiza la reconfiguración del derecho a la privacidad y la protección de datos personales ante internet, biometría y drones.[3] Sostiene que la protección de datos personales, apuntalada en el consentimiento, los avisos de privacidad y el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición), resulta insuficiente frente a tecnologías que rastrean, identifican y observan a las personas en contextos ordinarios. La elección de los tres casos responde a una estrategia analítica:

* Artículo de investigación en extenso. Artículo recibido: 19 de mayo de 2026. Artículo aprobado: 10 de junio de 2026.
[1] Licenciado en derecho por la Universidad Anáhuac y doctor en Derecho por el Instituto de Investigaciones Jurídicas de la UNAM. Profesor de Derecho Internacional Público en la Universidad Anáhuac México. Correo: ekanahuatif@gmail.com https://orcid.org/0009-0008-2838-6538.
[2] Licenciado en derecho por la Universidad Juárez Autónoma de Tabasco, Maestro y Doctorando en Derecho en la Facultad de Derecho de la UNAM. Tutor en el Programa de Posgrado en Derecho de la UNAM. Ha sido consultor externo para el Programa de las Naciones Unidas para el Desarrollo. Correo: Cienciajuridicaycomplejidad@gmail.com https://orcid.org/0000-0003-2472-7637
[3] Este artículo se relaciona con las líneas temáticas del curso intersemestral "Privacidad y tecnologías emergentes: implicaciones jurídicas", impartido por los autores en el Posgrado de la UNAM, a través de Educación Continua. El curso aborda, entre otros temas, privacidad, protección de datos personales, derecho al olvido, inteligencia artificial, biometría y drones. Véase: https://educacion-continua.posgrado.unam.mx/curso?id=238. fecha de consulta: 13 de mayo de 2026.

internet expresa la dimensión informacional y relacional; la biometría, la corporal e identitaria; y los drones, la espacial y observacional. A partir de una metodología jurídico-documental, analítica, propositiva y bibliométrica, se revisa doctrina, jurisprudencia, informes internacionales y el marco mexicano aplicable. El artículo concluye que la privacidad requiere un modelo preventivo, proporcional y responsable, basado en minimización, transparencia significativa, privacidad desde el diseño, trazabilidad y reparación efectiva.
**Palabras clave:** derecho a la privacidad; protección de datos personales; tecnologías emergentes; internet; biometría; drones.

**Abstract:** This article analyzes the reconfiguration of the right to privacy and the protection of personal data in relation to the internet, biometrics and drones. It argues that the protection of personal data, based on consent, privacy notices and subsequent exercise of ARCO rights (access, rectification, cancellation, and opposition), is insufficient for technologies that track, identify and observe individuals in ordinary contexts. The three cases serve an analytical purpose: the internet represents the informational and relational dimension; biometrics, the bodily and identity-based dimension; and drones, the spatial and observational dimension. Through a legal-documentary, analytical, normative and bibliometric approach, the article reviews scholarship, case law, international reports and the Mexican legal framework. It concludes that effective privacy protection requires a preventive, proportionate and accountable model based on minimization, meaningful transparency, privacy by design, traceability and effective remedies.
**Keywords:** right to privacy; protection of personal data; emerging technologies; internet; biometrics; drones.

SUMARIO. I. Introducción. II. El derecho a la privacidad y el derecho a la protección de datos personales ante el cambio tecnológico. III. Estado actual del campo de investigación: aproximación bibliométrica. IV. Internet y privacidad digital: rastreo, perfilamiento y pérdida de control informacional. V. Biometría y privacidad: cuerpo, identidad y vigilancia persistente. VI. Drones y privacidad: observación aérea, espacio público y

captación de terceros. VII. Contexto jurídico mexicano: bases normativas, límites y criterios para una protección eficaz. VIII. Conclusiones. IX. Referencias bibliográficas.

## I. Introducción

El artículo parte de una preocupación central: la distancia existente entre el reconocimiento y la regulación del derecho a la privacidad y a la protección de los datos personales, por un lado, y su protección efectiva en la vida cotidiana, por otro. Una persona puede ser titular del derecho a la privacidad y de derechos a la protección de sus datos personales; sin embargo, en la práctica puede no saber quién la observa, qué información se recaba, qué inferencias se producen, quién recibe esos datos o qué mecanismo real tiene para reclamar. Esa brecha se intensifica con tecnologías capaces de rastrear, identificar y observar sin una interacción visible con la persona afectada.

La pregunta central de investigación es ¿cómo se reconfiguran el derecho a la privacidad y el derecho a la protección de datos personales frente a tecnologías emergentes como internet, la biometría y los drones, y qué criterios jurídicos permiten protegerlo eficazmente frente al rastreo digital, la identificación corporal y la observación aérea?

La hipótesis sostiene que el derecho a la privacidad y a la protección de datos personales adquieren nuevas dimensiones porque las afectaciones actuales ya no se limitan a una privacidad negativa que radica en la prohibición de la intromisión directa en la intimidad y al ser dejado solo en este espacio; sino que encontramos su evolución a una privacidad positiva, en la que se adaptan los valores de protección a las sede digital, buscando permitir al individuo un control activo sobre el rastreo digital, perfilamiento, identificación biométrica, observación aérea, captura incidental de terceros e inferencias automatizadas, en relación con la recolección y uso de sus datos personales. Por ello, el modelo de protección a la privacidad y particularmente, de protección de datos personales, centrado en el consentimiento, aviso de privacidad y ejercicio posterior de derechos ARCO [4] debe complementarse con principios rectores como la prevención, la

[4] Existe una tendencia de expandir el tema de la "portabilidad" de datos como un elemento adicional a los derechos de acceso, rectificación, cancelación y oposición (ARCO), en este caso, se está hablando en algunos escenarios como "ARCOP". Un ejemplo sobre esto es el caso de los números telefónicos, que antes de la tendencia de la portabilidad eran considerados como caracteres alfanuméricos desligados del individuo, y hoy en día, son considerados un dato personal del titular de la línea, que puede incluso cambiar entre compañías telefónicas, conservando su número telefónico. Instituto de Transparencia, Acceso a la

proporcionalidad, la transparencia, la minimización de datos, la privacidad desde el diseño, la trazabilidad de responsables y la reparación efectiva.

El objetivo general consiste en analizar esas nuevas dimensiones y proponer criterios de protección aplicables al contexto mexicano. Para ello se reconstruye la evolución del derecho a la privacidad, se examinan los riesgos del entorno digital, y se estudian casos particulares como la biometría como dimensión corporal e identitaria, los drones como tecnologías de observación espacial, así como se proponen criterios normativos para una protección más eficaz.

La metodología es jurídico-documental, analítica y propositiva. Se revisa doctrina nacional e internacional, jurisprudencia, informes especializados y normativa mexicana; además, se incorpora una aproximación bibliométrica para ubicar la estructura del campo de investigación. Los casos de internet, biometría y drones se analizan por variación funcional, pues cada uno permite observar una forma distinta de afectación a la privacidad.

La elección de internet, biometría y drones no es arbitraria. Internet representa la dimensión informacional y relacional; la biometría, la dimensión corporal e identitaria; y los drones, la dimensión espacial y observacional. En conjunto, muestran que la privacidad y los datos personales ya no se protegen sólo frente a la detención de intromisiones al espacio privado, sino frente a entornos tecnológicos capaces de rastrear, identificar y observar a las personas en la vida diaria.

## II. El derecho a la privacidad y el derecho a la protección de datos personales ante el cambio tecnológico.

El derecho a la privacidad no es una categoría estática: cambia conforme se transforman los medios técnicos de observación, exposición, identificación y vigilancia. La formulación clásica de Warren y Brandeis surgió frente a tecnologías que modificaban la captura y difusión de la vida personal; desde entonces, cada innovación capaz de

Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, "La portabilidad de los datos personales es un derecho que se debe garantizar a todas las personas: especialistas," boletín DCS/155/2022, consultado el 13 de mayo de 2026, https://infocdmx.org.mx/index.php/2-boletines/7719-dcs-155-2022.html

ampliar la circulación de información obliga al Derecho a precisar los límites de la intromisión legítima.[5]

El derecho a la privacidad en un sentido negativo se ha entendido como derecho a no ser molestado. Posteriormente, con Alan Westin, se presenta otra dimensión del derecho a la privacidad positiva, no solo como la no intromisión ilegítima, sino como la decisión de determinar la información personal que se da a conocer a otros.[6]

Por ello, Daniel Solove propone abandonar una definición única y analizar problemas concretos de recolección, procesamiento, diseminación e invasión, enfoque especialmente útil frente a tecnologías emergentes.[7]

Helen Nissenbaum aporta otra clave: la privacidad como integridad contextual. El problema no se reduce a saber si una información es pública o privada, sino a determinar si su flujo respeta las normas del contexto, la finalidad, los sujetos que intervienen, la forma de captura, la retención y los posibles usos posteriores.[8]

Esta expansión también se reconoce en el derecho internacional. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[9] y el artículo 11 de la Convención Americana sobre Derechos Humanos[10] protegen contra injerencias arbitrarias o abusivas en la privacidad, familia, domicilio o correspondencia. La Corte Interamericana ha vinculado esta protección con las comunicaciones y con exigencias de legalidad, finalidad legítima, necesidad y proporcionalidad.[11]

La Oficina del Alto Comisionado de Naciones Unidas ha advertido que las tecnologías digitales y la inteligencia artificial pueden afectar la privacidad mediante vigilancia sistemática, automatización de decisiones y tratamiento masivo de datos. Esta advertencia confirma que el derecho a la privacidad es un derecho transversal, cuya

---

[5] *Cfr.* Warren, Samuel D. y Brandeis, Louis D., "The Right to Privacy", Harvard Law Review, Cambridge, vol. IV, núm. 5, 1890, pp. 193-220.
[6] *Cfr.* Westin, Alan, Privacy and Freedom, Nueva York, Ig Publishing, 2015, p. 5.
[7] *Cfr.* Solove, Daniel J., "A Taxonomy of Privacy", University of Pennsylvania Law Review, Philadelphia, vol. 154, 2006, pp. 477-564.
[8] *Cfr.* Nissenbaum, Helen, "Privacy as Contextual Integrity", Washington Law Review, Seattle, vol. 79, núm. 1, 2004, pp. 119-157.
[9] *Cfr.* Organización de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, Nueva York, 1966, art. 17.
[10] *Cfr.* Organización de los Estados Americanos, Convención Americana sobre Derechos Humanos, San José, 1969, art. 11.
[11] *Cfr.* Corte Interamericana de Derechos Humanos, Caso Escher y otros vs. Brasil, sentencia de 6 de julio de 2009, Fondo, Reparaciones y Costas, párr. 114.

afectación puede comprometer libertad de expresión, asociación, igualdad, debido proceso, participación política y libertad de movimiento.[12]

El derecho a la privacidad debe comprenderse como un espacio de autodeterminación informativa: permite deliberar, buscar información, formar opiniones, relacionarse y construir identidad sin observación o perfilamiento constante. Cuando la vida cotidiana se convierte en dato, el cuerpo en identificador permanente y el espacio físico en objeto de observación aérea, la privacidad deja de ser una frontera fija y se vuelve una condición de autonomía, dignidad y libertad.

Sobre el concepto de autodeterminación informativa, lo encontramos por primera vez en la afamada resolución del Tribunal Constitucional Federal Alemán sobre el Censo de Población, en la que la definió como aquella facultad del individuo de decidir el momento y los límites de la información personal que revela a terceros.[13]

En el Sistema Interamericano, este derecho a la autodeterminación informativa fue reconocido por la Corte Interamericana de Derecho Humanos en el Caso Cajar vs. Colombia, al señalar que en nuestra región existe un derecho autónomo a la autodeterminación informativa que tiene una relación directa con la protección de la vida privada y la dignidad de la persona.[14]

Como respuesta a la necesidad de protección de datos personales ante una economía de datos, la protección de datos personales se ha erigido como un derecho autónomo, que dota al sistema de las normas adjetivas necesarias para garantizar la autodeterminación informativa a través de los derechos ARCO.

Sin embargo, no podemos afirmar que, con el reconocimiento de este derecho y su ejercicio, se agoten los supuestos de riesgo que implica el uso de nuevas tecnologías en la vida diaria de los individuos, ya que su lógica de protección se relaciona principalmente con recabar lícitamente datos personales a través del consentimiento informado, así como imponer límites al responsable de su tratamiento y un cierto control del titular de estos,

---

[12] *Cfr.* Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, The Right to Privacy in the Digital Age, A/HRC/48/31, Ginebra, Naciones Unidas, 2021, párrs. 20-25.

[13] *Cfr.* Tribunal Constitucional Federal Alemán, "Sentencia BVerfGE 65,1 [Censo de Población]", en Schwabe, Jürgen (comp.), *Cincuenta años de jurisprudencia del Tribunal Constitucional Federal*, trad. de Marcela Anzola, 2009, p. 94.

[14] *Cfr.* Corte Interamericana de Derechos Humanos, Caso miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, sentencia del 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas, p. 179.

reflejado en los derechos ARCO. Debemos afirmar, como se demuestra en el presente artículo, que este alcance no es suficiente para brindar protección completa ante los supuestos usos que puede darse de los datos personales con la implementación de tecnologías emergentes.

Esta lectura dinámica puede reforzarse con la doctrina de la expectativa razonable de privacidad. Originalmente expuesta en 1967 en el caso Katz contra Estados Unidos, en el que se analizó la expectativa razonable de privacidad del individuo, estableciendo que con ella se puede garantizar la protección del derecho a la privacidad[15]:

En México, hemos tenido aproximaciones a esta visión para determinar la expectativa de derecho a la privacidad del individuo. Un ejemplo de ellos es el fragmento público del proyecto de sentencia del Amparo directo en revisión 5823/2018, en el que se examina la relación entre vida privada, privacidad de las comunicaciones y libertad de expresión en ámbitos controlados por la persona. Su utilidad para este artículo radica en superar una dicotomía rígida entre lo público y lo privado: frente a tecnologías de grabación, identificación y conservación de información, la expectativa de privacidad debe analizarse según contexto, sujeto, lugar, medio de obtención, grado de intrusión y finalidad.[16]

En consecuencia, el derecho a la privacidad debe interpretarse dinámicamente y con criterios de eficacia. La inviolabilidad del domicilio, la correspondencia y en general, del espacio privado, siguen siendo relevantes, pero hoy deben dialogar con la protección de datos personales, identidad digital, biometría, rastreo, vigilancia, perfiles e inferencias. Un derecho que depende de leer avisos extensos, comprender algoritmos o identificar responsables en los intermediarios corre el riesgo de perder un efecto útil para la debida protección, respeto y garantía de los derechos humanos en sede digital; por eso, las nuevas dimensiones del derecho a la privacidad y la protección de datos personales requieren anticipación, diseño y supervisión.

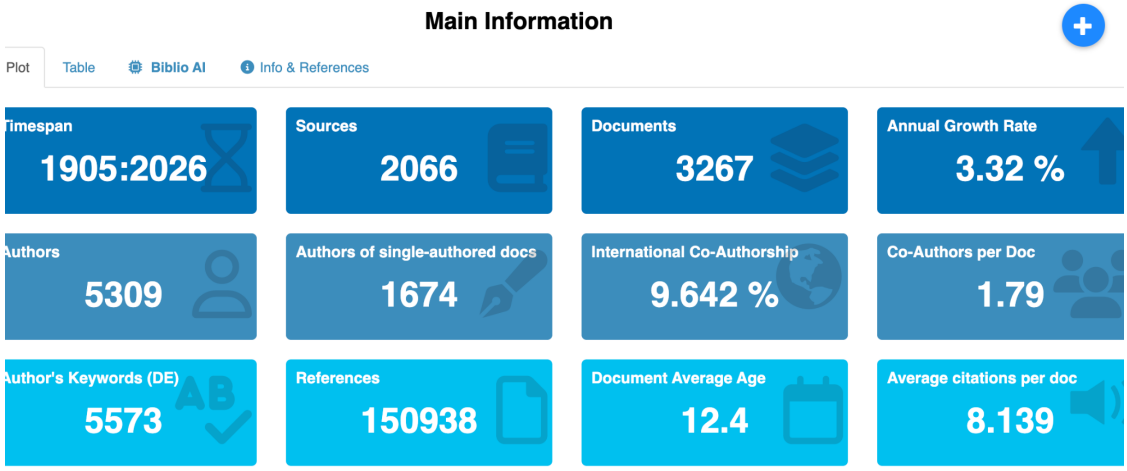
## III. Estado actual del campo de investigación: aproximación bibliométrica.

[15] *Cfr.* Quijano Decanini, C. (2022). Derecho a la privacidad en Internet. Tirant lo Blanch, p. 63.
[16] *Cfr.*Suprema Corte de Justicia de la Nación, Amparo directo en revisión 5823/2018, Primera Sala, fragmento público del proyecto de sentencia, párrs. 77-84, 103-110 y 115-118.

Para ubicar el estado actual del campo de investigación se incorporó una aproximación bibliométrica complementaria al análisis jurídico. Esta herramienta permite observar la estructura de la producción académica, identificar tendencias y justificar la selección de internet, biometría y drones dentro de una discusión más amplia sobre derecho a la privacidad, protección de datos personales y vigilancia.[17]

La búsqueda se realizó en Scopus a partir de la expresión exacta *right to privacy*[18], localizada en los campos de título, resumen y palabras clave. El corpus general arrojó 3267 documentos, publicados entre 1905 y 2026, distribuidos en 2066 fuentes y con participación de 5309 autores. Estos datos muestran una trayectoria amplia y sostenida, reactivada por debates recientes sobre tecnologías digitales, inteligencia artificial, protección de datos y vigilancia.[19]

**Figura 1.** Información general del corpus bibliométrico sobre *right to privacy*



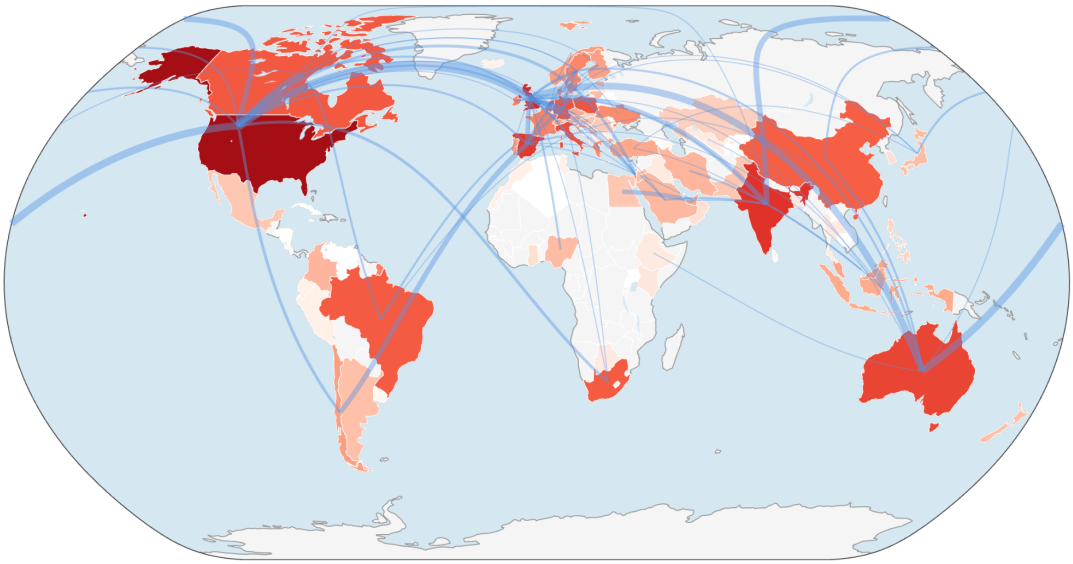

*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

El mapa de colaboración por países muestra una fuerte presencia de Estados Unidos, Reino Unido, Canadá, India, China, Australia y diversos países europeos, así como conexiones con América Latina, Asia y Oceanía. El dato confirma que la privacidad

[17] *Cfr.* Donthu, Naveen, Kumar, Satish, Mukherjee, Debmalya, Pandey, Nitesh y Lim, Weng Marc, "How to Conduct a Bibliometric Analysis: An Overview and Guidelines", Journal of Business Research, Ámsterdam, vol. 133, 2021, pp. 285-296.
[18] Se presentan los términos en inglés por los requisitos de operación del sistema Scopus.
[19] *Cfr.* Zupic, Ivan y Čater, Tomaž, "Bibliometric Methods in Management and Organization", Organizational Research Methods, Thousand Oaks, vol. 18, núm. 3, 2015, pp. 429-472.

tecnológica se discute en un espacio transnacional donde convergen enfoques constitucionales, regulatorios, tecnológicos y de derechos humanos.

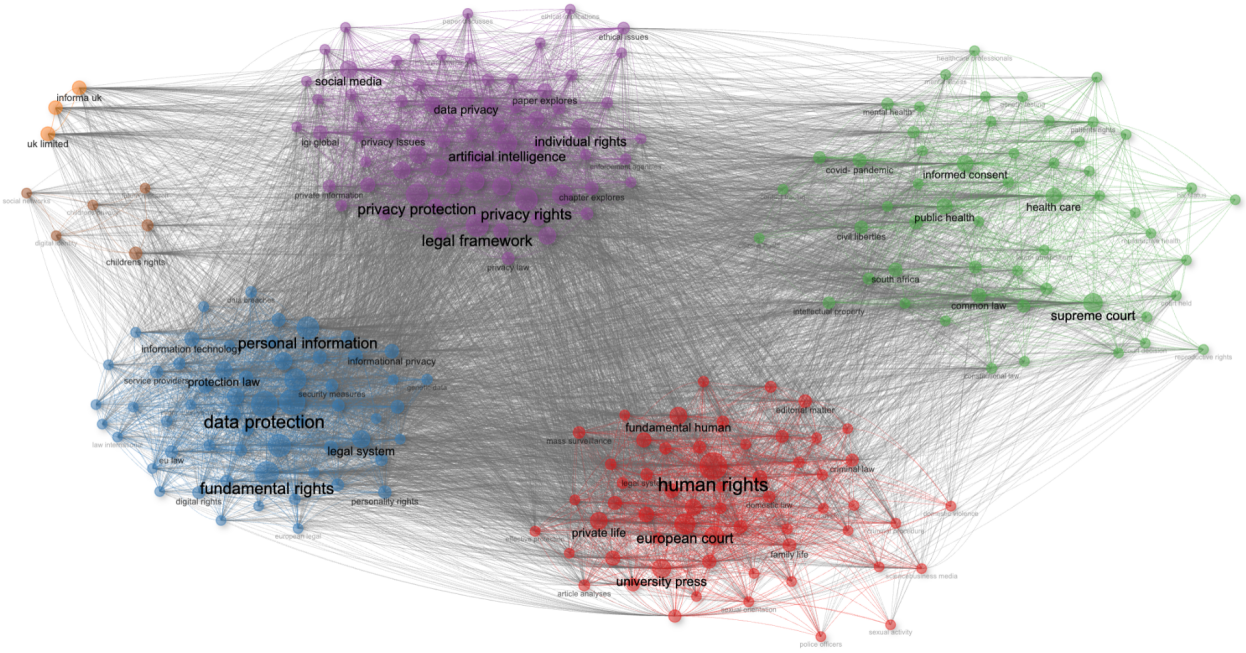
**Figura 2.** Mapa de colaboración internacional del corpus sobre derecho a la privacidad



*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

La red de coocurrencia muestra al menos cuatro núcleos: *data protection, personal information, fundamental rights y legal system; privacy protection, privacy rights, artificial intelligence, social media y legal framework; human rights, private life, European Court y fundamental human; e informed consent, public health, health care y Supreme Court*. Esta distribución confirma que el derecho a la privacidad contemporáneo se articula con protección de datos, derechos humanos, plataformas digitales, salud, inteligencia artificial y justicia constitucional.

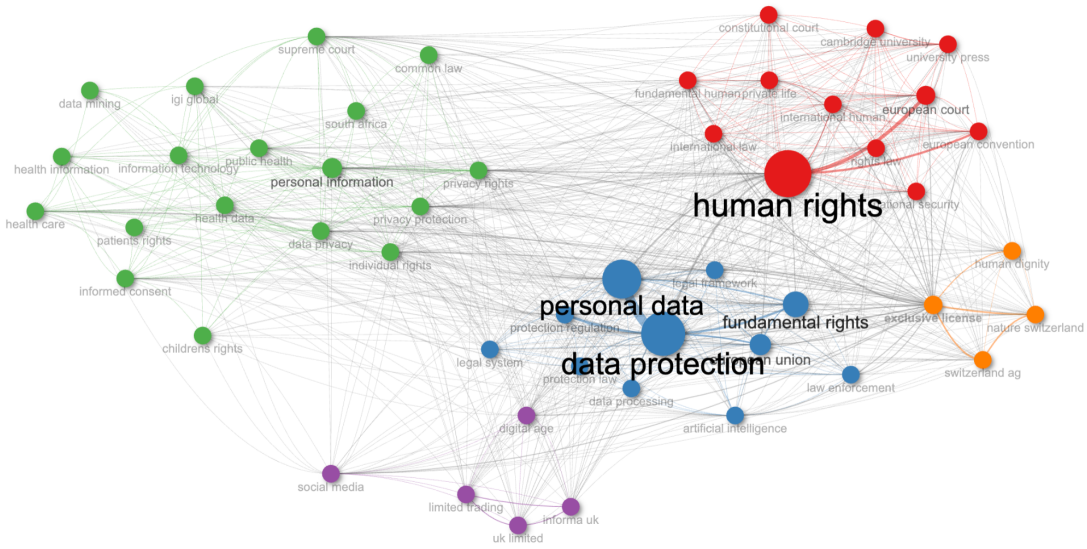
**Figura 3.** Red general de coocurrencia conceptual del corpus sobre right to privacy




*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

El acercamiento conceptual permite identificar los nodos que articulan la discusión jurídica: *human rights, data protection, personal data, fundamental rights, privacy protection, legal framework, artificial intelligence y law enforcement*. La imagen refuerza la tesis del artículo: la privacidad opera en la intersección entre datos personales, vigilancia, tecnologías inteligentes, actuación estatal, mercados digitales y otros derechos fundamentales.

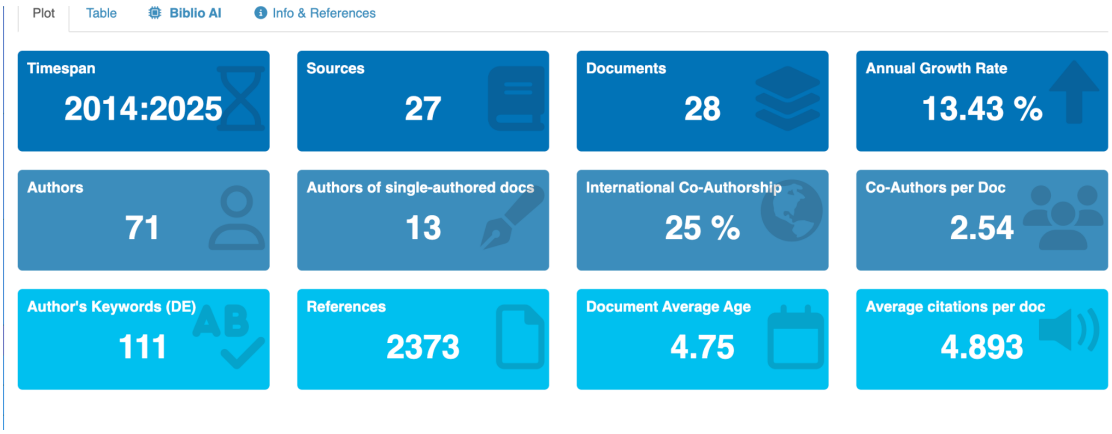
**Figura 4.** Mapa conceptual específico del campo: datos personales, derechos humanos y protección jurídica




*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

Para ubicar la dimensión específica de drones se realizó una búsqueda segmentada que combinó *right to privacy* con *drone* mediante el operador booleano AND, en los mismos campos de título, resumen y palabras clave. El subconjunto arrojó 28 documentos entre 2014 y 2025, 27 fuentes, 71 autores, 2373 referencias y 111 palabras clave de autor. Aunque pequeño, presenta una tasa de crecimiento anual de 13.43 %, 25 % de coautoría internacional y 2.54 coautores por documento, lo que sugiere un subcampo emergente.

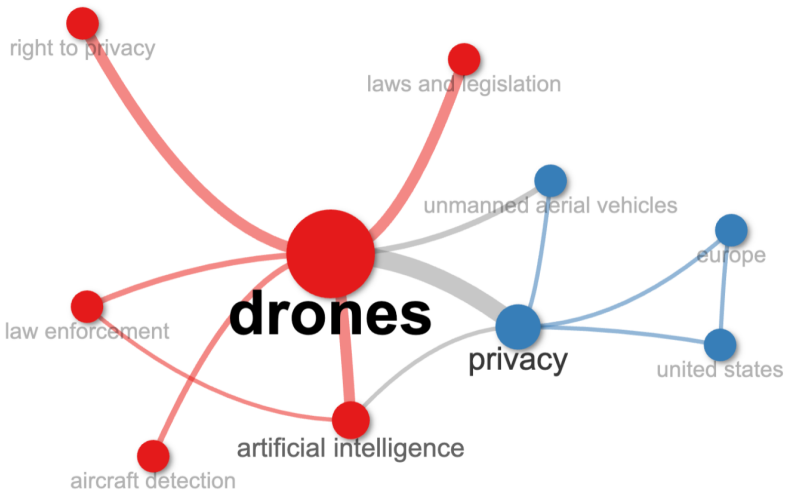
**Figura 5.** Información general del corpus segmentado sobre right to privacy AND drone




*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

La red específica muestra que el nodo drones se conecta con privacy, unmanned aerial vehicles, artificial intelligence, law enforcement, aircraft detection, laws and legislation y right to privacy. La posición de privacy como nodo de enlace revela que el problema no es sólo aeronáutico o técnico, sino también regulatorio, policial, tecnológico y de derechos fundamentales.

**Figura 6.** Red de coocurrencia del corpus segmentado sobre drones y derecho a la privacidad




*Fuente: Elaboración propia con bibliometrix/BiblioShiny, con datos de Scopus.*

En conjunto, las visualizaciones delimitan el objeto de estudio. La búsqueda general muestra la expansión del derecho a la privacidad hacia protección de datos, derechos humanos, inteligencia artificial y vigilancia; la búsqueda sobre drones evidencia un campo menor, pero relevante por desplazar la privacidad al espacio físico. Por ello, internet, biometría y drones funcionan como tres formas de afectación: rastreo informacional, identificación corporal y observación espacial.

Lo anterior nos ayuda a identificar la situación actual del campo de estudio, lo cual es útil para contextualizar la profundidad de las investigaciones que hay en torno al tema, así como los conceptos, nociones, autorías y regiones donde se está discutiendo la temática.

## IV. Internet y privacidad digital: rastreo, perfilamiento y pérdida de control informacional.

Internet representa la dimensión informacional y relacional de la privacidad. En México, la ENDUTIH 2024 estimó 100.2 millones de personas usuarias de internet, equivalentes al 83.1 % de la población de seis años y más. Su relevancia jurídica no está sólo en esa magnitud, sino en que cookies, historial de búsqueda, geolocalización, metadatos, redes sociales, aplicaciones y sistemas de recomendación permiten perfilar gustos, rutinas, relaciones, vulnerabilidades y conductas probables.[20]

La literatura sobre dataficación muestra que actividades antes efímeras —buscar, hacer clic, comprar, reaccionar o desplazarse— se convierten en datos acumulables, comparables y monetizables. La privacidad se altera porque la correlación de datos dispersos permite producir conocimiento sensible que la persona no cree haber revelado.[21]

El consentimiento opera con especial debilidad en internet. Las personas aceptan términos y condiciones de forma rutinaria, con información incompleta, sesgos, asimetrías de poder y costos de transacción. Así, el sistema formal presume consentimiento, mientras la experiencia cotidiana revela fatiga, opacidad y falta de control.[22]

La OCDE reportó en su Digital Economy Outlook 2024 que más de la mitad de las personas encuestadas evita ciertos sitios, aplicaciones o redes sociales por preocupaciones de privacidad, y que alrededor de un tercio siente falta de control sobre sus datos personales. El dato confirma que la privacidad digital es un componente de confianza pública.[23]

El perfilamiento es una de las formas más relevantes de afectación a la privacidad en internet. No siempre se necesita conocer un dato íntimo de manera directa; basta combinar fragmentos de información para inferir preferencias, riesgos, solvencia, salud, ideología, consumo o comportamiento probable. El perfilamiento puede tener efectos en

---

[20] *Cfr.* Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2024*, México, INEGI, 2025, p. 3.

[21] *Cfr.* Van Dijck, José, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology", Surveillance & Society, Kingston, vol. 12, núm. 2, 2014, pp. 197-208.

[22] *Cfr.* Acquisti, Alessandro, Taylor, Curtis y Wagman, Liad, "The Economics of Privacy", Journal of Economic Literature, Nashville, vol. 54, núm. 2, 2016, pp. 442-492.

[23] *Cfr.* Organización para la Cooperación y el Desarrollo Económicos, OECD Digital Economy Outlook 2024, vol. 2, París, OECD Publishing, 2024, cap. "Media consumption and privacy".

publicidad, crédito, empleo, seguros, seguridad, educación o servicios públicos. Por ello, la privacidad digital se relaciona con oportunidades reales y no sólo con la reserva subjetiva de información.

Shoshana Zuboff ha descrito el capitalismo de vigilancia como un modelo económico basado en la extracción de datos conductuales y su conversión en productos predictivos.[24] Más allá de las discusiones sobre el alcance de su tesis, resulta útil para comprender que internet no es sólo un medio de comunicación, sino un entorno de captura de valor informacional. La privacidad se tensiona cuando la arquitectura de plataformas incentiva recabar más datos de los necesarios, mantenerlos durante más tiempo y utilizarlos para modelar conducta.

La jurisprudencia comparada ilustra esta transformación. En Google Spain, el Tribunal de Justicia de la Unión Europea reconoció que los motores de búsqueda pueden afectar la privacidad al organizar información disponible y asociarla de forma persistente con el nombre de una persona. El efecto jurídico no provenía del secreto del dato, sino de su indexación y accesibilidad estructurada.[25]

En Digital Rights Ireland, el mismo tribunal invalidó la retención masiva e indiferenciada de datos de comunicaciones. El caso muestra que el derecho a la privacidad protege no sólo contenidos, sino también metadatos, horarios, ubicaciones y vínculos relacionales, especialmente cuando se analizan a gran escala.[26]

En el sistema interamericano, Escher y otros vs. Brasil permite ampliar la mirada: la protección de la privacidad comprende comunicaciones y exige límites jurídicos estrictos. En internet, esto incluye mensajes, trayectorias de navegación, datos de conexión, destinatarios, horarios y estructuras de relación.[27]

El big data intensifica estos riesgos. Elena Gil González ha señalado que el tratamiento masivo de datos genera beneficios económicos y sociales, pero exige no

[24] *Cfr.* Zuboff, Shoshana, *The Age of Surveillance Capitalism*, Nueva York, PublicAffairs, 2019, pp. 8-12.
[25] *Cfr.* Tribunal de Justicia de la Unión Europea, Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González, asunto C-131/12, sentencia de 13 de mayo de 2014.
[26] *Cfr.* Tribunal de Justicia de la Unión Europea, Digital Rights Ireland Ltd. vs. Minister for Communications, Marine and Natural Resources y otros, asuntos acumulados C-293/12 y C-594/12, sentencia de 8 de abril de 2014.
[27] *Cfr.* Corte Interamericana de Derechos Humanos, Caso Escher y otros vs. Brasil, cit., párr. 114.

soslayar la garantía del derecho a la protección de datos personales.[28] Esta tensión es central: la utilidad de los datos no elimina la necesidad de límites. En internet, la promesa de innovación, eficiencia o personalización puede convertirse en justificación para prácticas de seguimiento difíciles de advertir y controlar.

La dimensión relacional de internet es igualmente importante. Las personas no sólo entregan información propia; también generan datos sobre otras personas. Una fotografía compartida, una etiqueta, una conversación, una lista de contactos, una ubicación o una referencia indirecta puede afectar a terceros que no participaron en la decisión de publicar o compartir. Por ello, el consentimiento individual no basta para explicar todos los flujos informacionales. La protección del derecho a la privacidad en el espacio digital es también un problema de interdependencia.

Julie Cohen ha insistido en que la privacidad cumple una función estructural para la autonomía y para la vida democrática.[29] Si las personas saben que cada búsqueda, opinión o vínculo puede ser rastreado, clasificado y utilizado para influir en su comportamiento, se reduce el espacio de experimentación personal. La privacidad protege no sólo lo que se oculta, sino la posibilidad de explorar identidades, ideas y relaciones sin quedar fijado permanentemente por sistemas de clasificación.

En síntesis, internet muestra que la vida cotidiana se convierte en datos. El reto jurídico no es proteger un espacio de privacidad aislado de la red, sino asegurar que la participación digital no implique renunciar al control básico sobre los datos personales ni aceptar rastreo, perfilamiento o explotación informacional sin justificación y proporcionalidad suficiente.

## V. Biometría y privacidad: cuerpo, identidad y vigilancia persistente.

La biometría representa la dimensión corporal e identitaria de la privacidad. Los datos biométricos —rostro, huella, iris, retina, voz, geometría facial o patrones conductuales— permiten reconocer o verificar identidad mediante rasgos físicos o de

[28] *Cfr.* Gil González, Elena, Big data, privacidad y protección de datos, Madrid, Agencia Española de Protección de Datos-Boletín Oficial del Estado, 2016, pp. 13-16.
[29] *Cfr.* Cohen, Julie E., *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Nueva York, Oxford University Press, 2019, pp. 30-35.

comportamiento. Su utilidad para seguridad, autenticación o acceso no elimina sus riesgos, pues convierte el cuerpo en infraestructura de identificación y vigilancia.[30]

Aunado a ello, recaen en la categoría de datos personales sensibles reconocida por el sistema normativo vigente en nuestro país, por la grave afectación que puede implicar su uso indebido para el individuo.

La diferencia con otros datos personales es cualitativa: una contraseña puede modificarse, pero el rostro, la huella o el iris están ligados a la identidad corporal y no pueden sustituirse fácilmente. Por ello, una filtración, centralización indebida o uso secundario de datos biométricos puede producir daños persistentes.[31]

La biometría altera la relación entre presencia física e identificación. Una persona puede ser reconocida sin interactuar con el sistema, a partir de una cámara, una voz o una comparación automatizada con bases de datos. Marianne Díaz resume esta problemática bajo la idea del cuerpo como dato.[32]

El reconocimiento facial es especialmente sensible porque permite identificar de manera remota, automatizada y potencialmente masiva. Introna y Wood advierten que estos sistemas deben analizarse como formas de vigilancia algorítmica, no sólo como herramientas neutrales de seguridad.[33]

Los problemas de precisión y sesgo también son relevantes. Buolamwini y Gebru encontraron disparidades importantes en sistemas comerciales de análisis facial, con mayores errores en mujeres de piel más oscura. La biometría puede afectar el derecho a la privacidad, igualdad, no discriminación y debido proceso, tanto por identificar como por clasificar erróneamente.[34]

Las autoridades de protección de datos han advertido que los tratamientos biométricos requieren necesidad, proporcionalidad y alternativas menos intrusivas, sobre

[30] *Cfr.* Jain, Anil K., Ross, Arun y Prabhakar, Salil, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Nueva York, vol. 14, núm. 1, 2004, pp. 4-20.
[31] *Cfr* Ibidem, pp. 6-8.
[32] *Cfr* Díaz, Marianne, *El cuerpo como dato*, Santiago de Chile, Derechos Digitales, 2018, pp. 6-10.
[33] I *Cfr* ntrona, Lucas D. y Wood, David, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", Surveillance & Society, Kingston, vol. 2, núms. 2/3, 2004, pp. 177-198.
[34] *Cfr* Buolamwini, Joy y Gebru, Timnit, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research, vol. 81, 2018, pp. 77-91.

todo cuando implican identificación y no sólo verificación. Identificar a cualquiera dentro de una multitud es más intrusivo que confirmar voluntariamente una identidad declarada.[35]

En México, el debate constitucional sobre el Padrón Nacional de Usuarios de Telefonía Móvil mostró los riesgos de recabar datos identificatorios, incluidos biométricos, para un registro obligatorio. La discusión advirtió que la acumulación masiva de datos puede proporcionar al Estado capacidades intensas de vigilancia si no se observan los principios de finalidad legítima, necesidad y proporcionalidad, así como la implementación de controles estrictos.[36]

El caso PANAUT confirma que la seguridad pública puede ser una finalidad legítima, pero no toda recolección masiva es necesaria o proporcional. La exigencia de biométricos a toda la población usuaria de telefonía requiere una justificación adecuada y legítima, optar por alternativas menos invasivas e implemntar controles robustos de seguridad y acceso.[37]

La CURP biométrica actualiza esta tensión. La Ley General de Población prevé una clave con huellas dactilares y fotografía como documento nacional de identificación, así como una Plataforma Única de Identidad. [38] Estos sistemas pueden servir a finalidades públicas relevantes, pero concentran riesgos de centralización y usos secundarios.[39]

El Reglamento General de Protección de Datos de la Unión Europea considera los datos biométricos como categoría especial cuando se tratan para identificar de manera unívoca a una persona. La razón es clara: el dato biométrico puede convertir el cuerpo en identificador permanente y facilitar vigilancia sistemática.[40]

La biometría plantea al menos cuatro riesgos jurídicos. El primero es la irreversibilidad relativa: si una contraseña se filtra, puede cambiarse; si se filtra una plantilla biométrica, la persona no puede cambiar su rostro, su iris o sus huellas. El

---

[35] *Cfr* Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*, Madrid, AEPD, 2023.
[36] *Cfr* Suprema Corte de Justicia de la Nación, *Acción de inconstitucionalidad 82/2021 y acumulada 86/2021*, Pleno, sentencia relativa al Padrón Nacional de Usuarios de Telefonía Móvil.
[37] *Cfr.* Idem.
[38] *Cfr* . Cámara de Diputados del H. Congreso de la Unión, Ley General de Población, México, última reforma publicada en el Diario Oficial de la Federación el 16 de julio de 2025, art. 91 Bis.
[39] *Cfr* . Secretaría de Gobernación, Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad, Diario Oficial de la Federación, México, 27 de noviembre de 2025.
[40] *Cfr.* Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento General de Protección de Datos, Diario Oficial de la Unión Europea, 27 de abril de 2016, art. 9.

segundo es la posibilidad de identificación remota: el sujeto puede ser reconocido sin interacción consciente. El tercero es la centralización: las bases masivas aumentan el impacto de filtraciones o usos indebidos. El cuarto es la función de vigilancia: los datos biométricos pueden vincular presencia física con registros administrativos, cámaras, accesos o bases de seguridad.

También existe un riesgo de normalización. Cuando la biometría se introduce para trámites sencillos, controles de acceso, servicios financieros, educación, transporte o trabajo, la sociedad puede acostumbrarse a entregar datos corporales como condición ordinaria de participación. Esa normalización reduce la percepción de riesgo y debilita la capacidad de resistencia ciudadana. El Derecho debe evitar que la comodidad técnica sustituya el análisis de proporcionalidad, necesidad y finalidad al otorgar consentimiento para el tratamiento de datos personales.

La biometría no debe demonizarse. Puede apoyar la búsqueda e identificación de personas desaparecidas, reducir suplantaciones, mejorar servicios o facilitar accesibilidad. Pero precisamente por su utilidad debe regularse con rigor. La pregunta no es si la biometría puede servir, sino cuándo es necesaria, quién controla la base, qué datos se recaban, cómo se protegen, qué tratamiento reciben, quién accede, durante cuánto tiempo se conservan, qué usos secundarios están prohibidos y qué remedios tiene la persona afectada.

Desde la perspectiva del derecho a la privacidad, la biometría desplaza la privacidad hacia el cuerpo. La persona ya no sólo se protege frente a la divulgación de información íntima, sino frente a la conversión de rasgos corporales en objetos de tratamiento, comparación, clasificación y vigilancia. Esta dimensión corporal exige reglas reforzadas: consentimiento explícito, base legal clara para autoridades, evaluación de impacto, finalidad estricta, minimización, auditorías, seguridad técnica y mecanismos de corrección.

La biometría también exige distinguir entre autenticación e identificación. En la autenticación, la persona presenta voluntariamente un rasgo para confirmar una identidad previamente declarada. En la identificación, el sistema busca determinar quién es la persona a partir de una base de datos. La segunda modalidad es más intrusiva porque puede operar sin cooperación del individuo y a escala poblacional. Por ello, la

identificación biométrica remota debe someterse a controles más severos que la autenticación voluntaria y limitada.

En síntesis, la biometría es el segundo caso paradigmático porque muestra que el derecho a la privacidad ya no se agota en la información externa sobre la persona. El cuerpo mismo se vuelve dato, credencial y punto de acceso. Esta transformación exige que el Derecho trate los datos biométricos como información de especial sensibilidad, no por una preocupación abstracta, sino porque su mal uso puede afectar la identidad, la dignidad, la igualdad, la seguridad y la libertad de movimiento.

## VI. Drones y privacidad: observación aérea, espacio público y captación de terceros.

Los drones representan la dimensión espacial y observacional de la privacidad. Su relevancia no radica sólo en que vuelan, sino en que permiten observar, grabar y captar información desde perspectivas antes menos accesibles: calles, patios, azoteas, reuniones, ventanas, predios, vehículos o trayectorias. La literatura especializada ha señalado que los sistemas aéreos no tripulados pueden afectar privacidad y libertades civiles, sobre todo cuando se usan para vigilancia. El riesgo surge de la combinación de movilidad, cámara, accesibilidad, distancia del operador y dificultad de identificación del responsable.[41]

Los drones combinan seguridad aérea, responsabilidad civil, protección de datos, imagen, vigilancia, propiedad, espacio público y protección de terceros. Clarke y Bennett Moses advierten que la regulación civil presenta lagunas, especialmente frente a drones pequeños o microdrones, porque muchas reglas tradicionales fueron pensadas para aeronaves o cámaras fijas.[42] Bart Custers propone analizar los drones atendiendo a oportunidades y amenazas. Pueden servir para labores de rescate, protección civil, agricultura, inspección, monitoreo ambiental, periodismo o investigación; pero también facilitar acoso, seguimiento, captación íntima o recopilación de información sin consentimiento. La regulación debe distinguir usos, contextos y riesgos.[43]

---

[41] *Cfr.* Finn, Rachel L. y Wright, David, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications", Computer Law & Security Review, Londres, vol. 28, núm. 2, 2012, pp. 184-194.
[42] *Cfr.* Clarke, Roger y Bennett Moses, Lyria, "The Regulation of Civilian Drones' Impacts on Public Safety", Computer Law & Security Review, Londres, vol. 30, núm. 3, 2014, pp. 263-285.
[43] *Cfr.* Custers, Bart (ed.), The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives, Cham, Springer, 2016, pp. 1-10.

Tampoco conviene tratarlos sólo como amenaza. En el sector civil se han vuelto herramientas de fotografía aérea, filmación, inspección, agricultura de precisión y logística. La literatura técnica, sin embargo, advierte que su expansión requiere seguridad operacional, seguridad informática, privacidad y marcos regulatorios compatibles con la protección de datos.[44]

En México, la NOM-107-SCT3-2019 regula la operación de sistemas de aeronave pilotada a distancia desde un enfoque principalmente aeronáutico: clasificación, condiciones de operación, responsabilidades técnicas, restricciones y requisitos de vuelo. Esa base es necesaria, pero no resuelve el problema de posibles intromisiones a la privacidad.[45]

Un dron puede cumplir reglas de operación aérea y, al mismo tiempo, captar imágenes de terceros, registrar espacios semiprivados o realizar una vigilancia no advertida. Por ello, siguen abiertas preguntas sobre los límites de grabación, la información a personas afectadas, la responsabilidad por difusión indebida y las salvaguardas en escuelas, hospitales, domicilios, manifestaciones, así como los usos en tareas de seguridad pública.[46]

La analogía con la videovigilancia es útil pero insuficiente. En el caso Ryneš, el Tribunal de Justicia de la Unión Europea sostuvo que la excepción doméstica al régimen de protección de datos no cubre necesariamente una cámara privada que capta espacios públicos.[47] El criterio es relevante para drones porque muestra que la captación de imágenes de terceros no se vuelve jurídicamente irrelevante por el hecho de ser realizada por un particular. Sin embargo, el dron agrega movilidad, altura, distancia e incertidumbre sobre el operador.

Los drones tensionan la frontera entre espacio público y privado. Ser visto en la calle no equivale a ser grabado sistemáticamente desde el aire, seguido por un dispositivo

[44] *Cfr.* Santamarina-Campos, Virginia y Segarra-Oña, Marival (eds.), Drones and the Creative Industry: Innovative Strategies for European SMEs, Cham, Springer Open, 2018, pp. v-vi.
[45] *Cfr.* Secretaría de Comunicaciones y Transportes, Norma Oficial Mexicana NOM-107-SCT3-2019, que establece los requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano, Diario Oficial de la Federación, México, 14 de noviembre de 2019.
[46] *Cfr.* Ibidem, numerales 4 y 5.
[47] *Cfr.*Tribunal de Justicia de la Unión Europea, František Ryneš vs. Úřad pro ochranu osobních údajů, asunto C-212/13, sentencia de 11 de diciembre de 2014.

o incorporado a una base de imágenes. La privacidad también protege la posibilidad de moverse, reunirse y habitar espacios sin observación injustificada.

La Organización de Aviación Civil Internacional ha desarrollado marcos sobre gestión de tránsito de sistemas no tripulados que incluyen registro, identificación, geo-conciencia y mecanismos de coordinación.[48] Estos instrumentos muestran que la gobernanza de drones no puede reducirse a decisiones individuales del operador. Requiere infraestructura normativa y técnica para coordinar seguridad, responsabilidad y trazabilidad. Al hablar del derecho a la privacidad, esa trazabilidad resulta crucial: si alguien es afectado por un dron, debe existir posibilidad real de identificar al responsable.

La arquitectura técnica también regula. Lawrence Lessig señaló que el código puede funcionar como una forma de regulación al determinar qué conductas son posibles, fáciles o difíciles.[49] En drones, esta idea se traduce en geocercas, identificación remota, límites de altura, zonas restringidas, registros de operación, indicadores de captura y configuraciones por defecto. Estos mecanismos no sustituyen al Derecho, pero pueden hacerlo más eficaz cuando se diseñan con criterios públicos y auditables, que sean respetuosos con los derechos de usuarios y terceros.

Los drones muestran con claridad el problema de terceros no usuarios. Una persona puede ser grabada sin haber comprado el dispositivo, sin conocer al operador y sin tener contacto con la empresa fabricante. El modelo de consentimiento individual resulta impracticable en estos casos. La protección de la privacidad exige reglas objetivas: límites de captación, prohibición de grabación dirigida a espacios íntimos, deberes de información cuando sea posible, restricciones en zonas sensibles y mecanismos de protección.

El estudio de Zwickle, Farber y Hamm confirma que la preocupación no es hipotética: las personas encuestadas apoyaron con mayor intensidad reglas para limitar la exposición frente a drones no deseados, especialmente las orientadas al respeto al derecho a la privacidad individual, y mostraron menor apoyo a restricciones que obstaculizaran

[48] *Cfr.* Organización de Aviación Civil Internacional, Unmanned Aircraft Systems Traffic Management (UTM): A Common Framework with Core Principles for Global Harmonization, 3a. ed., Montreal, OACI, 2023, pp. 10-14.
[49] *Cfr.* Lessig, Lawrence, Code and Other Laws of Cyberspace, Nueva York, Basic Books, 1999, pp. 3-8.

usos de seguridad pública. Esto refuerza la necesidad de regulación diferenciada y contextualizada.[50]

La dimensión periodística requiere especial cuidado. Los drones pueden documentar desastres, protestas, daños ambientales o hechos de interés público. Una prohibición general afectaría la libertad de expresión e información. Sin embargo, el interés público no autoriza todo tipo de captación ni difusión. La ponderación debe considerar la necesidad, la relevancia, la expectativa razonable de privacidad, la minimización de imágenes de terceros y la protección de datos personales de personas vulnerables, particularmente si pensamos en los niñas, niños y adolescentes.

En el ámbito estatal, el uso de drones para seguridad pública o inspección administrativa exige controles reforzados. La observación aérea puede convertirse en vigilancia masiva e intrusiva si se despliega sin fundamentos legales claros, sin finalidad específica, sin límites temporales y sin mecanismos de control. La protección del derecho a la privacidad requiere que toda vigilancia estatal sea legal, necesaria, proporcional y sujeta a supervisión. El hecho de que la tecnología sea menos costosa que otras formas de vigilancia no reduce la exigencia de protección y respeto a los derechos humanos.

Los drones también afectan a espacios privados en los que se pueden obtener imágenes por vía área . Patios, azoteas, jardines, balcones o ventanas pueden ser visibles desde el aire, pero eso no implica que dejen de ser espacios privados.. El Derecho debe reconocer que la protección del derecho a la privacidad y a la protección de datos personales no se define únicamente por muros físicos, sino por expectativas razonables de no ser observado con tecnologías que alteran la perspectiva ordinaria. La captación aérea dirigida a espacios domésticos debe considerarse especialmente intrusiva.

La doctrina mexicana reciente ayuda a precisar este punto: la expectativa de privacidad protege a las personas y puede ser legítima en espacios públicos cuando, conforme al contexto, sea razonable esperar un cierto grado de privacidad. Por ello, la vigilancia con drones debe analizarse por su grado de intrusión y no sólo por la posibilidad física de observación aérea.[51]

---

50 *Cfr.* Zwickle, Adam, Farber, Hillary B. y Hamm, Joseph A., "Comparing Public Concern and Support for Drone Regulation to the Current Legal Framework", Behavioral Sciences & the Law, 2018, pp. 1-16, doi: 10.1002/bsl.2357.

51 *Cfr.* Suprema Corte de Justicia de la Nación, Amparo directo en revisión 5823/2018, cit., párrs. 108-126.

En síntesis, los drones muestran que el derecho a la privacidad también se disputa en el espacio físico, la calle, el aire y los lugares cotidianos de convivencia. La pregunta jurídica decisiva no es si un dron puede volar, sino en qué condiciones puede observar, registrar y conservar información sobre personas.

## VII. Contexto jurídico mexicano: bases normativas, límites y criterios para una protección eficaz.

México cuenta con bases constitucionales e internacionales para proteger la privacidad. El artículo 1o. constitucional permite interpretar este derecho conforme a la Constitución, los tratados internacionales, el principio pro persona y las obligaciones de promover, respetar, proteger y garantizar derechos humanos.

El artículo 6o. constitucional reconoce la información relativa a la privacidad y los datos personales en los términos legales, como un límite al derecho de acceso a la información. Esta disposición es relevante porque vincula acceso a la información, transparencia y límites derivados de la privacidad, tensión que se intensifica cuando la información circula entre autoridades, empresas y plataformas.

El artículo 16 constitucional reconoce el derecho a la protección de datos personales y los derechos de acceso, rectificación, cancelación y oposición. Sin embargo, el reconocimiento formal no garantiza eficacia si la persona no sabe que sus datos fueron tratados, no identifica al responsable o no puede ejercer remedios comprensibles y accesibles.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares regula el tratamiento legítimo, controlado e informado de datos personales en el sector privado. Sus principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad son especialmente relevantes para internet, biometría y servicios que integran tecnologías de captura.[52]

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece bases para autoridades y entes públicos, e incorpora herramientas

[52] *Cfr.* Cámara de Diputados del H. Congreso de la Unión, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México, texto vigente, art. 1, 6,7 y 9.

como privacidad por diseño y por defecto, así como evaluaciones de impacto. Estos mecanismos son centrales para plataformas públicas, sistemas biométricos, identificación estatal y tecnologías de vigilancia.[53]

La Ley General de Transparencia y Acceso a la Información Pública[54] y el Reglamento Interior de Transparencia para el Pueblo[55] forman parte del nuevo contexto institucional. Tras la desaparición del órgano autónomo anterior, el reto es asegurar capacidades técnicas, independencia funcional, recursos suficientes y mecanismos accesibles para proteger privacidad y datos personales.

El contexto mexicano presenta limitaciones recurrentes: formalización excesiva de avisos de privacidad, dependencia débil del consentimiento, fragmentación normativa entre sectores, remedios cotidianos difíciles de activar y vacíos frente a biometría y drones. Una tecnología puede cumplir una regla sectorial y, aun así, producir riesgos no atendidos por esa regulación.

A partir de este diagnóstico, la protección eficaz exige privacidad desde el diseño. La protección no debe añadirse al final como un documento, sino incorporarse desde la arquitectura de sistemas, plataformas, bases de datos, sensores y dispositivos, mediante configuraciones por defecto menos intrusivas, límites de retención, señales claras de captura y mecanismos de control accesibles.

El segundo criterio es minimización de datos. Las tecnologías deben recolectar sólo los datos necesarios para finalidades determinadas. En internet, esto exige limitar rastreo y usos secundarios. En biometría, implica evitar bases masivas cuando existan alternativas menos invasivas. En drones, supone reducir captación incidental y almacenamiento de imágenes no necesarias. La minimización es una regla de coherencia jurídica y técnica: si un dato no se necesita, no debe recolectarse ni tratarse.

También se requiere transparencia significativa: información comprensible, contextual y útil sobre cuándo se rastrea, identifica biométricamente o graba desde un

[53] *Cfr.* Cámara de Diputados del H. Congreso de la Unión, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, México, texto vigente, arts. 1, 2, 24, 70 y 71.
[54] *Cfr.* Cámara de Diputados del H. Congreso de la Unión, Ley General de Transparencia y Acceso a la Información Pública, México, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025, arts. 1o. y 2o.
[55] Reglamento Interior de Transparencia para el Pueblo, Diario Oficial de la Federación, México, 21 de marzo de 2025.

dron, quién es responsable y qué derechos pueden ejercerse. En tecnologías de captura ambiental, los deberes de información deben adaptarse a la situación concreta y no agotarse en avisos extensos.[56]

Las evaluaciones de impacto deben preceder a tecnologías de alto riesgo, como reconocimiento facial, plataformas biométricas, drones de vigilancia o sistemas de perfilamiento. La lógica preventiva de la Recomendación de la UNESCO sobre ética de la inteligencia artificial es trasladable a estas tecnologías: identificar riesgos, grupos afectados, alternativas menos intrusivas y medidas de mitigación antes de implementar.[57]

La proporcionalidad debe operar como criterio de control: toda afectación al derecho a la privacidad requiere finalidad legítima, idoneidad, necesidad y equilibrio.[58] En tecnologías emergentes, esta estructura evita tanto la prohibición general como la permisividad acrítica y obliga a justificar con mayor rigor los tratamientos más intrusivos.[59]

El sexto criterio es protección de terceros no usuarios. Muchas tecnologías afectan a personas que no contrataron, compraron ni aceptaron el sistema: transeúntes captados por drones, visitantes grabados por dispositivos inteligentes, personas identificadas por cámaras biométricas o usuarios perfilados por plataformas que integran datos de terceros. La eficacia del Derecho exige reconocer que la privacidad es relacional y que no todos los afectados son titulares directos de una relación contractual.

El séptimo criterio es trazabilidad y reparación efectiva. Cuando existe una afectación, debe ser posible identificar al responsable, conocer el tratamiento, exigir corrección o eliminación, suspender usos indebidos y obtener reparación. Sin trazabilidad, la privacidad se vuelve un derecho declarativo. La trazabilidad no debe confundirse con vigilancia total; debe entenderse como la capacidad institucional mínima para atribuir responsabilidad cuando una tecnología produce una afectación.

---

[56] *Cfr.* European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data through Video Devices, versión 2.0, Bruselas, 2020, pp. 7-12.
[57] UNESCO, Recomendación sobre la ética de la inteligencia artificial, París, UNESCO, 2021, pp. 16-20.
[58] *Cfr.* Barak, Aharon, Proportionality: Constitutional Rights and Their Limitations, Cambridge, Cambridge University Press, 2012, pp. 131-145.
[59] *Cfr.* Alexy, Robert, Teoría de los derechos fundamentales, Madrid, Centro de Estudios Políticos y Constitucionales, 2007, pp. 91-95.

El octavo criterio es responsabilidad diferenciada. No todos los actores tienen el mismo deber. Quien desarrolla una tecnología debe diseñarla con salvaguardas; quien la implementa debe justificar finalidad y proporcionalidad; quien la opera debe cumplir condiciones de uso; y quien almacena o transfiere datos debe garantizar seguridad y límites. Este reparto es indispensable porque los daños tecnológicos suelen surgir de cadenas de actores y no de una sola decisión individual.

El noveno criterio es supervisión especializada. La autoridad encargada de proteger datos y privacidad debe contar con capacidades técnicas para auditar algoritmos, bases biométricas, plataformas digitales y sistemas de captura audiovisual. La protección de la privacidad ante tecnologías emergentes requiere conocimiento jurídico, pero también comprensión técnica. Sin capacidades institucionales, la norma se vuelve insuficiente.

El décimo criterio es educación y cultura de privacidad y de protección de datos personales. La eficacia del derecho no depende sólo de sanciones; también exige que personas, empresas y autoridades comprendan riesgos. La alfabetización digital debe incluir privacidad, seguridad, datos personales, biometría y vigilancia. Una ciudadanía informada puede exigir mejores prácticas, pero esa exigencia no debe sustituir obligaciones jurídicas de responsables y autoridades.

La doctrina especializada permite reforzar esta conclusión. Lee Bygrave ha explicado que el derecho de protección de datos no sólo se orienta a controlar información, sino a estructurar relaciones de poder entre titulares, responsables y autoridades.[60] Esta lectura es útil para México porque muestra que el problema no termina con reconocer derechos ARCO; también implica distribuir cargas institucionales y técnicas para que el titular no quede solo frente a sistemas complejos.

Mireille Hildebrandt advierte que las tecnologías inteligentes reconfiguran las condiciones de la normatividad porque anticipan, clasifican y orientan conductas en entornos automatizados.[61] Si la regulación no comprende esa dimensión técnica, corre el riesgo de intervenir tarde. En materia de privacidad, esto significa que la protección debe

[60] *Cfr.* Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, La Haya, Kluwer Law International, 2002, pp. 57-63.
[61] *Cfr.* Hildebrandt, Mireille, *Smart Technologies and the End(s) of Law*, Cheltenham, Edward Elgar, 2015, pp. 1-15.

operar antes de que el daño se produzca, mediante diseño, auditoría, documentación y controles de finalidad.

Stefano Rodotà propuso comprender la protección de datos como una dimensión de ciudadanía y dignidad, no sólo como un problema patrimonial o de secreto.[62] En el ámbito mexicano, esta idea se relaciona con los análisis doctrinales sobre el derecho a la privacidad, que lo conciben como presupuesto de autonomía personal y límite frente a poderes públicos y privados.[63] De ahí que internet, biometría y drones deban estudiarse como problemas de privacidad y no sólo como herramientas de eficiencia.

Los Principios actualizados sobre la privacidad y la protección de datos personales del Comité Jurídico Interamericano también ofrecen criterios pertinentes: lealtad, finalidad, proporcionalidad, calidad, seguridad, responsabilidad y derechos de los titulares.[64] Estos estándares pueden orientar la interpretación de leyes mexicanas cuando las tecnologías emergentes generan conflictos no previstos expresamente por el legislador.

Las recomendaciones internacionales sobre inteligencia artificial, aunque no sean el centro de este artículo, son relevantes porque las tecnologías emergentes tienden a integrarse con sistemas automatizados de análisis. La OCDE ha destacado principios de robustez, transparencia, rendición de cuentas y respeto de derechos humanos en sistemas de IA.[65] Esa lógica puede proyectarse sobre internet, biometría y drones cuando incorporan análisis algorítmico, reconocimiento, clasificación o toma de decisiones.[66]

En materia biométrica, la Agencia de Derechos Fundamentales de la Unión Europea ha señalado que el reconocimiento facial en contextos de aplicación de la ley requiere salvaguardas estrictas por sus efectos sobre derechos fundamentales.[67] Aunque ese informe se refiere al entorno europeo, su razonamiento es trasladable: cuanto mayor

[62] *Cfr.* Rodotà, Stefano, La vida y las reglas: entre el derecho y el no derecho, Madrid, Trotta, 2010, pp. 57-66.
[63] *Cfr.* García Ricci, Diego, *El derecho a la privacidad*, México, Tirant lo Blanch, 2020, pp. 21-35.
[64] *Cfr.* Comité Jurídico Interamericano, *Principios actualizados sobre la privacidad y la protección de datos personales*, Washington, OEA, 2021, principios 1 a 6.
[65] *Cfr.* Organización para la Cooperación y el Desarrollo Económicos, *Recommendation of the Council on Artificial Intelligence,* OECD/LEGAL/0449, París, OCDE, adoptada el 22 de mayo de 2019 y modificada el 8 de noviembre de 2024.
[66] *Cfr.* Ibidem.
[67] *Cfr.* Agencia de la Unión Europea para los Derechos Fundamentales, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, Viena, FRA, 2019, pp. 21-28.

sea la capacidad de identificar personas en espacios públicos, mayor debe ser la exigencia de legalidad, necesidad, proporcionalidad y control independiente.

En el caso mexicano, la Plataforma Única de Identidad y la CURP biométrica requieren especial atención porque la Ley General de Población contempla mecanismos de consulta, validación y vinculación de identidad.[68] Los lineamientos de operación de dicha plataforma prevén reglas de desarrollo y gestión institucional, pero la eficacia de la protección dependerá de controles verificables, auditorías, seguridad, límites de acceso y prohibición de usos secundarios no justificados.[69]

Respecto de drones, la NOM-107-SCT3-2019 ofrece una base técnica necesaria para seguridad operacional, pero debe dialogar con reglas de protección de datos, uso de imagen de terceros, responsabilidad civil y vigilancia.[70] La regulación eficaz no debe tratar al dron sólo como aeronave ni sólo como cámara; debe reconocer que su uso puede reunir tránsito aéreo, captación audiovisual y afectación de terceros en un mismo acto.

En suma, México cuenta con una base normativa relevante, pero el reto consiste en convertir derechos reconocidos en protección cotidiana. Internet, biometría y drones muestran afectaciones digitales, corporales y espaciales que requieren articular protección de datos, estándares de derechos humanos, reglas sectoriales y responsabilidad preventiva.

Una regla sintetiza la propuesta: a mayor capacidad tecnológica para rastrear, identificar u observar, mayor debe ser la carga de justificación y responsabilidad. Así puede protegerse la privacidad sin bloquear la innovación, evitando que las personas se conviertan en objetos permanentes de seguimiento, clasificación o vigilancia.

## VIII. Conclusiones.

El derecho a la privacidad y la protección de datos personales no han perdido relevancia ante las tecnologías emergentes; por el contrario, se ha vuelto más importante. Internet, biometría y drones muestran que las afectaciones actuales incluyen rastreo

[68] *Cfr.* Cámara de Diputados del H. Congreso de la Unión, Ley General de Población, cit., arts. 91 Ter a 91 Sexies.
[69] *Cfr.* Secretaría de Gobernación, Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad, cit.
[70] *Cfr.* Secretaría de Comunicaciones y Transportes, Norma Oficial Mexicana NOM-107-SCT3-2019, cit.

digital, perfilamiento, identificación corporal, observación aérea, captura incidental de terceros e inferencias automatizadas.

La selección de los tres casos permitió responder la pregunta central del artículo. Internet expresa la dimensión informacional y relacional; la biometría, la corporal e identitaria; y los drones, la espacial y observacional. En los tres casos, el derecho a la privacidad y a la protección de datos personales se reconfiguran frente a tecnologías capaces de producir información sobre las personas sin control suficiente.

La hipótesis se confirma: el modelo adoptado en la actualidad para la protección de datos basado en consentimiento, aviso de privacidad y derechos ARCO resulta insuficiente frente a tecnologías opacas, persistentes, masivas o capaces de afectar a terceros no usuarios. El consentimiento constituye una piedra angular para el tratamiento de datos personales, pero no puede justificar por sí solo el uso desproporcionado e ilimitado de los datos personales en entornos complejos.

México cuenta con bases constitucionales y legales importantes; sin embargo, el desafío es la eficacia. Las normas deben traducirse en diseño preventivo, minimización, transparencia comprensible, evaluaciones de impacto, proporcionalidad, trazabilidad, protección de terceros, supervisión especializada y reparación efectiva.

La protección del derecho a la privacidad y a la protección de datos personales no deben verse como obstáculos a la innovación, sino como condición de legitimidad democrática de las tecnologías emergentes. Regular internet, biometría y drones no implica prohibirlos, sino establecer condiciones para que su uso no convierta la vida cotidiana en un espacio de rastreo, identificación y vigilancia intrusiva desproporcionada.

La conclusión general es que el derecho a la privacidad y el derecho a la protección de datos personales contemporáneos exigen pasar de una lógica reactiva a una preventiva. El Derecho debe intervenir en el diseño, implementación y supervisión de las tecnologías para que estos derechos dejen de ser una aspiración utópica ante el ideal de horizontalidad y funcionen como garantía efectiva para establecer un modelo de gobernanza respetuoso con la dignidad humana.

## IX. Referencias bibliográficas.

ACQUISTI, Alessandro, TAYLOR, Curtis y WAGMAN, Liad, "The Economics of Privacy", Journal of Economic Literature, Nashville, vol. 54, núm. 2, 2016.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Guía sobre tratamientos de control de presencia mediante sistemas biométricos, Madrid, AEPD, 2023.

AGENCIA DE LA UNIÓN EUROPEA PARA LOS DERECHOS FUNDAMENTALES, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, Viena, FRA, 2019.

ALEXY, Robert, Teoría de los derechos fundamentales, Madrid, Centro de Estudios Políticos y Constitucionales, 2007.

ARIA, Massimo y CUCCURULLO, Corrado, "bibliometrix: An R-tool for Comprehensive Science Mapping Analysis", Journal of Informetrics, Ámsterdam, vol. 11, núm. 4, 2017.

BARAK, Aharon, Proportionality: Constitutional Rights and Their Limitations, Cambridge, Cambridge University Press, 2012.

BUOLAMWINI, Joy y GEBRU, Timnit, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research, vol. 81, 2018.

BYGRAVE, Lee A., Data Protection Law: Approaching Its Rationale, Logic and Limits, La Haya, Kluwer Law International, 2002.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Constitución Política de los Estados Unidos Mexicanos, México, texto vigente.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México, texto vigente.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Ley General de Población, México, texto vigente.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, México, texto vigente.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Ley General de Transparencia y Acceso a la Información Pública, México, texto vigente.

CLARKE, Roger y BENNETT MOSES, Lyria, "The Regulation of Civilian Drones' Impacts on Public Safety", Computer Law & Security Review, Londres, vol. 30, núm. 3, 2014.

COHEN, Julie E., Between Truth and Power: The Legal Constructions of Informational Capitalism, Nueva York, Oxford University Press, 2019.

COMITÉ JURÍDICO INTERAMERICANO, Principios actualizados sobre la privacidad y la protección de datos personales, Washington, OEA, 2021.

CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Escher y otros vs. Brasil, sentencia de 6 de julio de 2009, Fondo, Reparaciones y Costas.

CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, sentencia del 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas.

CUSTERS, Bart (ed.), The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives, Cham, Springer, 2016.

DÍAZ, Marianne, El cuerpo como dato, Santiago de Chile, Derechos Digitales, 2018.

DONTHU, Naveen, KUMAR, Satish, MUKHERJEE, Debmalya, PANDEY, Nitesh y LIM, Weng Marc, "How to Conduct a Bibliometric Analysis: An Overview and Guidelines", Journal of Business Research, Ámsterdam, vol. 133, 2021.

EUROPEAN DATA PROTECTION BOARD, Guidelines 3/2019 on Processing of Personal Data through Video Devices, versión 2.0, Bruselas, 2020.

FINN, Rachel L. y WRIGHT, David, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications", Computer Law & Security Review, Londres, vol. 28, núm. 2, 2012.

GARCÍA RICCI, Diego, El derecho a la privacidad, México, Tirant lo Blanch, 2020.

GIL GONZÁLEZ, Elena, Big data, privacidad y protección de datos, Madrid, Agencia Española de Protección de Datos-Boletín Oficial del Estado, 2016.

HILDEBRANDT, Mireille, Smart Technologies and the End(s) of Law, Cheltenham, Edward Elgar, 2015.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2024, México, INEGI, 2025.

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO, LA PORTABILIDAD DE LOS DATOS PERSONALES ES UN DERECHO QUE SE DEBE GARANTIZAR A TODAS LAS PERSONAS: ESPECIALISTAS, Boletín: DCS/155/2022 Publicado por: Dirección de Comunicación Social / Ciudad de México 03 de agosto de 2022.

INTRONA, Lucas D. y WOOD, David, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", Surveillance & Society, Kingston, vol. 2, núms. 2/3, 2004.

JAIN, Anil K., ROSS, Arun y PRABHAKAR, Salil, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Nueva York, vol. 14, núm. 1, 2004.

LESSIG, Lawrence, Code and Other Laws of Cyberspace, Nueva York, Basic Books, 1999.

NISSENBAUM, Helen, "Privacy as Contextual Integrity", Washington Law Review, Seattle, vol. 79, núm. 1, 2004.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS, The Right to Privacy in the Digital Age, A/HRC/48/31, Ginebra, Naciones Unidas, 2021.

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, Unmanned Aircraft Systems Traffic Management (UTM): A Common Framework with Core Principles for Global Harmonization, Montreal, OACI, 2023.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, Pacto Internacional de Derechos Civiles y Políticos, Nueva York, 1966.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Convención Americana sobre Derechos Humanos, San José, 1969.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, OECD Digital Economy Outlook 2024, vol. 2, París, OECD Publishing, 2024.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, París, OCDE, adoptada el 22 de mayo de 2019 y modificada el 8 de noviembre de 2024.

QUIJANO, Decanini, C., Derecho a la privacidad en Internet, México, Tirant lo Blanch, 2022.

RODOTÀ, Stefano, La vida y las reglas: entre el derecho y el no derecho, Madrid, Trotta, 2010.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, Reglamento General de Protección de Datos, Diario Oficial de la Unión Europea, 27 de abril de 2016.

REGLAMENTO INTERIOR DE TRANSPARENCIA PARA EL PUEBLO, Diario Oficial de la Federación, México, 21 de marzo de 2025.

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, Norma Oficial Mexicana NOM-107-SCT3-2019, que establece los requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano, Diario Oficial de la Federación, México, 14 de noviembre de 2019.

SECRETARÍA DE GOBERNACIÓN, Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad, Diario Oficial de la Federación, México, 27 de noviembre de 2025.

SANTAMARINA-CAMPOS, Virginia y SEGARRA-OÑA, Marival (eds.), Drones and the Creative Industry: Innovative Strategies for European SMEs, Cham, Springer Open, 2018.

SOLOVE, Daniel J., "A Taxonomy of Privacy", University of Pennsylvania Law Review, Philadelphia, vol. 154, 2006.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Acción de inconstitucionalidad 82/2021 y acumulada 86/2021, Pleno.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Amparo directo en revisión 5823/2018, Primera Sala, fragmento público del proyecto de sentencia.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, Digital Rights Ireland Ltd. vs. Minister for Communications, Marine and Natural Resources y otros, asuntos acumulados C-293/12 y C-594/12, sentencia de 8 de abril de 2014.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, František Ryneš vs. Úřad pro ochranu osobních údajů, asunto C-212/13, sentencia de 11 de diciembre de 2014.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González, asunto C-131/12, sentencia de 13 de mayo de 2014.

UNESCO, Recomendación sobre la ética de la inteligencia artificial, París, UNESCO, 2021.

VAN ECK, Nees Jan y WALTMAN, Ludo, "Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping", Scientometrics, Dordrecht, vol. 84, núm. 2, 2010.

VAN DIJCK, José, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology", Surveillance & Society, Kingston, vol. 12, núm. 2, 2014.

WARREN, Samuel D. y BRANDEIS, Louis D., "The Right to Privacy", Harvard Law Review, Cambridge, vol. IV, núm. 5, 1890.

WESTIN, Alan, Privacy and Freedom, Nueva York, Ig Publishing, 2015.

ZUPIC, Ivan y ČATER, Tomaž, "Bibliometric Methods in Management and Organization", Organizational Research Methods, Thousand Oaks, vol. 18, núm. 3, 2015.

ZWICKLE, Adam, FARBER, Hillary B. y HAMM, Joseph A., "Comparing Public Concern and Support for Drone Regulation to the Current Legal Framework", Behavioral Sciences & the Law, 2018.

ZUBOFF, Shoshana, The Age of Surveillance Capitalism, Nueva York, PublicAffairs, 2019.