ISSN 3008-9484 | DOI 10.5281/zenodo.14509465 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 62-82

LA REGULACIÓN DE LA IA: LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD COMO DERECHOS HUMANOS

Regulating AI: Data Protection and Privacy as Human Rights

Rosa Merlín Rodríguez *

Universidad Nacional Autónoma de México
rmerlin@politicas.unam.mx
https://orcid.org/0009-0005-0191-4060

RECIBIDO: 14/10/2024 - ACEPTADO: 11/11/2024

Resumen: La inteligencia artificial tiene un gran potencial para mejorar el acceso a la información, pero también presenta riesgos significativos que requieren una regulación adecuada para su uso ético. La responsabilidad de asegurar un uso ético de la IA recae tanto en los Estados, que deben crear marcos legales adecuados, como en las empresas, que deben priorizar los derechos humanos. Es esencial gestionar eficazmente los datos personales para prevenir abusos. Por lo tanto, tanto los Estados como otros actores deben garantizar la privacidad y la no discriminación, implementando regulaciones que protejan los derechos humanos. Este artículo sugiere que adoptar un enfoque que integre los derechos humanos en el desarrollo de la IA promoverá un ecosistema tecnológico más responsable y sostenible.

Palabras clave: inteligencia artificial, derechos humanos: protección de datos, privacidad, regulaciones.

Abstract: Artificial intelligence has great potential to improve access to information, but it also presents significant risks that require adequate regulation for its ethical use. The responsibility for ensuring the ethical use of AI lies with both states, which must create appropriate legal frameworks, and companies, which must prioritize human rights. It is essential to effectively manage personal data to prevent abuse. Therefore, both states and other actors must ensure privacy and nondiscrimination by implementing regulations that protect human rights. This article suggests that adopting an approach that integrates human rights into the development of AI will promote a more responsible and sustainable technological ecosystem.

Keywords: artificial intelligence, human rights, data protection, privacy, regulations.

En un entorno globalizado e interconectado, la utilización masiva de datos que se gestionan desde aplicaciones electrónicas, plataformas en la nube, dispositivos del Internet de las Cosas y la inteligencia artificial (IA) presentan desafíos significativos en la regulación y manejo de la información. Aunque la IA tiene un gran potencial para resolver diversos problemas, su utilización sin principios éticos bien definidos puede representar riesgos importantes para los derechos humanos.

* Lic. en Derecho (Universidad Nacional Autónoma de México), Doctora en Derecho y Gobernanza Global (Universidad de Salamanca). Académica de la Facultad de Ciencias Políticas y Sociales de la UNAM.

> Las nuevas tecnologías generativas son una paradoja del progreso que pueden brindar soluciones a situaciones complejas pero que conllevan un alto riesgo de socavar la dignidad y las garantías fundamentales, advierte el responsable de velar por esos derechos, abogando por regulaciones que también promuevan conductas empresariales responsables y rendición de cuentas (Naciones Unidas, 2023).

En respuesta a esto, organizaciones internacionales como las Naciones Unidas, el Consejo de Europa y la Unión Europea están trabajando en marcos normativos para reducir estos riesgos. Un avance clave ha sido la "Recomendación sobre la Ética de la IA" (2021) de la Organización de las Naciones Unidas para la Educación la Ciencia y la Cultura (UNESCO), que establece pautas éticas aplicables en todas las fases del desarrollo de la IA. No obstante, aunque las resoluciones recientes del Consejo de Derechos Humanos de la ONU destacan riesgos importantes, aún faltan medidas concretas para prohibir o regular aquellas aplicaciones de IA que no cumplan con los estándares de derechos humanos. Esto resalta la urgencia de incorporar los derechos humanos en cada etapa del proceso de la IA, a través de mecanismos de gestión de riesgos efectivos impulsados por gobiernos y empresas.

El respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y la dignidad humana son esenciales en todo el ciclo de vida de los sistemas de IA. La dignidad inviolable de cada persona, independientemente de su raza, género, religión o condición social, es la base de los derechos humanos. Ningún ser humano o comunidad debe sufrir daños por el uso de IA, y estos sistemas deben mejorar la calidad de vida sin vulnerar los derechos o la dignidad. Además, en las interacciones con la IA, especialmente con personas vulnerables, su dignidad y derechos deben ser siempre respetados (UNESCO, 2021, p.18).

El uso indebido de la IA puede poner en riesgo derechos fundamentales como la libertad de expresión, la privacidad, la igualdad y la protección de datos. La IA presenta desafíos como oportunidades en el ámbito de los derechos humanos, lo que ha motivado su inclusión en diversas propuestas regulatorias internacionales. Es fundamental que el reconocimiento de los riesgos éticos y preocupaciones asociados con esta no frene la innovación. En lugar de ello, se debe fomentar una investigación responsable que no solo impulse el desarrollo tecnológico, sino que también garantice que este avance esté alineado con los derechos humanos, las libertades fundamentales y los principios éticos.

La UNESCO (2021, p. 5) subraya que la IA debe ser desarrollada y aplicada de forma que respete y promueva la dignidad humana, la privacidad, la igualdad y otros derechos. No se trata solo de identificar los riesgos, sino de convertir esas preocupaciones en oportunidades para garantizar que ésta mejore la vida de las personas sin violar sus derechos. Esta visión ética no solo puede proteger los derechos funda-

mentales, sino también abrir nuevas posibilidades para crear tecnologías más inclusivas, responsables y seguras.

Así, la clave radica en encontrar un equilibrio en el desarrollo de la IA y el respeto de los derechos humanos, fomentando un ecosistema tecnológico que priorice la dignidad y los valores éticos. Esto a fin de que la innovación genere un impacto positivo y duradero. No obstante, uno de los principales desafíos es definir con precisión lo que significa aplicar un enfoque de derechos humanos en este contexto. Este estudio busca arrojar luz sobre esa cuestión, subrayando el rol fundamental de los Estados en la creación de marcos legales y normativos para los sistemas de IA que promuevan la responsabilidad de las empresas.

El objetivo de este artículo es revisar las implicaciones de la IA y su regulación en el contexto de la privacidad y la protección de datos personales. Uno de los puntos más preocupantes es el uso de sistemas de IA que gestionan datos personales, ya que esto puede acarrear riesgos significativos, como el tratamiento inadecuado de la información y fallos de seguridad. Estas preocupaciones pueden afectar derechos fundamentales, incluidos el derecho a la vida, la no discriminación, la salud y la privacidad.

Los Estados tienen la capacidad de establecer normativas y políticas para regular el uso y acceso a tecnologías digitales y datos en línea, ajustándolas según sus intereses y valores nacionales: "Es necesario que las nuevas tecnologías proporcionen nuevos medios para promover, defender y ejercer los derechos humanos, y no para vulnerarlos" (UNESCO, 2021, p. 19).

A pesar de que existen marcos normativos tanto a nivel local como internacional para proteger los datos personales, el desafío principal radica en la necesidad de desarrollar mecanismos eficaces que aseguren la protección de los derechos humanos. Es crucial evaluar si el marco legal actual es suficiente para equilibrar la innovación tecnológica con la dignidad humana. Este análisis no solo busca identificar las limitaciones de la regulación existente, sino también proponer estrategias que integren los derechos humanos en el desarrollo de tecnologías de IA, fomentando un enfoque que priorice la seguridad y la ética en la gestión de datos personales.

En consecuencia, en la primera parte de este artículo se aborda la IA desde un punto de vista jurídico. En la segunda, se analizan los precedentes más notables de regulación de la IA. La tercera parte profundiza en aspectos fundamentales como son la protección de datos y la privacidad entendidas como derechos humanos. En la cuarta parte se desarrollan estas cuestiones desde el caso mexicano, repasando las leyes introducidas en los últimos años en materia de protección de datos, incluyendo la creación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). A pesar de estos avances, existen aún en México desafíos importantes. Este trabajo sugiere en las reflexiones finales la nece-

sidad de implementar un modelo de gobernanza coordinado con actores internacionales a fin de establecer un ecosistema digital más seguro y confiable para todas las personas.

I - LA IA: SU COMPRENSIÓN JURÍDICA

La comprensión jurídica de la IA está íntimamente relacionada con los desafíos éticos, sociales y técnicos que plantea su desarrollo. La IA ha permitido la automatización de decisiones en diversos ámbitos, lo que ofrece enormes oportunidades para mejorar servicios e industrias. Sin embargo, también genera importantes interrogantes sobre la responsabilidad, la ética y los derechos humanos. Cabe señalar que la IA no es de aparición reciente; sus orígenes se remontan a los años cincuenta cuando Alan Turing sentó las bases teóricas, y posteriormente se crearon los primeros programas "inteligentes", capaces de resolver problemas.

En los últimos veinte años, la IA, y más específicamente el aprendizaje automático, ha sido esencial en tecnologías digitales como los motores de búsqueda, los algoritmos de recomendación, los drones, los vehículos autónomos y los sistemas de reconocimiento facial. A medida que nuevas formas de IA generativa como *chatbots* y generadores de imágenes avanzados han ganado popularidad, han resurgido antiguos debates y surgido nuevos. Estos modelos tienen el potencial de generar cambios sociales significativos, superando a otras tecnologías de IA debido a su versatilidad, accesibilidad y capacidad para transformar sectores enteros. Sin embargo, también han provocado tanto entusiasmo como preocupación (De Souza Dias y Sagoo, 2024).

Woods (2023) define la inteligencia artificial como el uso de computadoras para tomar decisiones racionales que podrían haber sido tomadas por seres humanos. Mientras que, para De Souza Dias y Sagoo (2024), la IA es una tecnología global que trasciende fronteras y afecta significativamente tanto la vida individual como el tejido social a nivel mundial, influyendo en áreas como la calificación crediticia, las redes sociales, el desarrollo de armamento y la configuración del entorno informativo global.

Dado el avance de la IA, es fundamental contar con plataformas en la nube que permitan entornos separados para desarrollar y entrenar modelos de IA, garantizando al mismo tiempo la seguridad, el cumplimiento normativo y un rendimiento eficiente, incluso en momentos de alta demanda (Juri, 2023).

En este contexto, los derechos digitales adquieren una relevancia crítica. Los derechos humanos, especialmente en lo que respecta a la privacidad y la protección de datos, deben constituir el eje de cualquier regulación relacionada con la IA. Europa, a través del Reglamento General de Protección de Datos (RGPD), ha liderado es-

ta protección, destacando la importancia de equilibrar el progreso tecnológico con la protección de los derechos individuales.

La propuesta de incorporar los derechos digitales en constituciones nacionales, como sugiere Barrio (2023) para España, refuerza la idea de que estos derechos en el entorno digital son una extensión natural de los derechos humanos tradicionales. Sin embargo, sigue siendo un reto crear un marco normativo flexible y robusto que se mantenga al ritmo del avance tecnológico. Este desafío es especialmente notable a nivel global, donde el acceso y uso de la tecnología varía considerablemente entre países, lo que dificulta la creación de normas universales.

II – REGULACIÓN DE LA IA

La convergencia entre la IA y la protección de datos plantea un reto significativo, dado el delicado equilibrio entre el avance tecnológico y las exigencias regulatorias. Si bien la IA puede revolucionar diversas industrias y elevar el bienestar social, su uso a gran escala conlleva riesgos importantes para la privacidad y los derechos humanos. Para asegurar un desarrollo ético y sostenible, es imprescindible mantener un balance entre la innovación y la salvaguarda de los datos, lo que requiere la implementación de un marco normativo robusto que fomente el progreso sin comprometer los derechos individuales.

La transformación digital ha impactado profundamente los principios de la regulación jurídica, incluyendo los derechos humanos (Bieliakov *et al.,* 2023). Aunque la noción de "derechos humanos digitales" no es nueva en Europa, está ganando reconocimiento tanto nacional como internacional. Estos derechos, centrados en las libertades y derechos en internet, han sido respaldados por documentos como la "Resolución sobre la promoción, protección y realización de los derechos humanos en internet".[1]

Si bien los derechos digitales están emergiendo como una extensión natural de los derechos humanos establecidos en la Declaración Universal de Derechos Humanos, su reconocimiento global aún está en una etapa inicial y enfrenta varios desafíos como la rápida transformación de la tecnología que presenta dificultades para desarrollar normas claras y adaptables frente a los cambios constantes. Las diferencias en el acceso y uso de la tecnología entre países y grupos sociales complican la implementación universal de los derechos digitales y, a su vez, los derechos digi-

---

1 *Cf*. "Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo", Consejo de Derechos Humanos, Asamblea General de Naciones Unidas, 38º período de sesiones, 18 de junio a 6 de julio de 2018, disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_des/A_HRC_38_L10.pdf

tales pueden entrar en conflicto con otros derechos fundamentales como la libertad de expresión.

La convergencia entre la IA y leyes estrictas de privacidad, como el RGPD y marcos similares a nivel global, subraya la urgencia de desarrollar estrategias integrales y adaptativas para abordar estos desafíos de manera efectiva. Esto con el fin de salvaguardar los derechos de privacidad individual mientras permiten el progreso tecnológico. Con la proliferación de aplicaciones de IA en áreas como la atención médica personalizada y los sistemas de conducción autónoma, es fundamental integrar de manera efectiva los principios de protección de datos en todas las etapas del desarrollo de la IA (Yanamala y Suryadevara, 2023, p. 295).

La Unión Europea ha liderado la regulación de los derechos digitales con normativas como el RGPD, la cual ha experimentado diversas modificaciones, reflejadas en la actualización de la Ley Orgánica de Protección de Datos (LOPD), que ahora es la Ley Orgánica 3/2018. Esta ley busca la protección de los derechos digitales y autores como Barrio (2023) proponen una futura reforma constitucional para incluir estos derechos, por ejemplo, en la Constitución Española.

El activismo del Tribunal de Justicia de la UE, impulsado por la implementación de la Carta de los Derechos Fundamentales de la UE, fue clave para establecer un enfoque centrado en las personas y en la protección de sus derechos y libertades fundamentales en el ámbito digital. Este proceso normativo sigue en desarrollo bajo la actual Comisión Europea, que ha propuesto diversas iniciativas legales para crear un marco regulador más coherente y unificado. Sin embargo, aunque se priorizan los derechos individuales, estos esfuerzos presentan inconsistencias y ambigüedades que deben resolverse si la UE quiere lograr un marco jurídico común que asegure un entorno digital seguro, transparente y democrático (Pérez de las Heras, 2022).

La UE ha sido proactiva en la regulación de tecnologías digitales basada en valores y principios de derechos humanos y democracia. Desde el inicio ha abordado las implicaciones sociales y éticas de estas tecnologías, especialmente en cuanto a privacidad y seguridad.

Como parte de esta estrategia, se han aprobado directivas y reglamentos que impactan en el uso del mercado digital europeo y han surgido nuevos bienes jurídicos protegidos por la revolución digital. En una década, la Comisión Europea y el Parlamento han emitido más de 30 normativas que afectan las operaciones comerciales en línea (Hidalgo, 2020).

La estrategia digital europea que incorpora como uno de sus ejes clave a la Ley de Servicios Digitales y la Ley de Mercados Digitales. La Ley de Servicios Digitales se enfoca en garantizar un entorno digital más seguro para usuarios y empresas, protegiendo los derechos fundamentales en línea. Los principales temas que aborda incluyen la lucha contra el comercio e intercambio de bienes, servicios y conte-

nidos ilegales en la web, así como el control de los sistemas algorítmicos que facilitan la difusión de desinformación[2].

La segunda, define criterios para reconocer a las grandes plataformas en línea como "guardianes de acceso", centrándose en su influencia sistémica. Entre sus beneficios se encuentran la creación de un entorno más justo para las empresas que dependen de estas plataformas, la apertura de nuevas oportunidades para emprendedores y empresas tecnológicas emergentes, una mayor variedad de servicios y opciones para los consumidores, así como precios más competitivos. Aunque los guardianes de acceso podrán continuar innovando, no podrán emplear prácticas injustas que afecten a las empresas y usuarios que dependen de ellos[3].

El mercado único digital busca suprimir las barreras nacionales en las transacciones electrónicas, fundamentado en el principio del mercado común que favorece el libre movimiento de mercancías, personas, servicios y capitales en la Unión Europea. La Estrategia Europa 2020 subrayó el papel esencial de las tecnologías de la información y la comunicación (TIC) para alcanzar los objetivos de la Unión. Asimismo, el mercado único digital se considera una prioridad central en la Agenda para Europa 2019-2024, impulsada por la presidencia de la Comisión[4].

La creación de un mercado único digital en Europa ha promovido la armonización de normas y el desarrollo de una legislación integral para el comercio electrónico y los servicios digitales.

También la Agenda Digital para Europa de 2010 subrayó la importancia de las TIC para cumplir los objetivos de la Unión. En 2015, la Estrategia para el Mercado Único Digital impulsó el acceso a bienes y servicios digitales, el desarrollo de redes eficientes y el fortalecimiento de la economía digital. La estrategia de 2020 se enfocó en tecnologías que beneficien a las personas y fomenten una sociedad competitiva y democrática. En 2021, la Brújula Digital fijó objetivos en competencias, gobierno, empresas e infraestructuras digitales para el año 2030.

Es así que la Agenda Digital para Europa 2020-2030 busca fortalecer la soberanía digital y asegurar un entorno digital seguro, competitivo y sostenible. Basada en el Tratado de Funcionamiento de la Unión Europea (TFUE), la agenda se enfoca en

---

2 *Cf.* Reglamento de Ejecución (UE) 2023/1201 de la Comisión de 21 de junio de 2023 relativo a las disposiciones detalladas para la tramitación de determinados procedimientos por parte de la Comisión con arreglo al Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo: Ley de Servicios Digitales, DOUE. núm. 159, de 22 de junio de 2023, Recuperada de: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80876

3 *Cf.* Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales), DOUE, núm. 265, de 12 de octubre de 2022, Recuperada de: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81470

4 *Cf.* Base jurídica de La ubicuidad del mercado único digital, Parlamento Europeo, Recuperada de: https://www.europarl.europa.eu/factsheets/es/street/43/la-ubicuidad-del-mercado-unico-digital

empoderar a ciudadanos y empresas, fomentar el crecimiento digital y asegurar el cumplimiento de principios éticos en las tecnologías emergentes, como la IA, entre los cuales destacan los siguientes logros (Petit, Wala, *et. al*, 2024):

1. *Conectividad y telecomunicaciones*: se han eliminado los costos de itinerancia, mejorado la conectividad de banda ancha y reforzado la protección de datos y ciberseguridad. Esto garantiza un acceso equitativo a servicios digitales.
2. *Competitividad digital*: se adoptaron normativas como el Reglamento de Servicios Digitales y el Reglamento de Mercados Digitales, que promueven la competencia leal y definen responsabilidades claras para las plataformas en línea, especialmente en lo que respecta a la eliminación de contenidos dañinos.
3. *Inteligencia Artificial*: La Ley de Inteligencia Artificial de 2024 regula su uso, limitando la biometría y prohibiendo prácticas abusivas como la puntuación ciudadana. También se presentó una directiva para asegurar la responsabilidad civil en el uso de IA.
4. *Transformación empresarial y educativa*: Europa pretende que el 80% de los adultos adquiera competencias digitales básicas, aumentando la contratación de especialistas en TIC y promoviendo el uso de IA, la computación en la nube y los macrodatos en empresas.
5. *Infraestructura y tecnologías emergentes*: se promueve la conectividad 5G, el desarrollo de semiconductores y la creación de supercomputadoras, con una inversión significativa a través del Programa Europa Digital (7.500 millones EUR) para proyectos de IA, ciberseguridad y competencias digitales.
6. *Protección de datos y privacidad*: El RGPD sigue siendo un pilar en la protección de la privacidad, mientras que nuevas normativas sobre el uso de datos no personales buscan equilibrar la innovación con la seguridad.
7. *Servicios públicos digitales*: se impulsa la administración electrónica y la interoperabilidad de servicios públicos, con iniciativas para garantizar el acceso en línea a servicios esenciales y establecer un marco de identidad digital europea.

En conjunto, esta agenda refuerza la posición de Europa como líder en la gobernanza digital global, promoviendo la innovación tecnológica, la sostenibilidad y los derechos de los ciudadanos.

El pasado 13 de marzo de 2024, el Parlamento de la Unión Europea aprobó el Reglamento de Inteligencia Artificial (RIA), diseñado para proteger los derechos fundamentales y la seguridad, al tiempo que fomenta la innovación. Este reglamento busca establecer un marco jurídico uniforme para el desarrollo, comercialización y uso de sistemas de IA en la Unión, promoviendo una IA centrada en el ser humano, confiable y alineada con los valores de la UE.

El reglamento también garantiza la libre circulación de productos y servicios basados en IA, clasifica los sistemas según su nivel de riesgo e impone obligaciones para operadores dentro y fuera de la UE. Excluye sistemas de IA con fines militares o de seguridad nacional (Parlamento Europeo, 2024b).

Es indudable que el marco normativo de la UE tiene como objetivo fomentar una IA ética, orientada hacia el ser humano y fiable. Al crear un marco jurídico coherente, se garantiza que los sistemas de IA funcionen de manera responsable, en concordancia con los valores democráticos, evitando la fragmentación entre los Estados miembros y asegurando la libre circulación de productos y servicios.

Este reglamento clasifica los sistemas de IA de acuerdo con su nivel de riesgo y prohíbe ciertas prácticas que podrían comprometer la privacidad y los derechos fundamentales, resaltando la importancia de una regulación dinámica que fomente la innovación sin poner en peligro la protección de datos. La exclusión de sistemas de IA destinados a fines militares pone de manifiesto la complejidad que conlleva la regulación en este ámbito, mientras que la adopción de este reglamento establece un precedente que puede servir de modelo a seguir a nivel global en la intersección de la tecnología y los derechos humanos.

Sin embargo, Rafael de Asís Roig (2024, p. 28) identifica cuatro problemas clave en la intersección entre derechos y tecnologías emergentes, con un enfoque particular en la IA: en primer lugar, se plantea la nueva ética, cuestionando si el discurso de los derechos es realmente adecuado para enfrentar los retos tecnológicos, aunque no se pone en duda su universalidad. Segundo, se menciona la insuficiencia del discurso, destacando que el marco actual de derechos podría no ser suficiente para abordar los desafíos que presentan las nuevas tecnologías, lo que resalta la necesidad de establecer nuevos derechos, como los digitales y los "neuroderechos". Tercero, enfatiza la prioridad de la ética, argumentando que esta debe guiar las discusiones sobre derechos y tecnología. Finalmente, se observa la ausencia de un enfoque de derechos en la regulación tecnológica, subrayando la importancia de integrar la perspectiva de derechos humanos en las políticas relacionadas. Por lo que es fundamental revisar y ampliar el marco de derechos existentes, especialmente en el ámbito de los derechos digitales.

El Consejo de Derechos Humanos, en la resolución A/HRC/20/L.13[5], afirma que los derechos de las personas deben protegerse también en internet, destacando la necesidad de garantizar los mismos derechos que en el mundo *offline*. En especial, subraya la libertad de expresión y el acceso a la información, asegurando que internet siga siendo un espacio abierto y seguro para el ejercicio de los derechos humanos a nivel global.

---

5 A/HRC/20/L.13, "Promoción, protección y disfrute de los derechos humanos en Internet", Consejo de Derechos Humanos 20º período de sesiones, 29 de junio de 2012, Recuperado de: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_hrc_20_L13.pdf

III – LA PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD FRENTE A LA IA

El derecho a la privacidad es esencial para el ejercicio de los derechos humanos en ambos ámbitos, físico y digital. Este derecho constituye un pilar fundamental de las sociedades democráticas y es crucial para el ejercicio de libertades como la expresión, la asociación y reunión, así como para el acceso a derechos económicos y sociales. Su violación puede tener efectos desproporcionados en ciertos grupos, intensificando la desigualdad y la discriminación (ACNUDH, 2024).

El artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos prohíben las injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia, así como ataques al honor y la reputación de las personas. Ambos instrumentos garantizan el derecho a la protección legal contra tales injerencias. Aunque el derecho a la privacidad no es absoluto en el marco de los derechos humanos internacionales, cualquier intervención debe estar justificada por la ley y someterse a un examen riguroso de necesidad y proporcionalidad.

Si bien la privacidad es un elemento fundamental de la dignidad humana y requiere protección legal, el derecho a la privacidad se centra en la capacidad de una persona para mantener ciertos aspectos de su vida alejados del escrutinio público.

La privacidad se define como el aspecto más íntimo de la vida de una persona, incluyendo sus sentimientos, pensamientos, emociones, vida familiar y relaciones personales. El derecho a la privacidad capacita a los individuos para decidir sobre su espacio privado y regular la intromisión de terceros, incluidos los Estados, permitiendo así la distinción entre lo que debe ser público y lo que debe permanecer privado. Sin embargo, estos conceptos han evolucionado debido al avance tecnológico, que ha permitido una mayor exposición de aspectos que antes se consideraban exclusivamente privados. En este contexto, es crucial reflexionar sobre la importancia de preservar la privacidad, especialmente en la era de la IA (Mendoza, 2022).

Se debe tener presente que la falta de una adecuada protección de la privacidad en la era de la IA puede afectar la democracia y la libertad individual, así como amenazar libertades personales y minar la confianza en las instituciones. La IA facilita la recolección masiva de datos, lo que permite el acceso a aspectos íntimos de la vida de las personas y plantea dilemas éticos sobre su uso. Sin olvidar que el papel de las empresas tecnológicas en la economía digital puede poner en riesgo el papel de los Estados en la protección de derechos fundamentales.

De tal forma que la protección de la privacidad en la era de la IA es fundamental por varias razones: en primer lugar, porque la privacidad es crucial para la preservación de la democracia y la libertad; en segundo lugar, porque las tecnologías modernas permiten la recolección y procesamiento masivo de datos en tiempo real, lo que

revela aspectos íntimos de las personas; y en tercer lugar, porque el creciente poder de las corporaciones en la economía digital puede reducir el rol de los Estados en la salvaguarda de derechos fundamentales, como la privacidad (Mendoza, 2022).

Por ello, es vital establecer marcos regulatorios sólidos que garanticen la privacidad como un derecho inviolable y salvaguarden el bienestar humano ante los intereses comerciales.

La protección de datos personales es crucial en un entorno en el que los sistemas de IA son capaces de recolectar y procesar grandes cantidades de información. Como se ha mencionado anteriormente, el artículo 12 de la Declaración Universal de Derechos Humanos reconoce el derecho a la no injerencia en la vida privada, lo cual establece un fundamento esencial para la evolución de las normativas y la inclusión de diversas figuras jurídicas que defienden la privacidad.

Las crecientes inquietudes sobre el uso de la IA destacan la necesidad de establecer regulaciones efectivas que protejan la privacidad de los individuos. La presencia de algoritmos sesgados y sistemas de vigilancia inapropiados representa importantes desafíos, ya que pueden amenazar la integridad de la información personal y violar los derechos de las personas. Por lo tanto, es fundamental crear marcos regulatorios que aseguren no solo la protección de los datos personales, sino también la justicia y la transparencia en la aplicación de tecnologías emergentes.

La protección de datos personales y la privacidad son temas críticos que requieren atención a nivel internacional, especialmente en el contexto de la IA. Las resoluciones adoptadas en diversas conferencias internacionales resaltan la importancia de establecer un marco normativo que garantice estos derechos como parte integral de los derechos humanos. Esta necesidad se hace evidente en diferentes foros, donde se ha discutido la urgencia de contar con regulaciones efectivas para salvaguardar la privacidad en un mundo cada vez más digitalizado.

La 27ª Conferencia en Montreux enfatizó la necesidad de que los derechos a la protección de datos y la privacidad sean reconocidos como derechos humanos exigibles a través de un instrumento jurídicamente vinculante por parte de la ONU. Esta declaración es fundamental, ya que establece un precedente que impulsa a los países a adoptar legislaciones que garanticen estos derechos. Asimismo, la 28ª Conferencia en Montreal instó a mejorar la cooperación internacional en la protección de datos y la privacidad, subrayando que un enfoque global es esencial para abordar los desafíos que plantea un mundo interconectado (OEA, 2013).

En cuanto a la necesidad de establecer estándares comunes, la 30ª Conferencia en Estrasburgo y la 31ª Conferencia en Madrid adoptaron estándares internacionales sobre protección de datos y privacidad. Estas normas son cruciales para guiar el tratamiento de la información personal, asegurando que se respeten los derechos de los individuos en diversos contextos. Además, la 32ª Conferencia en Jerusalén

instó a los gobiernos a desarrollar una convención internacional vinculante, lo que resalta la importancia de contar con un marco legal sólido que proteja los derechos de privacidad y datos personales en un entorno digital sin fronteras (OEA, 2013).

Finalmente, la 35ª Conferencia Internacional reafirmó la necesidad de un enfoque equilibrado que no solo proteja los derechos humanos, sino que también mejore la transparencia en el procesamiento de datos. Esta transparencia es vital para asegurar la integridad de las redes y evitar comprometer la libertad de expresión y los intereses económicos. En conjunto, estas conferencias reflejan un consenso creciente sobre la importancia de proteger la privacidad y los datos personales en la era de la IA (OEA, 2013).

En consecuencia, es necesaria la creación de estándares normativos globales que funcionen como leyes modelo e incentiven la cooperación entre países en un contexto de transacciones y flujos de datos internacionales, donde se privilegie el respeto a los derechos humanos.

IV - LA PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD EN MÉXICO

Los datos personales se comparan con el "nuevo petróleo" de la era de la información, debido a su potencial para generar valor económico en una época donde la información es un recurso clave. Los datos personales se definen como cualquier información que puede identificar o hacer identificable a una persona física, y son fundamentales para definir la identidad, la privacidad y la seguridad de los individuos (INAI, s.f.). En un mundo cada vez interconectado por internet donde la digitalización y las plataformas electrónicas son fundamentales, la gestión y protección de estos datos se vuelve esencial para preservar la dignidad y la seguridad de las personas.

Esto subraya la relevancia de salvaguardar y administrar de forma adecuada los datos personales, ya que su uso conlleva repercusiones tanto económicas como éticas, siendo esencial para el crecimiento de la economía digital. Actualmente, los datos personales cuentan con un valor económico, equiparable a ciertos activos intangibles, tales como el *software* o el valor comercial de los nombres de dominio. Esto ha llevado a considerarlos como el petróleo de la sociedad de la información y del conocimiento (Mendoza, 2022, p.269).

Los derechos a la protección de datos personales y a la privacidad son dos derechos humanos reconocidos por la Constitución Política de los Estados Unidos Mexicanos. El primero está destinado a salvaguardar el control que las personas tienen sobre el uso de sus datos personales, mientras que el segundo busca proteger su privacidad o vida privada. A estos derechos se añade el derecho al secreto de las comunicaciones, ya que, con frecuencia, los usuarios de redes sociales y otros servi-

cios digitales se conectan mediante plataformas de mensajería electrónica, correo electrónico u otros servicios disponibles para su uso (Recio Gayo, 2022, p.19).

La protección de datos personales en México ha avanzado a través de diversas reformas legislativas. En 2002, la Ley Federal de Transparencia introdujo principios sobre la protección de datos en el ámbito gubernamental. En 2009, una enmienda constitucional reconoció la protección de datos personales como un derecho fundamental, lo que llevó a la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010 y su reglamento en 2011. En 2014, se creó el INAI, el cual supervisa el cumplimiento de estas leyes, imponiendo sanciones cuando se violan los derechos de los titulares de datos. Posteriormente, en 2017, la Ley General de Protección de Datos Personales en Posesión de Entidades Gubernamentales reguló el manejo de datos por parte de autoridades gubernamentales.

Esta normativa exige el respeto a los principios legales e internacionales, garantizando una protección integral de los datos personales en todos los contextos, fortaleciendo el derecho a la privacidad en el entorno digital. Como se puede observar, México ha creado un robusto marco legal para proteger los datos personales, asegurado por el artículo 16, segundo párrafo de la Constitución:

> 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 (Cámara de Diputados, 2024a).

Así, se establecen normas para la recolección, uso, almacenamiento, divulgación y transferencia de datos personales, con el objetivo de asegurar tanto la privacidad como la autodeterminación de los individuos (Morales y Flores, 2023, p.210).

Estas normas se rigen a través de los principios ARCO (Acceso, Rectificación, Cancelación y Oposición) que permiten a las personas controlar el uso de sus datos personales en posesión de entidades públicas a nivel federal, estatal o municipal. El término ARCO corresponde a las siglas que identifican cada uno de estos derechos ejercibles por el titular:

1. *Derecho de Acceso*: Cada persona tiene el derecho de solicitar y obtener información sobre los datos personales que están en poder de una entidad. Esto incluye conocer qué datos se tienen, cómo se utilizan y con qué fines.
2. *Derecho de Rectificación*: Las personas pueden pedir que se corrijan o modifiquen datos personales que sean incorrectos, incompletos o desactualizados. Este derecho asegura que la información sobre una persona sea precisa y actual.

3. *Derecho de Cancelación*: Los individuos tienen la facultad de solicitar la eliminación de sus datos personales de una base de datos. Este derecho permite que la información sea suprimida cuando ya no sea necesaria para los fines para los que fue recolectada.

4. *Derecho de Oposición*: Las personas pueden oponerse al tratamiento de sus datos personales en ciertos casos, especialmente cuando se considera que el tratamiento no es legítimo o que afecta negativamente a sus derechos. Esto puede incluir la oposición a la utilización de datos para fines específicos, como marketing.

El ejercicio de los derechos ARCO es exclusivo del titular de los datos, su representante legal o un representante autorizado, y debe realizarse mediante procedimientos gratuitos ofrecidos por la entidad pública correspondiente. Estos derechos se enfocan en proteger los datos personales cuyo tratamiento ha sido autorizado por el titular, a diferencia del derecho al olvido, que abarca cualquier información personal, aunque con restricciones, especialmente cuando entra en conflicto con otros derechos, como la libertad de expresión.

En cuanto a la posibilidad de que organizaciones sin fines de lucro presenten recursos en nombre de los titulares de datos o busquen una reparación colectiva, la ley no contempla esta opción. Solo los titulares de los datos o sus representantes legales pueden buscar reparaciones por infracciones (Data Protection Laws and Regulations Mexico, 2024).

La protección de los datos personales está estrechamente relacionada con el derecho a la privacidad, el cual es reconocido en el artículo 16 de la Constitución mexicana en los párrafos 1 y 12, en donde no está permitido intromisiones en la vida de las personas, en su familia, domicilios o documentos, tampoco en sus comunicaciones privadas, a menos que sea requerido por autoridad competente conforme a la ley:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley (Cámara de Diputados, 1917).

El derecho a la privacidad en México revela un marco legal en constante evolución, adaptado para enfrentar los desafíos de la era digital. La Ley Federal de Protección de Datos Personales en Posesión de Particulares establece principios clave

como legalidad, consentimiento, información, calidad y seguridad para la gestión de datos personales por entidades privadas, protegiendo así la privacidad individual y garantizando un manejo adecuado de la información. Complementando esta ley, la Ley General de Protección de Datos Personales en Posesión de Entidades Gubernamentales extiende estos principios al sector público, asegurando una protección uniforme a nivel nacional. Además, a través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) antes IFAI[6], en cuya reforma constitucional de 2014 se le dota de autonomía constitucional con el objetivo de crear un sistema de coordinación entre la federación y las entidades federativas (Carreón, 2023, p.150); juega un papel esencial en la supervisión y aplicación de estas leyes, promoviendo la cultura de protección de datos y resolviendo reclamaciones para mantener los derechos digitales robustos y efectivos.

Varios instrumentos internacionales abordan los derechos vinculados a la privacidad entre los que se destacan el artículo 12 de la Declaración Universal de Derechos Humanos de 1948, el artículo 11 de la Convención Americana de Derechos Humanos de 1966, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos 1966, el artículo 8 del Convenio Europeo de Derechos Humanos 1950, y la Carta de los Derechos Fundamentales de la Unión Europea 2000.

Cuadro A.
Instrumentos internacionales relacionados con la privacidad

Instrumento Internacional	Artículo Relacionado
Declaración Universal de los Derechos Humanos	Artículo 12: protege la privacidad contra injerencias arbitrarias.
Pacto Internacional de Derechos Civiles y Políticos	Artículo 17: protege la privacidad y la correspondencia contra injerencias arbitrarias.
Convención Americana de Derechos Humanos	Artículo 11: garantiza la protección de la vida privada y la honra personal.
Convenios de la OIT sobre derechos fundamentales de los trabajadores	Si bien no se encuentra un artículo directo sobre la protección de la vida privada, abordan derechos laborales y condiciones dignas.
Convención Americana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belem Do Para)	Si bien no se especifica un artículo directo sobre la protección de la vida privada, aborda aspectos relacionados que se vinculan a la violencia de género.

6 IFAI, el entonces Instituto Federal de Acceso a la Información Pública, en 2015 se convirtió en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Convención Interamericana para la Eliminación de todas las Formas de Discriminación de las Personas con Discapacidad	Si bien no se encuentra un artículo directo sobre la protección de la vida privada, aborda derechos y no discriminación que indirectamente pueden relacionarse con la privacidad.
Convenio Europeo de Derechos Humanos (1950)	El Artículo 8 salvaguarda el derecho a la privacidad al asegurar que ninguna entidad gubernamental pueda intervenir en la vida privada, familiar, domicilio o correspondencia de un individuo, salvo que dicha intervención sea conforme a la ley, necesaria y proporcionada en el contexto de una sociedad democrática.
Carta de los Derechos Fundamentales de la Unión Europea (2000)	El Artículo 7 garantiza el derecho a la privacidad al afirmar que cada persona tiene el derecho a que se respete su vida privada, familiar, domicilio y comunicaciones. Esto refuerza la protección de la privacidad dentro del marco legal de la Unión Europea.

Fuente: elaboración propia, con apoyo en ChatGPT.

Como observamos en el cuadro, se muestran los instrumentos jurídicos internacionales y regionales en donde tratan la protección de la privacidad y también se señalan algunos otros que pueden tener una conexión indirecta con dicho derecho (si bien no hacen énfasis en la era digital, se extiende su protección a ésta).

Por ejemplo, la Convención de Belém do Pará aborda la protección de los derechos de las mujeres frente a la violencia, y aunque no se encuentre explícitamente el derecho a la privacidad lo protege dada su vinculación con éste.

El artículo 3 establece que toda mujer tiene derecho a una vida libre de violencia, tanto en el ámbito público como en el privado. Este artículo pone de relieve la importancia de la privacidad como un aspecto esencial en la protección de las mujeres contra la violencia, garantizando que puedan vivir sin el temor a invasiones en su esfera personal y sin que sus vidas privadas sean objeto de abuso (OEA, 1994).

El artículo 4 señala que toda mujer tiene derecho al reconocimiento, goce, ejercicio y protección de todos los derechos humanos y libertades consagradas por los instrumentos regionales e internacionales sobre derechos humanos. Este artículo refuerza que el derecho a la privacidad es un componente fundamental de los derechos humanos universales, estableciendo una base sólida para su protección en el contexto de la violencia de género (OEA, 1994).

El artículo 10 exige que los Estados Partes informen a la Comisión Interamericana de Mujeres sobre las medidas adoptadas para prevenir y erradicar la violencia contra las mujeres, así como sobre las dificultades encontradas en la implementación de estas medidas. Este requerimiento implica un compromiso con la protec-

ción de estas medidas. Este requerimiento implica un compromiso con la protección de la privacidad de las mujeres afectadas, garantizando que la información sobre sus experiencias y datos personales se maneje con confidencialidad y respeto (OEA, 1994).

La Convención de Belém do Pará resalta la importancia del derecho a la privacidad en la protección de las mujeres contra la violencia mediante algunos artículos importantes. Este derecho es esencial no solo para salvaguardar la vida privada de las mujeres, sino también para garantizar que puedan ejercer plenamente sus derechos humanos sin enfrentar invasiones o violaciones de su intimidad, lo cual aplica al ámbito del ciberespacio. Al proteger la privacidad, se asegura un entorno en el que las mujeres puedan vivir libres de violencia y abuso, y en el que sus derechos y libertades fundamentales estén debidamente resguardados. La integración del derecho a la privacidad en la Convención contribuye a una efectiva de la protección de los derechos digitales y de privacidad en el contexto de la violencia de género.

La privacidad en internet abarca una amplia gama de cuestiones, desde el manejo de datos personales con fines publicitarios hasta la vigilancia electrónica, y su interrelación con otros derechos humanos, como la libertad de expresión. Esta preocupación también se extiende a las redes sociales y servicios digitales, donde los usuarios deben actuar con precaución para protegerse contra acciones ilícitas, como el robo de identidad o fraudes.

La digitalización ha permitido la recolección extensa de datos, que abarca desde la actividad en internet hasta la información en redes sociales, generando riesgos considerables para la privacidad.

En las redes sociales, de acuerdo con Recio Gayo (2022, pp. 47-51), la persona usuaria es la titular de sus datos personales y, en muchos casos, también la responsable de su tratamiento. No obstante, existen otros actores, como los proveedores de la red social (SRS), proveedores de aplicaciones y socios, que también pueden asumir esta responsabilidad. Estos actores gestionan y deciden sobre el uso de los datos personales, especialmente para fines comerciales y publicitarios. Además, los socios pueden analizar o combinar estos datos con otros obtenidos a través de servicios digitales, lo que subraya la importancia de que los usuarios revisen las políticas de privacidad para identificar a los responsables del tratamiento de sus datos. A diferencia de los responsables, los encargados del tratamiento solo procesan datos para prestar un servicio, sin utilizarlos para fines propios.

Es crucial que los usuarios conozcan las plataformas que utilizan, incluyendo la identidad de las empresas que las gestionan, el tipo de datos que recopilan, sus usos y sus prácticas de manejo de datos. Utilizar responsablemente las redes sociales y servicios digitales, limitando la información personal compartida y manteniéndose alerta frente a posibles usos indebidos, es esencial para proteger la privacidad y los

derechos asociados.

El INAI ha publicado diversas recomendaciones orientadas a proteger a la población frente a ciberdelitos, tales como el fraude, el robo de identidad y el ciberacoso, poniendo un enfoque especial en la seguridad de los menores y el uso responsable de las redes sociales. Asimismo, en 2022, presentó directrices para el manejo de datos personales en sistemas de IA, resaltando la importancia de estas tecnologías por su capacidad para recolectar, analizar y compartir datos personales. Estas recomendaciones están diseñadas para fomentar un uso ético y adecuado de la información personal tanto en el ámbito público como privado.

Si bien México ha logrado avances en ciberseguridad y desarrollo digital, aún enfrenta desafíos importantes en su capacidad para responder a riesgos cibernéticos y fomentar el desarrollo digital. De acuerdo con indicadores de 2024 se observa que:

· México ocupa el puesto #42 del *National Cyber Security Index*, el cual mide la capacidad de los países para prevenir, manejar y responder a los ciberataques, por lo que es urgente que el gobierno implemente medidas de ciberseguridad más sólidas para enfrentar los riesgos en constante aumento (NCSI, 2024).

· En el *Global Cybersecurity Index* ocupa el lugar #52, destacando brechas en infraestructura, capacidades legales y técnicas, así como en cooperación internacional.

· El #62 en el *E-Government Development Index*, lo cual refleja la necesidad de avanzar en la digitalización y accesibilidad de los servicios gubernamentales.

· *Network Readiness Index* también en el lugar #62, México enfrenta retos en infraestructura tecnológica y habilidades digitales.

A pesar de las propuestas legislativas en materia de ciberseguridad, las posiciones que ocupa México en estos índices indican que aún hay áreas importantes que necesitan mejorar. Por lo que debe concentrar sus esfuerzos en optimizar su capacidad para enfrentar las ciberamenazas y promover servicios más seguros en internet. Es esencial que esto se refuerce con políticas y regulaciones adecuadas para salvaguardar los derechos digitales en un contexto digital cada vez más expuesto a ciberataques. Sobre todo, que la cultura de la prevención de riesgos sea un pilar que el Estado mexicano incorpore dentro de sus ciberestrategias.

V - REFLEXIÓN FINAL

El impulso acelerado de la IA en diversos sectores ha aumentado las inquietudes sobre la protección de datos y la privacidad. Asimismo, los retos éticos asociados con la implementación de la IA, tales como el sesgo algorítmico y la escasez de transpa-

rencia, han emergido como aspectos cruciales que necesitan ser abordados.

La protección de datos personales en la era de la IA no sólo es un imperativo moral y ético, sino es esencial para salvaguardar los derechos humanos. En un mundo digitalizado, es crucial que los derechos a la privacidad y la protección de datos se integren plenamente en la protección de la dignidad y libertad de las personas. Su implementación en diversas áreas de nuestra vida cotidiana genera serios desafíos, como el riesgo de sesgos algorítmicos y vigilancia excesiva, lo que hace necesaria la creación de regulaciones claras que prevengan el uso indebido de la información personal.

Además, en un entorno tecnológico en constante cambio, es vital que las regulaciones se adapten a las nuevas realidades para garantizar que los derechos de los ciudadanos se protejan de manera efectiva. Por lo tanto, la protección de datos y la privacidad deben reforzarse mediante un marco legal robusto y cooperativo a nivel internacional y nacional. Solo así podremos asegurar que la tecnología actúe como una herramienta de empoderamiento en lugar de un mecanismo de control.

Aunque existen propuestas de ley sobre ciberseguridad y de la IA, los índices internacionales revelan que aún persisten áreas críticas que requieren atención. En México no existen leyes que regulen estas materias. Es esencial que el Estado establezca un enfoque preventivo y de riesgos para hacer frente a las ciberamenazas. Por lo que se requiere de un modelo de gobernanza coordinado con actores internacionales a fin de establecer un ecosistema digital más seguro y confiable para la ciudadanía.

REFERENCIAS

Asís, R. de. (2024). De nuevo sobre Inteligencia Artificial y derechos humanos. *Derechos y Libertades: Revista de Filosofía del Derecho y Derechos Humanos*, (51), 25-40. https://doi.org/10.20318/dyl.2024.8582

ACNUDH (2024). *Normas internacionales relativas a la privacidad digital*. https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

Bieliakov, K., Tykhomyrov, O., Radovetska, L. y Kostenko, O. (2023). Digital Rights in the Human Rights System. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations*, 10(1). https://hrcak.srce.hr/305542

Botero Marino, C. (2012). Libertad de expresión e internet, Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, OEA. https://oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

Cámara de Diputados (1917). *Constitución Política de los Estados Unidos Mexicanos*. https://diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Carreón, C. (2023). La protección de la legislación mexicana en materia de Internet en un contexto de trabajo híbrido. En Hernández, F. (Coord.). *Esquemas de trabajo híbrido y nuevos escenarios internacionales en las bibliotecas jurídicas*. Instituto de Investigaciones Jurídicas, UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/15/7210/37.pdf

Data Protection Laws of The World (2024). México. https://dlapiperdataprotection.com/index.html?t=law&c=MX

De Souza, T. y Sagoo, R. (2024). AI Governance in the Age of Uncertainty: International Law as a Starting Point. *Just Security*. https://www.justsecurity.org/90903/ai-governance-in-the-age-of-uncertainty-international-law-as-a-starting-point/

Hidalgo, A. (2020), "Derecho digital en la unión europea, Techlaw y mercado único digital en la década 2010-2020", *Comares Editorial*, España. Disponible en: https://biblioteca.utc.mx/cgi-bin/koha/opac-detail.pl?biblionumber=436845.

Mendoza Enríquez, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), pp.179-207- https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-214720210000200179.

Morales y Flores (2023). Mexico. En *Privacy, Data Protection and Cybersecurity* (Chapter 12), Edition 10, *Law Business Research Ltd*. https://www.santamarinasteta.mx/wp-content/uploads/2023/11/Mexico-1.pdf.

Naciones Unidas (2023). La inteligencia artificial requiere una gobernanza basada en los derechos humanos. Noticias. https://news.un.org/es/story/2023/11/1526062.

NCSI (2024). *Mexico. National Cyber Security Index*. https://ncsi.ega.ee/country/mx/42.

Organización de Estados Americanos (2013). Resolución La Protección de Datos y la Privacidad deben asegurarse mediante el Derecho Internacional. https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_varsovia_2013_resol_proteccion_datos.pdf

Parlamento Europeo (2024a). La Eurocámara aprueba una ley histórica para regular la inteligencia artificial, 13/03, Unión Europea. https://www.europarl.europa.eu/news/es/press-room/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial.

Parlamento Europeo (2024b). *Reglamento de Inteligencia Artificial*, Texto Aprobado, Unión Europea. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

Pérez de las Heras, B. (2023). El Acuerdo de Libre Comercio entre la Unión Europea y Nueva Zelanda: promoviendo una agenda climática global. *Araucaria*, 25(54). https://revistascientificas.us.es/index.php/araucaria/article/view/23417

Petit A., Wala Z., et. al. (2024). "Una Agenda Digital para Europa". Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/factsheets/es/sheet/64/una-agenda-digital-para-europa

Recio Gayo, M. (2022). *La privacidad en las redes sociales*. INAI. México.

UNESCO (2021). *Recomendación sobre la ética de la inteligencia artificial*, Francia. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa.locale=en.

Woods, A. K. (2023). Digital Sovereignty+Artificial Intelligence. En Anupam Chander, and Haochen Sun (Eds.). *Data Sovereignty: From the Digital Silk Road to the Return of the State*, New York, 2023; online edn, Oxford Academic, 14 Dic. 2023, *Oxford Academic*. https://academic.oup.com/book/55328/chapter/428796733.

Yanamala, A. y Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, Vol. 1(01), pp. 294-319. https://ijaeti.com/index.php/Journal/article/view/392.