EL DERECHO A LA PRIVACIDAD EN MÉXICO ANTE LA INTELIGENCIA ARTIFICIAL Y EL BIG DATA: DESAFÍOS REGULATORIOS

THE RIGHT TO PRIVACY IN MEXICO IN THE FACE OF ARTIFICIAL INTELLIGENCE AND BIG DATA: REGULATORY CHALLENGES

Allegra Tellez Dominguez[1]

SUMARIO: 1. Introducción, 2. Estado del arte, 3. Metodología, 4. Derechos digitales en el contexto de los derechos humanos, 5. El impacto de la era digital en la privacidad, 6. Retos legales y regulatorios, 7. Brechas en la normativa mexicana, 8. Resultados y discusión, Fuentes de consulta

RESUMEN

El artículo analiza el derecho a la privacidad ante la inteligencia artificial y el *big data*; el cómo se ha convertido en un desafío fundamental para México, destacándose los desafíos por las brechas normativas y el analfabetismo digital. Se revisa la regulación del derecho a la privacidad en el entorno digital actual, destacándose las carencias en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su falta de armonización ante las nuevas tecnologías. Se menciona el impacto del Reglamento General de Protección de Datos de la Unión Europea y de la Ley N°18.331 de Protección de Datos Personales y Habeas Data de Uruguay como modelos internacionales de protección de datos y se habla sobre los retos legales y regulatorios en México, incluyendo la recolección masiva de datos por parte de las plataformas digitales y su falta de

ABSTRACT

The article analyzes the right to privacy in the face of artificial intelligence and big data, how it has become a fundamental challenge for Mexico, highlighting the challenges of regulatory gaps and digital illiteracy. The regulation of the right to privacy in the current digital environment is reviewed, highlighting the shortcomings in the Federal Law on the Protection of Personal Data in Possession of Private Parties and its lack of harmonization in the face of new technologies. The impact of the European Union's General Data Protection Regulation and Uruguay's Law No. 18,331 on the Protection of Personal Data and Habeas Data as international models of data protection is mentioned, and it discusses the legal and regulatory challenges in Mexico, including the massive collection of data by digital platforms and their lack of transparency. Finally, the need

1 Licenciada en Derecho por El Colegio de Veracruz (titulación en proceso), donde ha consolidado una formación jurídica integral con especial interés en las ramas penal y civil. Su preparación combina el análisis crítico de las normas con una visión práctica del ejercicio legal, orientada a la construcción de soluciones justas y eficientes.

DOI: https://doi.org/10.5281/zenodo.16740314

RECIBIDO:14 de mayo de 2025
ACEPTADO: 10 de julio de 2025

transparencia. Por último, se examina la necesidad de fortalecer la educación digital y actualizar el marco normativo del país para garantizar una mejor protección de los datos personales. En general, el artículo estudia la vulneración de derechos humanos, especialmente el de privacidad, por la dispersión y falta de homologación del marco normativo en la era digital con el uso de la tecnología y la inteligencia artificial.

PALABRAS CLAVE: derecho a la privacidad digital, protección de datos, analfabetismo digital, marco normativo mexicano

to strengthen digital education and update the country's regulatory framework to ensure better protection of personal data is examined. In general, the article studies the violation of human rights, especially privacy, due to the dispersion and lack of homologation of the regulatory framework in the digital age with the use of technology and artificial intelligence.

KEYWORDS: right to digital privacy, data protection, digital illiteracy, Mexican regulatory framework

1. Introducción

En la actualidad, el derecho a la privacidad se enfrenta a un gran desafío, impulsado por el constante crecimiento de las nuevas tecnologías. Las redes sociales, plataformas digitales, dispositivos móviles, la inteligencia artificial (IA) y el *big data* han modificado la manera en que los individuos interactúan, trabajan, se informan y comparten datos, generando así nuevas dinámicas tanto sociales como jurídicas que desafían los marcos ya establecidos de protección de la privacidad.

A diferencia de épocas anteriores, el derecho a la privacidad se ha visto vulnerado con mayor frecuencia en estos últimos años, dado que cada interacción en línea, desde una simple búsqueda a través de un navegador web hasta la participación en redes sociales o el uso de cualquier aplicación móvil dejan un rastro de información personal (huella digital) que se queda almacenado, y que podría llegar a ser vendido o utilizado con diversos fines; los cuales, la mayoría de sus veces, no tienen el conocimiento o consentimiento pleno de los usuarios.

El presente artículo tiene como objetivo analizar a profundidad el derecho a la privacidad en la era digital desde una perspectiva jurídica. Se examina el impacto que han tenido las nuevas tecnologías ante el derecho a la privacidad como: la inteligencia artificial (IA) y la recolección de datos a través de redes sociales y plataformas; se evalúan los principales retos legales y regulatorios como la falta de armonización entre las leyes ya establecidas y las nuevas tecnologías, el analfabetismo digital que existe tanto en empresas como en individuos; y se identifican las principales brechas en la normativa mexicana, teniendo como punto de referencia el Reglamento

General de Protección de Datos (RGPD) de la Unión Europea.

En el estudio resulta relevante que este contexto de dinámica social cambiante, de una presencia significativa de la tecnología y el uso de la inteligencia artificial para casi todas las actividades humanas contribuye a facilitar muchas de ellas, pero también tiene una parte negativa, la vulneración de diversos derechos, como los tratados en el trabajo ante la ausencia de un marco normativo completo.

Con este análisis se busca aportar al debate que existe sobre la privacidad digital, resaltando la urgencia de reformar los marcos legales existentes del país y el promover y concientizar a la población mexicana, sobre una cultura de responsabilidad y transparencia ante el manejo de la información personal. Lográndose mediante un enfoque integral que combine la legislación, educación y supervisión, es que será posible garantizar la protección de este derecho ante el nuevo entorno digital.

2. Estado del arte

El derecho a la privacidad ha experimentado un importante desafío en la era digital actual. Diversos estudios y autores han abordado el tema desde distintas perspectivas, ofreciendo un amplio panorama. Algunos de ellos son los siguientes.

En el artículo "El derecho a la intimidad en la era de la tecnología de las comunicaciones: una reflexión desde el derecho constitucional" de Alfredo Gutiérrez Ortiz Mena, se discute la necesidad de proteger el derecho a la privacidad y cómo la tecnología moderna puede llegar a obstaculizar este derecho. Como la privacidad ha pasado de ser una defensa contra el estado a ser un derecho complejo que incluye el control de los datos personales en el entorno digital.

En el artículo "Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital" María Álvarez Caro analiza cómo el derecho al olvido es importante para que los usuarios manejen su identidad en línea y protejan sus datos personales que pueden estar de manera indefinida en la web. Esto coincide con la necesidad de adaptar y reformar los marcos legales.

En el artículo "Derecho a la privacidad en la sociedad de la información" Isaura Judith Moreno Pérez y Marina Del Pilar Olmeda García reflexionan sobre la vulnerabilidad de los individuos ante la tecnología por la gran comercialización de los datos personales y la falta de conciencia de sus derechos. Igualmente, abogan por una mejor educación digital que promueva la protección de la privacidad.

Y, por último, en el artículo "El derecho a la protección de datos personales en la era digital" María Fernanda Sánchez Díaz argumenta que los datos personales se han convertido en un recurso valioso, por lo que se requiere de un enfoque ético y centrado en los derechos humanos para garantizar su protección. Se coincide igualmente con la necesidad de actualizar los marcos legales y regulatorios.

a) Teorías

Para otorgarle el soporte teórico y doctrinario al trabajo se tomaron como

referencia el enfoque, principios y características de la teoría del garantismo jurídico de Luigi Ferrajoli y la teoría iusnaturalista en este caso desde la visión de Norberto Bobbio.

La teoría del garantismo jurídico "Es un modelo de derecho fundado en la subordinación a la ley de todos los poderes, a garantías de esos derechos, que normalmente son establecidos por las cartas constitucionales" (Ferrajoli, 2021).

Es decir, para el garantismo lo "natural" son los individuos y sus derechos, necesidades e intereses. Desde esta perspectiva, la privacidad no es un derecho opcional, sino una garantía constitucional que se debe proteger sin excepción, especialmente frente a las nuevas amenazas tecnológicas.

En la era digital, el garantismo jurídico implica que el Estado tiene la obligación de mantener actualizado el marco legislativo, crear mecanismos eficientes de control y supervisión, y sancionar las practicas que vulneren la privacidad de los usuarios.

Es por ello que el tema, al exponer la importancia de la garantía de un derecho que está fundamentado ante la ley, responde a una necesidad de los individuos y es de interés común en la época actual lo cual lo convierte en un derecho de garantismo jurídico.

La teoría iusnaturalista es una doctrina filosófica que distingue aquello que esté dictado por la naturaleza de lo establecido y convenido por los hombres. Varios representantes del iusnaturalismo comparten una tesis básica:

> El derecho natural no sólo se distingue del derecho positivo, sino que además es superior a éste porque emana de una naturaleza divina o racional que determina lo justo y lo válido en términos universales, esto es, con independencia de los dictados particulares de cada Estado (Bobbio, 1991).

Es decir, se defiende que todos los derechos humanos existen de manera connatural, derivado de la naturaleza racional y digna del ser humano, independiente de su reconocimiento legal. Desde esta perspectiva, el derecho a la privacidad es un derecho universal y necesario para el desarrollo libre de la personalidad y vida privada de cada individuo.

El iusnaturalismo fortalece la idea de que toda persona, por el simple hecho de ser humano, tiene derecho a controlar y manejar su información personal, a protegerla y a vivir sin intromisiones arbitrarias, aun cuando las leyes no estén reformadas o desactualizadas. La privacidad, al ser un derecho de noción natural y universal, debiendo de hacerse cumplir y valer, lo convierte en un derecho natural.

3. Metodología

La investigación es básica documental, dado que se origina y mantiene en un marco teórico, con base en la recopilación de datos cualitativos con el propósito en específico de analizar en el trabajo la vulneración de derechos, especialmente la de derechos de privacidad de las personas en la era digital. La pretensión es incrementar los conocimientos en el tema que se investiga

a través de la consulta de documentos para desentrañar el contenido y discurso de la doctrina y normas para plantear escenarios de mejora.

El enfoque es cualitativo, debido a que se centra en el análisis y recopilación de información obtenida de entrevistas, artículos, libros, grupos de difusión, foros y observaciones de otros autores. Esto, con el objetivo de tener una mayor amplitud y profundidad en la comprensión y corroboración de la información. Mientras que, el método sería deductivo sociológico porque se hace uso de los instrumentos técnicos necesarios para el desarrollo de nuevos conocimientos a base de los ya existentes que se encuentran argumentados ante la ley; con el propósito de explicar o interpretar el fenómeno jurídico y tener una comprensión más profunda y completa de dicha naturaleza. Esto con el análisis de teorías, leyes, postulados o principios de aplicación universal y de validez comprobada.

Por último, las técnicas a utilizar de la presente investigación son: análisis de documentos, ya que permitirá determinar la relación que existe entre dos o más variables e interpretar diferentes opiniones. El instrumento utilizado fue la investigación documental, que es la recopilación y selección de información a través de documentos. Además del análisis de contenido y discurso, por un lado, del marco normativo existente y de los estudios realizados por expertos en la materia.

4. Derechos digitales en el contexto de los derechos humanos

En México no existe como tal una ley específica que regule los denominados "derechos digitales". Sin embargo, estos derechos no deben entenderse como un nuevo catálogo de derechos, sino como la proyección de los derechos humanos ya establecidos, pero en el entorno digital. La Constitución Política de los Estados Unidos Mexicanos (CPEUM) y la Ley Federal de protección de Datos Personales en Posesión de los Particulares (LFPDPPP) conforman el marco jurídico principal que garantiza su protección.

El alto comisionado de las Naciones Unidas para los Derechos Humanos ha señalado que "Los mismos derechos que las personas tienen fuera de línea también deben protegerse en línea" (ONU, 2018), lo que implica que los derechos digitales, en realidad, son la manifestación de los derechos humanos: la libertad de expresión, el acceso a la información y el derecho a la privacidad, pero en el ámbito digital. Su objetivo principal es garantizar que los usuarios puedan ejercer con libertad, seguridad y protección sus actividades a través de cualquier plataforma digital o red social.

Dentro del conjunto de "derechos digitales", uno de los pilares, y en el que se basa la presente investigación, es el derecho a la privacidad, cuya protección es esencial para salvaguardar la autonomía personal en la era digital.

a) Derecho a la privacidad

El derecho a la privacidad es reconocido como un derecho fundamental, tanto por el marco jurídico nacional como por el

internacional. El juez Abe Fortas lo describe como "El derecho a ser dejado solo; a vivir la propia vida como uno elija, libre de asalto, intrusión o invasión excepto aquellas que puedan justificarse por manifiestas necesidades de una comunidad que vive bajo un Estado de derecho". Es decir, la privacidad significa el poder decidir por uno mismo el cómo vivir, qué compartir y qué no, sin que terceras personas se entrometan sin una razón valida y legal (Corral, 2000).

En México, su fundamento se encuentra en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos e igualmente en el artículo 12 de la Declaración Universal de Derechos Humanos; también en el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos, que expresamente disponen que nadie podrá ser "Objeto de injerencias arbitrarias o ilegales en su vida privada", alcanzando de esta manera la protección del individuo en la esfera más íntima de su persona. El Comité de Derechos Humanos de la Organización de Naciones Unidas también ha determinado que: "Debe estar garantizado respecto de todas esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas" (Hernández, 2016).

Por ello, la privacidad es un derecho fundamental y necesario al que toda persona debe de tener libre acceso sin excepción, es por ello por lo que no se debe dejar de lado y tomar su control, ya que es la única forma en que se puede tomar las riendas sobre qué información queremos que sí se comparta y cuál no, para poder asumir este nuevo papel de la vida en las redes sociales de forma segura.

Los seres humanos necesitan de la privacidad, para poder explorar nuevas ideas con libertad, y para formar su propia opinión. La privacidad protege de ser juzgados, de la presión social y abusos de poder. Es fundamental para ser un individuo autónomo libre.

5. El impacto de la era digital en la privacidad

Con la llegada de la era digital y su uso masivo, se ha llegado a transformar radicalmente la forma en que se manejan los datos personales, generando tanto beneficios como riesgos en términos de privacidad.

a) *Big data* e IA

La inteligencia artificial (IA) ha llegado a desempeñar un papel muy importante en esta nueva era; por un lado, ofrece herramientas avanzadas para mejorar la seguridad y la gestión de datos, pero, por otro lado, plantea desafíos en términos de vigilancia y uso indebido de la información personal.

La capacidad de la IA para analizar grandes volúmenes de datos (*big data*) de manera concisa y rápida ha permitido avances notorios en la detección de fraudes, la ciberseguridad y personalización de servicios; sin embargo, esta misma capacidad también es utilizada de forma negativa, monitoreando y recopilando los datos personales sin el consentimiento adecuado, lo que genera una gran falta y preocupación sobre la invasión de la privacidad digital.

Unos de los grandes desafíos de la IA en la protección de datos, que menciona Futuro

Legaltech, son los siguientes:

1. Desigualdad en el acceso a la tecnología: no todas las organizaciones tienen el mismo conocimiento o acceso a herramientas.
2. Violaciones de privacidad: debido a que no se lleva una regulación adecuada, existe el peligro de que la información personal sea utilizada sin el conocimiento de los usuarios.
3. Explotación de datos personales: explotar datos personales con fines comerciales, ejemplo: publicidad dirigida.
4. Transparencia y responsabilidad: los procesos internos no son transparentes ni claros.

b) Papel de las redes sociales y las plataformas digitales en la recolección de datos personales

Las redes sociales y plataformas digitales desempeñan un papel fundamental en la recopilación, procesamiento y uso de datos personales de millones de usuarios. A través de diversas estrategias, las plataformas generan una huella digital sobre los intereses, hábitos y comportamientos de cada uno de los usuarios, basándose en las búsquedas, visualizaciones, compras, etcétera; que realizan cada uno de ellos (Rodríguez, 2023).

Algunas de las estrategias que utilizan las plataformas digitales para la recolección de datos son:

1. Información brindada directamente por los usuarios: los usuarios, al aceptar los términos y condiciones del servicio y la política de privacidad, dan la autorización a la plataforma de dar el uso de esos datos (Rodríguez, 2023).

   Entre los datos personales recopilados por algunas redes sociales durante su proceso de registro encontramos:

   Nombre, fecha de nacimiento, número de teléfono celular, correo electrónico, información de geolocalización de la persona, IP del equipo utilizado, información biométrica (huella facial, de voz o digital), datos de métodos de pago, entre otros (Rodríguez, 2023).
2. Información recopilada de la actividad en la plataforma: la plataforma o red social monitorea en todo momento la actividad del usuario, con el objetivo de guardar sus preferencias, mostrar contenido personalizado, recopilar datos analíticos, y mostrar anuncios personalizados (Gobierno de España, 2025).
3. Seguimiento fuera de la aplicación: varias de las plataformas y redes sociales utilizan un sistema de seguimiento de huella para seguir rastreando la actividad del usuario incluso después de que este salga de la plataforma o red social. Esto se logra mediante las *cookies* y pixeles de seguimiento, herramientas de monitoreo y la vinculación con otras aplicaciones (Gobierno de España, 2025).

6. Retos legales y regulatorios

La creciente recopilación de datos personales por parte de las redes sociales y plataformas digitales ha generado importantes desafíos legales y regulatorios. México, al igual que otros países, enfrenta dificultades para garantizar una protección efectiva de la privacidad de los usuarios.

a) Armonización de la reciente reforma a la LFPDPPP ante las nuevas tecnologías

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) es el principal instrumento normativo en México que se encarga de: "Regular el tratamiento de los datos personales que poseen los particulares. Esto con el fin de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas". Es decir, que establece los principios, derechos, deberes y procedimientos que van enfocados a proteger los datos personales de cada individuo frente a usos indebidos o no autorizados por parte de las grandes empresas, organizaciones u otros particulares (INAI, 2021).

Esta ley fue publicada en el año 2010, pero con la reciente reforma, publicada el 20 de marzo de 2025, representa un mayor esfuerzo por armonizar el marco jurídico con los nuevos desafíos tecnológicos. Algunos de los cambios más notorios incluyen la amplia definición de lo que es considerado "dato personal" y de los sujetos que son regulados, incluyendo a las personas morales y ampliando las responsabilidades de los encargados de su tratamiento. Igualmente, se fortalecen las obligaciones en torno al consentimiento, el cual debe de ser claro, libre, específico y otorgado por separado para cada propósito, eliminándose así el margen de "para fines compatibles". También se pide que los avisos de privacidad sean más fáciles de entender y estén adaptados a los medios digitales. Se obliga a las empresas a proteger la confidencialidad de los datos, incluso tras la terminación de la relación con el usuario y se solicita consentimiento para cualquier transferencia de datos a terceros, salvo en los casos establecidos por la ley. Finalmente, se incorpora el derecho de oposición frente a tratamientos automatizados que afecten al usuario, como los generados por inteligencia artificial (IA), y se establece un nuevo procedimiento para que las personas puedan defender sus derechos, incluyendo la opción de acudir a un juez especializado. Sin embargo, la reforma también genera dudas, ya que sustituyó al INAI por la Secretaría Anticorrupción y Buen Gobierno, transfiriéndole sus funciones.

Por último, se presenta un análisis breve y conciso del impacto de uno de los conceptos mencionados en la tabla 1, para lograr una mejor comprensión:

Consentimiento: Con la reciente reforma, ahora se especifica que sea libre, específico e informado el consentimiento, además de que debe ser otorgado por separado para cada propósito. Esto, a diferencia de su definición anterior, que era ambigua.

La nueva reforma busca contrarrestar las prácticas comunes de las plataformas digitales, donde el consentimiento es genérico, poco claro o forzado; un ejemplo de ello es al hacer clic en "Aceptar todo".

Por ello ahora, legalmente, las plataformas deben desglosar los usos de datos y obtener consentimiento individual para cada uno, ejemplo: uso con fines publicitarios o para análisis interno.

Tabla 1. Modificación de la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Concepto	Antigua versión LFPDPPP	NLFPDPPP
Aviso de privacidad	Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.	Documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos, de conformidad con el artículo 14 de la presente Ley.
Bases de datos	El conjunto ordenado de datos personales referentes a una persona identificada o identificable.	Conjunto ordenado de datos personales referentes a una persona identificada o identificable condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Consentimiento	Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.	Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable.	Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Datos personales sensibles	Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.	Aquellos datos personales que afecten a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
Derechos ARCO	No había definición en la LFPDPPP.	Derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Fuente de acceso público	Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta Ley.	Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa, y sin más exigencia que su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás disposiciones jurídicas aplicables.
Responsable	Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.	Sujetos regulados a que se refiere la fracción XVI de este artículo.
Sujetos regulados	No había definición en la LFPDPPP.	Personas físicas o morales de carácter privado que llevan a cabo el tratamiento de datos personales;
Tratamiento	La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
Transferencias	Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la titular, del responsable o de la persona encargada del tratamiento.

Fuente: Nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación. Basham. https://basham.com.mx/nueva-ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares-publicada-en-el-diario-oficial-de-la-federacion/

b) Analfabetismo digital en empresas y usuarios

La brecha digital tiene diversas manifestaciones, una de las cuales es el analfabetismo digital. Este concepto sugiere la existencia de una nueva problemática, distinta a la que se conoce.

En la actualidad, la comunicación no solo fluye a través del lenguaje escrito, sino que también mediante las nuevas tecnologías. Por lo tanto, así como hay personas que no saben leer o escribir, hay personas que no tienen las suficientes habilidades para acceder a la red de comunicación o información de las nuevas tecnologías. Es decir, el analfabeta digital es "Aquella persona que realiza sus actividades personales, educativas y profesionales sin llegar a vincularse con las plataformas digitales o informarse de ellas" (s.a., 2023). En México, 23% de los internautas son

considerados analfabetas digitales (aproximadamente 20 millones de personas). Mientras que "65.5% de las micro, pequeñas y medianas empresas (MiPymes) poseen un conocimiento básico sobre actividades de internet" (IFT, 2024).

> Existe una muy baja cultura con respecto a la prevención de delitos o ataques cibernéticos, mientras que el 90.6% de los usuarios de internet se preocupan por la ciberseguridad, solo el 50% de ellos realmente considera y se asegura que sus dispositivos este verdaderamente protegidos de estos riesgos (Laris, 2023).

El impacto de esto causa consecuencias directas en la seguridad y privacidad de los datos personales. Ejemplo: en usuarios, la falta de habilidades digitales dificulta la comprensión de la importancia que tiene proteger los datos personales. Mientras que, para las empresas, la falta de conocimiento en ciberseguridad aumenta el riesgo de brechas y las posibles sanciones legales que podrían llegar a tener (Calderón, 2024).

Para poder evitar estos riesgos es necesario el promover la alfabetización digital tanto a usuarios como a empresas, a través de la educación en protección de datos y la creación de conciencia sobre la privacidad.

La importancia de la alfabetización digital como componente vital de la vida cotidiana es cada vez más evidente. En la actualidad, se ha hecho indispensable el uso de plataformas digitales, ya que las personas se han hecho dependientes de ellas para mantenerse informados, conectados y productivos en el día a día.

c) Casos de hackeos masivos y filtraciones de datos personales

Durante la última década se ha llegado a presentar un gran número de casos de ciberataques, hackeos o filtraciones de datos personales, tanto a nivel nacional como internacional. A continuación se expondrán algunos, detallando las repercusiones que han conllevado y cómo han llegado a afectar a millones de usuarios y empresas.

1. En 2012, LinkedIn sufrió de un ciberataque que en un principio se creía haber afectado a 6.5 millones de usuarios, sin embargo, en 2016 se descubrió el verdadero alcance. Una base de datos con 167 millones de cuentas robadas de LinkedIn se puso a la venta en la dark web. La brecha se produjo por la forma insegura en la que la plataforma almacenaba las contraseñas y la política de cifrado obsoleta (Bloomberg/AP, 2016).
2. En 2013, Target sufrió un ciberataque que afecto a 70 millones de clientes, logrando no solo obtener información personal como nombres, direcciones, correos electrónicos o números de teléfono, sino que aproximadamente 40 millones de los 70, se vieron afectados con el robo de sus datos bancarios. Dicho ataque se llevó a cabo usando un malware PoS, o malware en el punto de venta, que afectó a los lectores de tarjetas bancarias y cajas registradoras (Contreras, 2023).
3. En 2014, eBay sufrió un ciberataque a través de cuentas comprometidas de empleados. Se afectó a 145 millones de usuarios, a los que la compañía contactó unos meses después para pedirles que

cambiaran sus contraseñas (Contreras, 2023).

4. En 2018, Sony Pictures sufrió un ciberataque en el que se robó información personal y financiera de empleados y actores famosos. La información robada se utilizó para realizar amenazas e intentos de extorsión. El FBI investigó el incidente y concluyó que fueron *hackers* de Corea del Norte (Araujo, 2023).
5. En 2016, Yahoo! Informó que sufrió una brecha de seguridad, dos años atrás (2014), que comprometió las cuentas de correo de 500 millones de usuarios. Dejando expuestos datos como direcciones de correo, contraseñas, fechas de nacimiento, números de teléfono, nombres y apellidos, entre otra información adicional (Contreras, 2023).
6. En 2018 se descubrió que 87 millones de usuarios de Facebook (Meta) fueron vulnerados por la empresa de análisis de datos, Cambridge Analytica, al haber accedido de manera ilícita a sus cuentas, logrando obtener información personal, con el propósito de utilizarla y explotarla para influir en la campaña presidencial de EE. UU. de 2016 (Contreras, 2023).
7. En 2018, Quora sufrió un ciberataque en el que su seguridad fue vulnerada, permitiendo el acceso a información confidencial de aproximadamente 100 millones de usuarios de la plataforma. Se robó información personal como: los nombres, direcciones de correo electrónico, contraseñas, datos importados de redes sociales, y seguridad de los datos (Riquelme, 2021).
8. En abril de 2020 Nintendo confirmó haber sido víctima de un ataque que comprometió aproximadamente 160,000 cuentas de usuario, la compañía dio a conocer tiempo después que no fue demasiado precisa ya que se le sumaron otros 140,000 afectados, llegando a ser casi 300,000 usuarios. Desde entonces, Nintendo ha hecho hincapié en la utilización de un doble factor de autenticación que permitiría dotar de una capa más de seguridad a sus usuarios y evitar este tipo de ataques (s.a., 2020).
9. Entre el 5 y 11 de julio de 2020, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el Banco de México (Banxico) y el Sistema de Administración Tributaria (SAT) sufrieron afectaciones en sus respectivas páginas de internet (Riquelme, 2021).
10. Entre mayo y junio de 2020, la Secretaría de la Función Pública sufrió un problema de seguridad que expuso las declaraciones patrimoniales de 830,000 funcionarios, cifra que representa a más de la mitad de los empleados de la Administración Pública Federal. Entre la información vulnerada venían las claves de identificación fiscal (RFC) y de registro de población (CURP), además del sexo de los funcionarios afectados (Riquelme, 2021). Para noviembre del mismo año, el INAI determinó que la Secretaría de la Función Pública había fallado al no proteger la confidencialidad

11. En octubre de 2020, los datos de 4.7 millones de usuarios de la Fintech Clip fueron puestos en venta en un foro de internet. Entre esos datos iban los correos electrónicos y números telefónicos de los usuarios (Riquelme, 2021).
12. En 2020, la Agencia Digital de Innovación Pública de la Ciudad de México (ADIP), entidad creada por la administración de Claudia Sheinbaum, sufrió un ataque de seguridad que expuso la información personal de varios ciudadanos; información que estuvo disponible mediante varias direcciones de fácil acceso a través de Google (Riquelme, 2021). La información expuesta estaba vinculada a quejas y denuncias que habían sido levantadas dentro de su Sistema Unificado de Atención Ciudadana (SUAC) (Riquelme, 2021).

7. Brechas en la normativa mexicana

Como se ha visto previamente, la rápida evolución de tecnologías como la IA, ha llegado a rebasar lo ya establecido en las leyes a través de los años; por lo cual, la normativa mexicana presenta diversas brechas o vacíos legales que le dificultan garantizar la protección de datos a los usuarios ante las nuevas tecnologías. Algunas de esas brechas son: la desactualización frente a nuevas tecnologías, falta de educación digital, debilidad en la implementación y supervisión, y, la más relevante, la falta de armonización entre normativas.

Como bien se planteó durante la inauguración del foro inteligencia artificial, que se llevó a cabo el 3 de marzo del 2024, la comisionada del INAI, Josefina Román Vergara, señaló: "Es urgente actualizar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, pues no contempla disposiciones específicas sobre el uso de la Inteligencia Artificial aun cuando esta tecnología se alimenta, esencialmente, de datos personales […]". Al igual que Román Vergara del Instituto de Investigaciones Jurídicas (IIJ) de la UNAM, resaltó que "Es necesario contar con un marco que regule el uso de este tipo de tecnología y garantice el respeto de los derechos de la población en general y, en particular, de niñas, niños y adolescentes, quienes constituyen un sector vulnerable en el entorno digital" (Universal, 2024).

> Llevamos muchos años conviviendo con inteligencia artificial, pero, particularmente, en estas últimas fechas nos hemos dado cuenta de que es un tema al que hay que ponerle atención; tenemos que ocuparnos; tenemos que normarlo de la mejor manera, sin inhibir el uso de las tecnologías de la información, pero sí, poniendo en el centro de esta normativa la protección de las personas y sus derechos (Vergara, 2024).

a) Falta de armonización normativa

Otros países han avanzado más en la regulación del derecho a la privacidad a través de nuevas tecnologías. Dos ejemplos de ello son el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley N°18.331 de Protección de Datos Personales y Habeas Data de Uruguay.

1. Reglamento General de Protección de Datos (RGPD) de la Unión Europea

Conocida porque "[...] Es la norma más estricta del mundo en materia de privacidad y seguridad" (CUE, 2024), establece los requisitos específicos para empresas y organizaciones sobre recolección, almacenamiento y gestión de los datos personales. Este reglamento se aplica tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE (RGPD, 2022).

Es decir, se encarga de regular la recopilación, almacenamiento y gestión de datos personales a las empresas y organizaciones, solo aplicando a las que tratan con información personal de personas que vivan en la Unión Europea.

Igualmente, algunas de las normativas o derechos más relevantes que menciona el Reglamento General de Protección de Datos (RGPD) son:

1.1 Categorías especiales de datos

Los datos personales que no se pueden tratar son:

- Origen racial o étnico
- Orientación sexual
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación sindical
- Datos genéticos, biométricos o sanitarios, salvo en casos específicos (por ejemplo, cuando se da un consentimiento explícito o cuando el tratamiento es necesario por razones de interés público esencial, sobre la base del Derecho nacional o de la UE)
- Condenas e infracciones penales, a menos que lo autorice el derecho nacional o de la UE

1.2 Tratamiento de datos

Se establece que los datos deben tratarse de manera lícita para un fin específico y legítimo y solo deben de tratarse los necesarios para alcanzar ese objetivo. La empresa debe cerciorarse de que se cumpla con las condiciones para el tratamiento de datos personales.

> Condiciones: el interesado ha dado su *consentimiento*, los datos personales son necesarios para respetar una *obligación contractual* con el interesado, los datos personales son necesarios para cumplir una *obligación legal*, los datos personales son necesarios para proteger los *intereses vitales* del interesado, los datos personales se tratan para una *misión de interés* público; se actúa en *interés legítimo* de la empresa, siempre que en el tratamiento de los datos del interesado no se vean gravemente afectados los derechos y libertades fundamentales de este; si los derechos de esa persona prevalecen sobre los intereses de la empresa, no se pueden tratar sus datos personales (RGPD, 2022).

Y, en caso de consentimiento, se aplican normas estrictas para el tratamiento de datos, con el objetivo de garantizar que el interesado comprenda lo que está consintiendo. El consentimiento debe darse de manera libre, específica, informada e inequívoca, mediante una solicitud presentada en un lenguaje claro y sencillo, expresándose mediante un acto afirmativo. Y, cuando la persona consienta el tratamiento de datos, solo se podrán tratar para los fines que haya dado su

conocimiento, ofreciéndose también la posibilidad de retirar su consentimiento.

1.3 Transparencia
Los usuarios deben de recibir información clara sobre quien, como y porque tratan sus datos personales. Exponiéndose principalmente: la identidad del responsable, el motivo, la base jurídica, el receptor de los datos.

1.4 Normas específicas para menores de edad
Para el acceso a una red social o cuenta de descarga de contenido, es necesario primero obtener la autorización parental, ejemplo: a través de una notificación al teléfono celular del padre, madre o tutor.

1.5 Derecho de supresión (derecho al olvido)
El usuario puede solicitar la supresión de sus datos personales; es decir, se les permite la eliminación de los datos.

1.6 Violación de datos. Proporcionar la notificación adecuada

Se le considera violación de datos a la divulgación accidental o ilegal a destinatarios no autorizados de datos que sean responsabilidad de una empresa; así como su indisponibilidad temporal o modificación.

Si se produce una violación de datos que representa un riesgo para los derechos y las libertades individuales, es preciso notificarlo a la autoridad de protección de datos competente en un plazo de 72 horas a partir del momento en que se conozca la infracción.

En caso de que la violación de datos signifique un alto riesgo para las personas afectadas, la empresa está obligada a informarles.

2. Ley N°18.331 de Protección de Datos Personales y Habeas Data de Uruguay
Uruguay es otro ejemplo valioso, ya que sus normativas en protección de datos presentan una integración coherente entre la ley, reglamento y autoridad de control.

Existen varias normativas que establecen las disposiciones relativas a la protección de datos personales, como “La ley 18381 de acceso a la información pública, la ley no. 18.335 de 08/15/2008 relativa a Derechos y obligaciones de los pacientes y usuarios de los servicios sanitarios, la ley no. 18.244 de 12/27/2007 relativa a deudores de alimentos morosos, etc.”, pero la ley madre de todas es la Ley no. 18.331 de Protección de Datos Personales y Habeas Data (Data protection guide Uruguay, s. f.).

Uruguay adoptó la Ley N°18.331 de Protección de Datos Personales y Habeas Data en 2008, la cual se encarga de regular la acción de habeas data e introduce algunos principios relevantes como la privacidad, el consentimiento, la responsabilidad proactiva, el registro obligatorio de bases de datos y la notificación de brechas de seguridad. En 2020, se actualizo la ley con el Decreto N°64/020, derivado de la Ley 19.670, reforzando obligaciones como la evaluación de impacto y designación del delegado de Protección de Datos; es decir, de la Unidad Reguladora y Control de Datos

Personales (URCDP) (Data protection guide Uruguay, s. f.).

Este marco normativo ha permitido a Uruguay alcanzar un alto nivel de protección, llegando a ser reconocido incluso por la Unión Europea, garantizando una aplicación coherente entre la ley, su reglamento y autoridad regulatoria, la URCDP (Casado, 2024). Incluso, se incorporan principios modernos alineados con el Reglamento General de Protección de Datos (RGPD) europeo. Algunos de los más relevantes son los siguientes:

- Privacidad desde el diseño y por defecto (Decreto 64/020, Art.11)
- Consentimiento informado y expreso (Ley 18.331, Art. 9)
- Evaluación de impacto en protección de datos (PIA) (Decreto 64/020, Art. 14)
- Notificación obligatoria de brechas de seguridad (Decreto 64/020, Art. 12)
- Registro obligatorio de bases de datos (Ley 10.331, Art, 19)

8. Resultados y discusión

El estudio reveló que la protección del derecho a la privacidad en México enfrenta una gran variedad de limitaciones ante la evolución de los medios digitales y nuevas tecnologías. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) es ineficaz ante los nuevos fenómenos como el uso de *big data*, inteligencia artificial (IA) y recolección de datos biométricos, lo que crea vacíos legales relevantes.

Además, se identificó un alto nivel de analfabetismo digital tanto en empresas como en usuarios, lo cual incrementa la vulnerabilidad de los datos personales. Las plataformas digitales se aprovechan de esta situación mediante mecanismos poco transparentes y confiables de recolección de datos biométricos, mayormente sin el conocimiento o consentimiento real de ello.

Los casos de hackeos masivos, tanto a nivel nacional como internacional, confirman la fragilidad de los sistemas de protección de datos. Esto comparado con otras regulaciones como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley N°18.331 de Protección de Datos Personales y Habeas Data de Uruguay, México presenta importantes fallas en términos de actualización normativa.

En consecuencia, fortalecer la protección de la privacidad en México no es solo el hecho de actualizar o reformar el marco normativo, sino también el fomentar una mayor cultura de responsabilidad digital, impulsar la capacitación tanto a las empresas como a la población, y reforzar las capacidades de transparencia, control y vigilancia del tratamiento de datos personales.

Propuestas

Derivado de los hallazgos y análisis realizados en el presente estudio, se identifican algunas acciones necesarias para fortalecer la protección del derecho a la privacidad en México. Con estas propuestas se busca principalmente responder a las brechas normativas detectadas, así como al bajo nivel de alfabetización digital que predomina en el país.

1. Incorporación de principios del Reglamento General de Protección de Datos de la Unión Europea (RGPD) en la legislación mexicana.
Con el objetivo de armonizar la normativa mexicana con los marcos internacionales, se sugiere adoptar algunos de los siguientes principios del RGPD:

- Consentimiento (art. 7, RGPD): fortalecer el consentimiento, asegurarse de que sea libre, especifico, informado y revocable en cualquier momento, otorgado mediante actos claros.
- Derecho a la supresión o "derecho al olvido" (art. 17, RGPD): garantizar la eliminación de datos personales cuando ya no sean necesarios o cuando el usuario retire su consentimiento.
- Evaluación de impacto en la protección de datos (art. 35, RGPD): establecer que es obligatorio realizar evaluaciones previas al tratamiento de datos en casos de alto riesgo, como en el uso de la inteligencia artificial (IA) o de los datos biométricos.

Con estas medidas se fortalecería la autonomía informativa de los usuarios y se limitarían las prácticas abusivas en los entornos digitales.

2. Estrategia de alfabetización digital con enfoque en la protección de datos.
Se sugiere implementar una campaña a nivel nacional que sea permanente sobre la educación digital ciudadana, bajo el nombre tentativo "Protege tu huella digital", con el objetivo de capacitar a la población sobre los derechos digitales, protección de datos, seguridad en línea y uso ético de las plataformas digitales.

Se daría a través de cursos virtuales y presenciales por niveles (básico, intermedio y avanzado), dirigidos a usuarios, estudiantes, docentes, servidores públicos, y mipymes; igualmente se proporcionaría material didáctico accesible y se crearían espacios de difusión en medios públicos o redes sociales.

Con estas acciones se lograría contribuir a no solo mitigar el analfabetismo digital, sino a fomentar una mayor cultura de responsabilidad y prevención en torno a la privacidad digital.

Referencias

(s.a). (2020) Eleconomista.net. https://www.eleconomista.net/tendencias/Nintendo-confirmo-que-los-datos-personales-de-160000-cuentas-fueron-expuestas-en-un-intento-de-ciberataque-20200424-0033.html

(s. f.). Europa.eu. de https://www.consilium.europa.eu/es/policies/data-protection-regulation/

(s. f.). Org.mx. de https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-656-de-las-mipymes-tienen-un-conocimiento-basico-en-cuanto-las-actividades-que-realizan-en?

¿Cuál es el impacto de un analfabeta digital ante los riesgos y vulnerabilidades en el ciberespacio? (2021). Blog Sector Enerético en RH | AMEDIRH; Asociación Mexicana en Dirección de Recursos Humanos. https://www.amedirh.com.mx/blogrh/recursos-humanos/cual-es-el-impacto-de-un-analfabeta-digital-ante-los-riesgos-y-vulnerabilidades-en-el-ciberespacio/?

Alfabetización digital debe considerar protección de datos personales. (s. f.). Org.mx., de https://www.infoem.org.mx/es/contenido/noticias/alfabetizaci%C3%B3n-digital-debe-considerar-protecci%C3%B3n-de-datos-personales-como?

Araujo, A. (2023). Ciberataques: Conoce los 10 más famosos de la historia. Hackmetrix Blog. https://blog.hackmetrix.com/los-10-ciberataques-mas-famosos-de-la-historia/

Basham Ringe y Correa S.C. (2025). Nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación. Basham. https://basham.com.mx/nueva-ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares-publicada-en-el-diario-oficial-de-la-federacion/

Bloomberg/AP. (2016). Hackeo a LinkedIn en 2012 pasó de 6 millones a 117 millones de cuentas. El Financiero. https://www.elfinanciero.com.mx/tech/hackeo-a-linkedin-paso-de-millones-a-117-millones-de-cuentas/

Bobbio, N. (1991). El positivismo jurídico: Lecciones de filosofía del derecho. Fondo de Cultura Económica.

Calderón, C. (2024). El analfabetismo digital afecta a 23% de los internautas que hay en México. El Financiero. https://www.elfinanciero.com.mx/empresas/2024/06/18/el-analfabetismo-digital-afecta-a-23-de-los-internautas-que-hay-en-mexico/

Caro, M. Á. (2015). Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital. Editorial Reus.

Código Penal Federal, (2021).

Cómo recolectan y usan su información los sitios web y las aplicaciones. (2021). Consumer Advice. https://consumidor.ftc.gov/articulos/como-recolectan-y-usan-su-informacion-los-sitios-web-y-las-aplicaciones?utm_source.com

Constitución Política de Los Estados Unidos Mexicanos, (2007).

Contreras, R. (2023). Los 10 ciberataques más grandes de la década. Computing. https://www.computing.es/seguridad/los-10-ciberataques-mas-grandes-de-la-decada/

Convención Americana sobre Derechos Humanos, (1981).

Data protection guide Uruguay. (s. f.). Multilaw.com. https://multilaw.com/Multilaw/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Uruguay.aspx?

de Datos Personales Inai, M. L. G. P. N. C. D. E. P. (s. f.). REDES SOCIALES Y PROTECCIÓN DE DATOS PERSONALES. Redipd.org. de https://www.redipd.org/sites/default/files/inline-files/Panel_9_Redes_Sociales_y_PDP_ok-INAI.pdf

El papel fundamental de la alfabetización digital en los contextos de desplazamiento forzado. (2024). https://www.fmreview.org/disrupcion-digital/casswell/?

Ferrajoli, L. (2021). La democracia a través de los derechos: El constitucionalismo garantista como modelo teórico y como proyecto político. Gedisa.

Futurolegaltech.es. (s. f.). Impacto de la IA en la Privacidad y Protección de Datos. https://futurolegaltech.es/impacto-de-la-ia-en-la-privacidad

Gobierno de España. (2025). Derechos digitales: ¿qué son y cómo protegerlos? La Moncloa. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/Paginas/2025/050225-que-son-los-derechos-digitales.aspx

Gutiérrez Ortiz Mena, A. (2014). El derecho a la intimidad en la era de la tecnología de las comunicaciones: una reflexión desde el derecho constitucional. Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional, 1(31).

Impacto de la IA en la Privacidad y Protección de Datos. (s. f.). Futurolegaltech.es. de https://futurolegaltech.es/impacto-de-la-ia-en-la-privacidad

Moreno Pérez, I. J., & Olmeda García, M. D. P. (2021). Derecho a la privacidad en la sociedad de la información. ADVOCATUS, 37.

Normativa y legislación en PDP – Marco Internacional de Competencias de Protección de Datos Personales para Estudiantes. (s. f.). Org.mx., de https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

Privacidad de datos en la era de la IA. (2024). Canvia. https://canvia.com/privacidad-datos-inteligencia-artificial/

Privacidad en el entorno digital – Marco Internacional de Competencias de Protección de Datos Personales para Estudiantes. (s. f.). Org.mx. de https://micrositios.inai.org.mx/marcocompetencias/?page_id=657

Proceso Digital. (2018). Ciberataque en plataforma Quora expone datos de 100 millones de usuarios. Proceso Digital. https://proceso.hn/ciberataque-en-plataforma-quora-expone-datos-de-100-millones-de-usuarios/

Protección de Datos conforme al reglamento RGPD. (2022). Your Europe. https://europa.eu/

youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Riquelme, R. (2021). 2020, en 12 hackeos o incidentes de seguridad en México. El Economista. https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

Rodríguez, F. (2023). Protección de datos personales, redes sociales en América Latina y Caribe. Gobernarte. https://blogs.iadb.org/administracion-publica/es/que-esta-pasando-con-nuestros-datos-personales-en-las-redes-sociales/?utm_source=com

Sánchez Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital. Revista eurolatinoamericana de derecho administrativo, 10(1), e235.

Unión Europea. (2012). Commission Decision 2012/484/EU on the adequate level of protection of personal data in Uruguay. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0484

Universal, E. (2024). Inai urge a actualizar LFPDPPP para regular uso de IA. Yahoo! Noticias. https://es.us/inai-urge-actualizar-lfpdppp-regular-083231720.html?

Белих, А. (2019). Artículo 35 RGPD. Evaluación de impacto relativa a la protección de datos. Gdpr-text.com - GDPR Text, Translation and Commentary; GDPR-Text.com. https://gdpr-text.com/es/read/article-35/