Privacidad, huella digital y derecho a la protección de datos personales en Internet

Privacy, Digital Footprint, and the Right to Protection of Personal Data on the Internet

María Fernanda Sánchez Díaz[1]

Resumen: Este artículo examina los derechos relacionados con la privacidad y la protección de datos personales mediante el adecuado manejo de nuestra huella digital, una identidad en línea de la cual resulta inevitable escapar, dado que muchas de las actividades cotidianas nos obligan a interactuar con Internet y sus diversas formas de participación, moldeando así nuestra presencia digital con repercusiones tanto favorables como desfavorables. En este contexto, es imperativo reconocer que nuestra realidad tangible está cada vez más vinculada a la dimensión digital, y que recae en la responsabilidad individual y estatal fomentar una cultura de respeto hacia la privacidad y la protección de datos personales.

[1] Licenciada en Derecho, Maestra en Derecho y Doctora en Derecho (Universidad Nacional Autónoma de México). Máster en Protección Internacional de los Derechos Humanos (Universidad de Alcalá). Catedrática de la Universidad Nacional Autónoma de México en la Licenciatura en Derecho y en el Posgrado en Derecho. Miembro del Sistema Nacional de Investigadores del CONAHCYT.

Palabras clave: Privacidad, huella digital, Internet, datos personales, redes sociales

Abstract: This article examines the rights related to privacy and personal data protection through the proper management of our digital footprint, an online identity from which it is inevitable to escape, given that many everyday activities compel us to interact with the Internet and its various forms of engagement, thus shaping our digital presence with both favorable and unfavorable consequences. In this context, it is imperative to recognize that our tangible reality is increasingly linked to the digital world, and that it is the responsibility of individuals and the state to foster a culture of respect for privacy and the protection of personal data.

Keyword: Privacy, Digital Footprint, Internet, Personal Data, Social Networks

Recibido: 14.5.2024 Aceptado: 20.9.2024

Sumario

1. Introducción

2. El derecho humano a la privacidad

3. La huella digital en Internet

4. Derecho a la protección de datos personales en Internet

5. Conclusiones

1. Introducción

El reconocimiento jurídico de los derechos humanos ha sido el resultado de una batalla que se ha prolongado a lo largo de varios siglos, remontándonos desde la histórica "Carta de Derechos" de 1215 hasta el principal modelo adoptado por naciones como México, representado por la Declaración Francesa de los Derechos del Hombre y del Ciudadano de 1789.

Dada la progresividad que configura a los derechos humanos, con el paso del tiempo, hemos sido testigos de una mayor aceptación de derechos adaptados a contextos sociales, políticos, jurídicos, económicos y ahora digitales. Si bien es crucial el reconocimiento legal de estos derechos para otorgarles un carácter vinculante, es evidente que la protección para garantizar su ejercicio efectivo no ha alcanzado los resultados deseados por la sociedad. Las modificaciones legales no son suficientes si las instituciones no se fortalecen con un enfoque de democracia constitucional. Es esencial que la sociedad participe de manera creciente y proactiva para exigir el Estado el respeto de sus derechos.

En el caso específico de México, existen disposiciones constitucionales que reconocen el derecho a la privacidad y la protección de datos personales. Además, derivado de la reforma constitucional del 10 de junio de 2011 en materia de derechos humanos, se cuenta con lo estipulado en instrumentos internacionales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos

Civiles y Políticos y el Convenio 108 de Europa, todos ellos de carácter vinculante para el Estado mexicano. Esto implica un catálogo más amplio de reconocimiento de los derechos humanos, junto con legislación específica en la materia y organismos constitucionales autónomos como el INAI y sus homólogos a nivel local. Sin embargo, ante la disrupción tecnológica que experimentamos, estas medidas han quedado en cierta forma obsoletas para abordar el impacto que la tecnología tiene en nuestros derechos y en nuestra vida cotidiana.

Esta situación se ve agravada por la falta de conciencia social y estatal para comprender la dinámica que implica una vida digital, comenzando por entender lo que es la huella digital y su impacto a corto, mediano y largo plazo en nuestra vida pública y privada, así como la intervención de terceras personas en la generación de parte de nuestra huella digital al compartir información sobre nosotros en diversas plataformas sociales.

Se han realizado avances normativos para contrarrestar los efectos del uso inadecuado de estas plataformas, aunque estos han sido mayormente reactivos en lugar de preventivos. Un ejemplo de ello es el caso europeo, donde se ha implementado el primer registro de reconocimiento del derecho al olvido en Internet. Este derecho es crucial y debe ser legalmente reconocido en todos los países, debido a las implicancias que su ausencia está teniendo, especialmente en un nuevo contexto digital que involucra a la Inteligencia Artificial (IA), la Inteligencia Artificial Generativa (IAG) y la tecnología vinculada con el Metaverso, el cual ya impacta la vida real de las personas. No obstante, nos

encontramos en un escenario carente de normatividad y, en consecuencia, sin protección efectiva para los usuarios.

No podemos correr el riesgo de que la tecnología avance al punto de dejar obsoleta nuestra legislación, sin considerar su impacto en los derechos humanos y en diversos sectores de la vida política, social, económica y jurídica. El problema a abordar en esta investigación es identificar los riesgos que existen para la sociedad en general en el entorno digital, donde los derechos humanos, especialmente el derecho a la privacidad y a la protección de datos personales, se han visto afectados por la disrupción tecnológica de los últimos años. La interacción con la tecnología es fundamental para la huella digital que estamos formando, de la cual nadie está exento.

La evolución tecnológica constituye un importante imán para los que consideramos como parte de los denominados “grupos vulnerables”, como son las niñas, niños y adolescentes, quienes pueden poner en riesgo su integridad física, sexual y psicológica al no comprender los alcances y consecuencias del uso indebido de Internet, comenzando a formar su huella digital desde una edad muy temprana. Esta situación se agrava cuando personas sin escrúpulos utilizan esa información con fines maliciosos; por ejemplo, creando videos o audios falsos *deep fake* mediante el uso de la IAG.

De acuerdo con el estudio “Youth Perspectives on Online Safety 2023”, el año pasado, más del 59% de menores de edad reportó haber experimentado un daño potencial en su experiencia en línea, mientras

que de 1 a 3 menores reportaron haber tenido una interacción de índole sexual en Internet (cfr. Thorn, 2024: 12).

La hipótesis de este artículo consiste en demostrar que la protección de nuestros derechos humanos, tanto a nivel normativo como institucional, está volviéndose obsoleta frente al avance imparable de los desarrollos tecnológicos. Estos desarrollos están siendo y seguirán siendo utilizados por empresas, individuos y gobiernos, en ocasiones para la toma de decisiones económicas, de política pública, de seguridad, entre otros; pero en el peor de los escenarios, para discriminar y obtener beneficios económicos ilegales a partir de la información recopilada y a veces manipulada en el mundo digital.

2. El derecho humano a la privacidad

El reconocimiento de los derechos humanos como parte integral de un marco jurídico debidamente positivizado representa uno de los avances más significativos en la historia legal hasta la actualidad. El derecho a la privacidad se encuentra entre los derechos más susceptibles en el contexto de los avances tecnológicos. En la presente investigación, se examinarán las medidas de protección necesarias para asegurar la vigencia de este derecho en un mundo que cada vez adopta más la utilización de la tecnología basada en IA y la IAG, en ocasiones con pleno conocimiento de sus implicaciones para la sociedad y, en muchas otras, sin percatarse de los efectos que acarreará la interacción con este

tipo de tecnología, exponiendo a grupos considerados vulnerables, como niños y adolescentes, a un mayor riesgo.

> *Los niños de hoy integran la primera generación que no ha conocido una época anterior a los teléfonos inteligentes. Constituyen la primera generación cuya atención sanitaria y educación están cada vez más medidas por aplicaciones y dispositivos basados en IA, y algunos de ellos serán los primeros en desplazarse regularmente en vehículos autónomos. También representan la generación que requiere abordar los riesgos ligados a la IA, como la creciente brecha digital, la automatización del trabajo y las violaciones de la privacidad, antes de que estos se consoliden aún más en el futuro. Aunque muchos gobiernos y organizaciones ya están tratando de desarrollar políticas y sistemas de IA centrados en el ser humano, las consideraciones específicas relativas a los niños también deben desempeñar un papel central en el desarrollo de la IA. Esto reviste especial importancia dado que las repercusiones que las tecnologías basadas en la IA pueden tener en los niños no siempre son evidentes* (UNICEF, 2021: 20).

En este sentido, es evidente la necesidad de un nivel más sólido y eficiente de protección de los derechos de la infancia frente a lo que ya está surgiendo con la Inteligencia Artificial en un contexto en el que la interacción con este tipo de tecnología por parte de ese grupo será cada vez más común, sin que los riesgos y efectos puedan considerarse normales desde una perspectiva jurídica, con consecuencias que podrían ser irreversibles.

A pesar de que el reconocimiento de los derechos humanos implicó limitar el poder del Estado, la evolución tecnológica del último siglo ha

alterado el panorama. La defensa de los derechos humanos requiere análisis desde diversas perspectivas de vulnerabilidad y protección, como el derecho a la privacidad y a la información personal, lo que obliga al Estado a salvaguardar al ciudadano ante el poder que están adquiriendo las empresas que crean, utilizan y promueven los avances tecnológicos. Este poder, que en muchas ocasiones está al alcance de cualquier individuo, a menudo implica que las personas, por desconocimiento, ceden sus datos personales.

En México, la reforma constitucional del 10 de junio de 2011 amplió el catálogo de derechos humanos, equiparando en términos de protección aquellos reconocidos en la Constitución Política de los Estados Unidos Mexicanos y todos los instrumentos internacionales en materia de derechos humanos ratificados por el Estado mexicano.

> *Artículo 1. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.*

> *Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.*
>
> *[…]*
>
> *Queda prohibida la discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otro que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas* (Constitución Política de los Estados Unidos Mexicanos, 2024).

Como se puede observar, el primer artículo de la Constitución adopta un enfoque más garantista de los derechos humanos, reconociendo el principio *pro persona*. Además, el último párrafo, que ha sido citado en este artículo, establece la prohibición de la discriminación, proporcionando así una salvaguarda más amplia —que incluso podría abarcar la discriminación derivada de nuestro comportamiento en Internet—, nuestra huella digital y los datos que proporcionamos, los cuales pueden y son empleados para elaborar perfiles sobre nosotros, perfiles que podrían desembocar en la denegación de empleo, acceso a servicios de salud, servicios financieros, entre otros.

Esto implica otorgar la protección más extensa a la persona, incluso en situaciones donde un juez o jueza deba decidir entre la aplicación de dos normas, optando por aquella que ofrezca una mayor protección para la persona. Esta decisión deberá tomarse, naturalmente, desde diversas

perspectivas, como la de género, personas adultas mayores, niñas, niños y adolescentes, migrantes, personas indígenas y personas con algún tipo de discapacidad, todos ellos considerados dentro de los denominados "grupos vulnerables". Ellos requieren una protección más profunda por parte de los legisladores, al crear y aprobar leyes que impactarán directa o indirectectamente en nuestros derechos humanos, así como por parte de los jueces, quienes al momento de dictar una sentencia deben valorar en todo momento elementos que pudieran ser generadores de discriminación, conocidos en términos jurídicos como "categorías sospechosas".

> *Son categorías sospechosas los criterios mencionados en el último párrafo del artículo 1º de la Constitución: el origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas. Y, a su vez, que la norma legal analizada tenga una proyección central sobre los derechos humanos garantizados por la Constitución.*
>
> *Se trata de un examen de proporcionalidad estricto, que se compone de un análisis constitucional de legitimidad, idoneidad, necesidad y proporcionalidad en estricto sentido* (Sánchez, 2017).

Por otro lado, en el artículo 6 de la Carta Magna se establecen una serie de principios para el ejercicio del derecho de acceso a la información, incluyendo a su vez el derecho a la protección de datos personales:

> *Artículo 6. (…)*
>
> *Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*
>
> *II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*
>
> *Artículo 16. 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…*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros* (Constitución Política de los Estados Unidos Mexicanos, 2024).

Se puede observar que la legislación mexicana busca adecuarse a los desafíos contemporáneos, ofreciendo un marco jurídico sólido para proteger la privacidad y los datos personales en un entorno cada vez más digitalizado y, por ende, más propenso a vulnerar los derechos humanos.

A nivel internacional, México ha ratificado instrumentos internacionales vinculantes como la Declaración Universal de Derechos

Humanos de 1948 y el Pacto Internacional de Derechos Civiles y Políticos de 1966, que reconocen el derecho a la privacidad:

> *Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (Declaración Universal de Derechos Humanos, 1948).*
>
> *Artículo 17. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
>
> *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques* (Pacto Internacional de Derechos Civiles y Políticos, 1966).

Adicionalmente, a nivel regional, la Convención Americana sobre Derechos Humanos de 1978, en su artículo 11, protege el derecho a la honra y la dignidad, dos derechos que se han visto especialmente afectados ante el uso indebido de la tecnología comprometiendo los datos personales:

> *Artículo 11. Protección de la honra y de la dignidad.*
>
> *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*
>
> *Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*
>
> *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques* (Convención Americana sobre Derechos Humanos, 1978).

A pesar del reconocimiento global del derecho humano a la privacidad y la obligación del Estado de protegerlo, la evolución tecnológica plantea desafíos, especialmente en el ámbito digital, que carece de un marco normativo adecuado. La creciente autorregulación por parte de las empresas de tecnología, sustituyendo la obligación del Estado de regular esta nueva realidad, presenta aspectos positivos, pero también negativos que requieren de medidas preventivas (cfr. Quijano, 2022).

Diversas resoluciones internacionales, como las de la Organización de las Naciones Unidas (ONU) desde el año 2013, destacan la necesidad de abordar la protección del derecho a la privacidad en la era digital. A pesar de que la evolución tecnológica ha beneficiado a la población mundial, es crucial reconocer que gobiernos, empresas y ciertos sectores de la sociedad llevan a cabo actividades de vigilancia cibernética y recopilación de datos que violan los derechos humanos (cfr. Naciones Unidas, 2014, 1).

La última resolución emitida por la ONU resalta temas importantes como la IA y la recopilación de datos personales, subrayando preocupaciones como:

> *Expresando preocupación porque con frecuencia las personas, en particular los niños, no dan o no pueden dar su consentimiento libre, explícito e informado a la venta o la reventa múltiple de sus datos personales, y que la recopilación, el procesamiento, el uso, el almacenamiento y el intercambio de datos personales, incluidos datos delicados, han aumentado considerablemente en la era digital.*
>
> *Observando que en la observación general núm. 16 del Comité de Derechos Humanos se recomienda que los Estados tomen medidas eficaces para impedir la retención, el procesamiento y el uso ilegales de datos personales almacenados por las autoridades públicas y las empresas.*
>
> *Observando también que el uso de la inteligencia artificial puede contribuir a promover y proteger los derechos humanos y puede llegar a transformar los Gobiernos y las sociedades, los sectores económicos y el mundo del trabajo, y que también puede tener diversas repercusiones de gran alcance, incluso con respecto al derecho a la privacidad* (Naciones Unidas, 2020, 3 y 4).

En este contexto, el derecho a la privacidad enfrenta riesgos constantes debido al referido avance tecnológico. La información compartida en Internet, especialmente por parte de grupos vulnerables —como son niñas, niños y adolescentes—, expone su intimidad, lo que requiere atención especializada y focalizada, como advierte la ONU.

Como señala acertadamente el investigador Miguel Recio Gayo, debemos considerar otro derecho afectado por la dinámica tecnológica, como el derecho al secreto de las comunicaciones, ya que "en muchos casos los usuarios de redes sociales u otros servicios digitales se comunican a través de servicios de mensajería electrónica, correo electrónico u otros servicios que se ponen a su disposición" (Recio, 2022: 19). Al respecto, es importante señalar que la dinámica laboral, social y familiar de las personas se ha transformado y demanda de una comunicación más rápida y eficiente, por lo que la mensajería tipo *WhatsApp*, las conversaciones vía *Zoom* —entre otro tipo de plataformas—, permiten a sus dueños la obtención de datos sobre sus usuarios, datos que transformarán en beneficios económicos, o incluso en algún otro fin de legalidad cuestionable.

A nivel nacional, México reconoce constitucionalmente el derecho a la privacidad, y además cuenta con dos leyes secundarias en materia de protección de datos personales: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (publicada en 2010) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (publicada en 2017). Esta última regula la protección de datos personales en el sector público a nivel federal, mientras que cada entidad federativa cuenta con su propia legislación para proteger los datos personales en el ámbito gubernamental.

Además del marco jurídico específico mencionado, las resoluciones de la Suprema Corte de Justicia de la Nación han contribuido a establecer una protección más amplio al detallar los alcances del derecho a la

privacidad derivado de la Constitución Política de los Estados Unidos Mexicanos y los instrumentos internacionales ratificados por México.

Si bien el derecho a la privacidad ha enfrentado desafíos a lo largo de la historia, el Internet se ha convertido en un instrumento que permitió un acceso más rápido e intrusivo en la vida privada, en ocasiones con el consentimiento de la persona afectada, pero también mediante intromisiones ilegales.

> *la privacidad de los usuarios de Internet es parte de las políticas públicas de diversas organizaciones internacionales de las que México es parte; como por ejemplo, la Organización para la Cooperación y el Desarrollo Económico (OCDE), que ha elaborado importantes directrices y documentos relativos a políticas públicas objeto de varios instrumentos internacionales, tales como la Carta de Derechos Humanos y Principios para Internet elaborada en el seno de la Coalición por los Derechos y Principios de Internet (en inglés, Internet Rights and Principles Coalition) y que es parte del Foro para la Gobernanza de Internet de las Naciones Unidas; así como la Guía de los Derechos Humanos para los usuarios de Internet aprobada por el Consejo de Europa a través de la Recomendación del Consejo de Ministros a los Estados miembros sobre una Guía de los derechos humanos para los usuarios de Internet* (Piñar y Recio, 2016, 39).

A pesar de estos avances, hemos sido testigos de la vulnerabilidad del derecho a la privacidad, particularmente en un entorno político y económico donde la información obtenida a través de Internet se convierte en un recurso valioso, equiparable al petróleo en términos económicos.

> *En 2020 la Universitat Oberta de Catalunya publicó un interesante artículo sobre el comercio de datos personales en Internet. Según este texto, los datos personales con los que cuentan las plataformas y redes sociales que usamos tienen un valor cuantificable. Lo pusieron de manifiesto operaciones como la que llevó a cabo hace cinco años Facebook, cuando compró la aplicación WhatsApp por más de 21.800 millones de dólares* (Albarrán, 2023).

El comercio de datos personales ha sido una constante en las distintas plataformas, como se observa en el caso de *WhatsApp* y *Facebook*. WhatsApp, una empresa dominante en el mercado de mensajería instantánea, compartió datos personales de sus usuarios con la plataforma de Facebook. Ante esta situación, Argentina decidió dictar medidas cautelares mientras se analizaba el uso que Facebook daría a los datos compartidos por WhatsApp.

> *Entre los datos se encuentran: el acceso a la libreta de direcciones, número de teléfono, datos de operaciones (por ejemplo, si se usa Facebook Pay o Tiendas en WhatsApp), información relacionada con el servicio, información sobre interacción con las empresas cuando se usa el servicio, información sobre el dispositivo móvil y la dirección IP* (Secretaría de Coordinación de Producción, 2021).

Esta comercialización de datos personales, aunque lucrativa, conlleva una intrusión en la privacidad y puede resultar en violaciones al derecho al honor, a la imagen y otros derechos, como se evidenció en el caso de Edward Snowden, que reveló el alcance del espionaje gubernamental, permitiendo un acceso no autorizado a conversaciones, imágenes y

demás información digital y no digital de las personas, misma que llega a comprometer su vida personal en todos los ámbitos.

Como señala Carissa Véliz de manera muy acertada:

> *La privacidad es la llave que abre la cerradura de tus aspectos más íntimos y personales, aquellos que te hacen más tú, y más vulnerable. Tu cuerpo desnudo. Tus fantasías y experiencias sexuales. Tus enfermedades pasadas y presentes, y aquellas que podrías tener en el futuro. Tus miedos, pérdidas y fracasos. Lo peor que hayas hecho, dicho o pensado nunca. Tus debilidades, errores y traumas. El momento en el que más vergüenza hayas pasado. Ese familiar que desearías no tener. La noche de tu peor borrachera* (Véliz, 2022, 61).

Aunque Internet ha transformado el mundo en múltiples aspectos, incluyendo el económico, político y social, también ha dado lugar a la llamada violencia digital, donde la violencia verbal, psicológica se traslada al ámbito virtual, impactando profundamente en la privacidad y la intimidad de las personas. Es importante comprender que la interacción que tenemos con cualquier dispositivo que se conecte a Internet, puede convertirse en un arma en nuestra contra.

Cuando surgieron las redes sociales a través de Internet, en un contexto digital y legal con lagunas normativas, fronteras poco claras y ausencia de personal especializado para atender esta situación, así como de recursos materiales, se generó un clima de impunidad donde las violaciones a la privacidad se volvieron frecuentes y normalizadas, teniendo como principal factor el anonimato que permite la interacción en dichas redes.

En este sentido, es esencial establecer mecanismos efectivos para sancionar estas conductas y garantizar la protección de la privacidad en un mundo donde nuestra huella digital perdura indefinidamente. Es necesario comprender que, al compartir nuestras debilidades, nuestros miedos, estamos permitiendo que aquellas personas que tengan acceso a dicha información tengan el poder de generarnos algún daño que puede tener un impacto a corto, mediano o largo plazo en todos los ámbitos en los que interactuamos.

La responsabilidad compartida de proteger la privacidad recae tanto en el Estado y en la sociedad como en las empresas. Es crucial promover una cultura de respeto hacia la privacidad y otros derechos, así como fomentar una navegación responsable en Internet.

3. La huella digital en Internet

El derecho a la privacidad se ve comprometido en su eficacia debido a la huella digital que los usuarios de Internet van dejando, tanto de manera directa como indirecta, lo cual impacta en diversos aspectos de la vida diaria, desde lo más básico hasta lo más íntimo.

En términos sencillos, la huella digital representa el rastro que dejamos en la red a través de nuestras actividades en línea, búsquedas en la web, participación en redes sociales y otros aspectos que pueden ser utilizados en nuestra contra en situaciones relacionadas con empleo, servicios, becas, créditos bancarios, asuntos migratorios y otros contextos, tanto públicos como privados.

> *Otros datos que pueden formar parte de la huella digital son: la dirección IP* (Internet Protocole) *del dispositivo usado para la conexión; el tipo de navegador; la ubicación geográfica del equipo; el idioma; y el sistema operativo.*
>
> *En ocasiones, también contiene información personal como datos de inicio de sesión; nombre; dirección de correo electrónico; número telefónico; historial de navegación; perfiles en redes sociales; fotos; subscripciones a* blogs *y comentarios en foros* (Justicia digital, 2023).

La situación de riesgo asociada con la huella digital se ha visto notablemente alterada por la pandemia de COVID-19, en el sentido de que ha provocado cambios significativos en nuestros hábitos de vida tanto en el mundo físico como en el virtual. La vida en línea engloba todas las actividades realizadas mediante dispositivos electrónicos, desde teléfonos móviles, computadoras y tabletas hasta electrodomésticos inteligentes y vehículos con tecnología avanzada. Cada interacción en la red, como un "me gusta", un clic en un sitio web o una compra en línea, contribuye a la generación de datos que, con la evolución del *Big Data*, ayudan a definir nuestra identidad digital, también conocida como huella digital o "identidad 2.0".

> *La "identidad digital", también conocida como "identidad 2.0", es la versión en Internet de la identidad física de una persona. Está compuesta por millones de datos que proporcionamos en la red, más allá de nuestro e-mail y dirección, que incluye fotos, datos bancarios y preferencias de consumo. Esta ID 2.0 es lo que somos en la red, y por eso, es importante siempre saber qué se dice sobre nosotros, dónde y por qué, tanto hacia nuestra persona como para nuestra organización.*
>
> *Esta ID 2.0 a lo largo del tiempo deviene en una verdadera "huella digital", que se construye por las interacciones de la propia persona y también por terceros sin el consentimiento o la plena conciencia del proceso. Cuanto más publiquemos, más identidad creamos y más fuerte será la presencia de la misma para orientar a los algoritmos* (Campos, 2021).

En el mejor de los casos, nuestra huella o identidad digital nos convierte en un producto y en un objetivo publicitario específico, lo que permite comprender mejor a la población en diversos ámbitos, ya sea con fines económicos, políticos, sociales o, desafortunadamente, delictivos. En el peor de los escenarios, esta huella digital puede ser utilizada para discriminar, extorsionar o incluso para que nuestra información personal termine en la denominada *deep web*.

Es importante destacar que la *deep web* no se limita únicamente a actividades ilícitas, sino que también ha servido como un medio para la navegación en Internet en países con regímenes autoritarios, para realizar transacciones económicas mediante criptomonedas como *bitcoin* y su tecnología de *blockchain,* así como para resguardar información gubernamental sensible en temas de seguridad, entre otras funciones (cfr. Nares, 2018).

Un ejemplo reciente sobre el uso de nuestra información por parte de los gobiernos lo encontramos en la resolución de la Corte Interamericana de Derechos Humanos (Corte IDH) en el asunto "Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs. Colombia", resolviendo condenar al Estado colombiano por violaciones a los derechos humanos del mencionado colectivo de abogados. Estas violaciones incluyeron la elaboración de perfiles mediante actividades de inteligencia y el intercambio de información recopilada con grupos paramilitares, lo cual afectó la integridad de esos abogados y violentó —entre otros derechos— el derecho a la autodeterminación informativa reconocido en la Convención Americana sobre Derechos Humanos, "que incluye el derecho a acceder y controlar los datos de carácter personal que obren en archivos públicos. En tal sentido, según se indicó en la Sentencia, el actuar estatal configuró la vulneración de dicho derecho" (Corte IDH, 2024, 1).

Este caso es solo uno de muchos que han ocurrido y seguirán sucediendo mientras la sociedad siga pasiva ante estas invasiones a la privacidad, tanto por parte del sector público como del privado. Es responsabilidad de todos involucrarse y hacer valer los límites normativos a estos abusos, en beneficio propio y de la sociedad.

En lo que respecta a la tecnología y nuestra interacción con ella, es fundamental considerar su uso adecuado o inadecuado, especialmente cuando se trata de menores de edad, que son un grupo especialmente vulnerable en este ámbito. La falta de conciencia sobre este tema puede conducir a situaciones en las que las imágenes compartidas en Internet

se utilicen en contra nuestra o aparecen en ellas. Es importante recordar que no tenemos un control absoluto sobre la información que se comparte sobre nosotros en Internet. Muchas personas subestiman el potencial uso de la información que comparten, incluso elementos aparentemente simples como reuniones familiares, vacaciones, la escuela de sus hijos, estilos de vida que brinden un sentido de pertenencia social, o incluso algo tan sutil como un emoticono, que a través del análisis de datos permite identificar estados de ánimo para fines publicitarios o manipulativos en decisiones políticas, como se evidenció en el caso "Cambridge Analytica y Facebook" en las elecciones presidenciales de Estados Unidos en 2018, donde se buscaba favorecer al candidato y posterior presidente, Donald Trump.

La destacada situación que ilustra la vulnerabilidad de nuestra información se manifestó en el caso mencionado de la siguiente manera:

> *En 2013 un profesor de la Universidad de Cambridge llamado Aleksandr Kogan desarrolló —como un proyecto personal ajeno a la universidad— un test que proponía a los usuarios descubrir su personalidad.*
>
> *Cuando un usuario quería hacer la prueba llamada "thisisyourdigitallife" ("estaestuvidadigital", en español), la app solicitaba permisos para acceder a su información personal y también a la de su red de amigos.*

> *De esta forma, los individuos que hacían el test y aceptaban las condiciones para ello estaban proporcionando todos sus datos al desarrollador de la app, al que, a la vez, le permitían recolectar la información de todos sus contactos.*
>
> *Unas 265.000 personas accedieron al test desarrollado por Kogan. Lo que, sumando la red de amigos de cada uno de estos usuarios, le permitió acceder a "unos 50 o 60 millones de perfiles de Facebook en dos o tres meses", según Wylie.*
>
> *Entre la información que recabó la app se encuentra la información personal de los perfiles, actualizaciones de estado, "me gusta" y "en algunos casos, mensajes privados".*
>
> *Ello, según le dijo Wylie a The Guardian, le permitió a Cambridge Analytica conocer a qué tipo de mensaje iba a ser susceptible cada usuario para tratar de influir en su forma de pensar, así como el contenido, el tema y el tono que debían usar en cada caso* (BBC Mundo, 2018).

El progreso tecnológico nos ha convertido en un objeto deseable tanto para empresas como para individuos sin escrúpulos que buscan beneficiarse dañando a otros, sin importar si son niños o personas adultas. Esta evolución nos sitúa como el producto a consumir, ya que todas nuestras acciones generan datos que, debidamente analizados, pueden convertirse en negocios multimillonarios y ser utilizados para influir en nuestras decisiones políticas, económicas y sociales. El caso "Cambridge Analytica" también reveló que no solo los datos personales de quienes decidieron participar en el *test* fueron objeto de tratamiento ilegal, sino también los de los contactos de esas personas, comprometiendo así la privacidad de terceros, por ello es crucial

comprender lo que implica nuestra huella digital, principalmente sus alcances desde el punto de vista negativo. Situaciones como las listas negras en juicios laborales en México subrayan la importancia de hacer valer nuestros derechos de acceso, rectificación, cancelación, oposición y portabilidad (o "Derechos ARCOP"), para combatir la discriminación como es el caso de la discriminación laboral. Este tipo de acontecimientos, como el de "Cambridge Analytica", nos llevan a reflexionar sobre nuestra identidad digital y su impacto en nuestros derechos humanos, dado que la identidad digital contribuye a forjar una reputación en línea. Sin embargo, esta reputación digital no siempre refleja con precisión quiénes somos, ya que en ocasiones está manipulada por la imagen que terceros proyectan sobre nosotros, pudiendo ser en algunas ocasiones favorecedora, pero en muchos casos difamatoria y con la intención de causar daño de manera deliberada (cfr. López, 2022).

En la presente era digital, nuestra presencia en línea trasciende más allá de meros datos identificativos o una simple imagen de perfil en redes sociales. La identidad digital se ha convertido en un complejo mosaico que refleja nuestra interacción en Internet. En este contexto, surgen desafíos cruciales para la gestión de la identidad digital. Entre ellos, destaca la necesidad de abordar la privacidad y seguridad de nuestros datos personales, considerando las posibles amenazas como la suplantación de identidad, fraudes, extorsiones y secuestros. Otro desafío crucial es el acoso cibernético, que a menudo afecta a los menores de edad y a las mujeres, siendo ejemplificado por reformas legales como la denominada "Ley Olimpia", que condujo a una serie de

reformas para prevenir y combatir la violencia digital hacia las mujeres, modificando la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y el Código Penal Federal. Además, resulta crucial afrontar el descontrol sobre la información que circula en línea sobre nosotros, dado que una vez difundida en Internet, perdemos el dominio sobre el alcance global, como lo evidenció la necesidad de ajustes normativos en México con la "Ley Ingrid", que modificó nuevamente el Código Penal Federal para sancionar "los delitos contra la administración de justicia cometidos por servidores públicos, particularmente a los funcionarios que filtren imágenes de víctimas de violencia" (Sánchez, 2023).

> *este cambio en la forma y medios de informarse implica un gran reto y responsabilidad para la sociedad contemporánea: la instantaneidad de la información, la falta de un control previo y efectivo y la multiplicidad de emisores de información, la mayoría de ellos no periodísticos. Estos desafíos se han cristalizado en una serie de problemáticas, entre las que se destacan la difusión de las fake news, noticias falsas creadas con fines políticos, económicos y humorísticos, enviadas a través de las redes sociales y compartidas por sus lectores, quienes las consideran erróneamente verídicas. Por tanto, existen actualmente problemáticas a la hora de controlar las noticias falsas, lo que ha generado que estas sean utilizadas con fines electorales, arruinando campañas electorales de candidatos o deteriorando la imagen pública de políticos y gestores* (Lazer et al., 2018 en Pineda et al., 2020).

Ante este panorama, las noticias falsas no solo desinforman sobre temas de interés general, sino que también se emplean para dañar la imagen y reputación de personas, incluso recurriendo al uso de IAG. Un

ejemplo es el caso de la cantante estadounidense Taylor Swift, quien fue víctima de violencia digital mediante la manipulación de imágenes generadas por IA que la mostraban desnuda en escenarios ficticios, siendo ampliamente compartidas en redes sociales con la intención de difamarla. En este caso, se informó que "millones de internautas se han topado en los últimos días con imágenes falsas donde Swift aparece completamente desnuda en diferentes escenarios, todos ellos vinculados al equipo de futbol americano de los Kansas City Chiefs, del cual Travis Kelce —novio de la cantante nacida en Pensilvania— es una de las máximas estrellas" (Calle, 2024). Este incidente subraya la urgencia de abordar los desafíos éticos y legales asociados con la proliferación de contenido falso en el entorno digital actual. El caso de Taylor Swift ilustra claramente un ejemplo de violencia digital que vulnera la dignidad y el derecho al honor. Además, hay casos que han sido llevados a juicio por discriminación generada a partir de algoritmos que determinan el tipo de anuncios publicitarios en plataformas y a qué segmento de clientes se dirigen. Estos anuncios se crean con sesgos derivados de la información que compartimos en nuestros perfiles de redes sociales —como nuestra raza, género, edad, ocupación o estado civil—, acompañados de la idiosincrasia de los programadores de los algoritmos, lo que deriva en que sean utilizados de manera discriminatoria hacia los usuarios. Un caso destacado de esta problemática se evidencia en la publicidad de plataformas como *Facebook*:

> *Cuando Neutah Opiontennione, una residente de Washington DC de 54 años, descubrió que Facebook le ocultaba algunos anuncios sobre productos financieros por ser una mujer mayor, decidió que debía hacer algo al respecto. El pasado mes de octubre, Opiotennione se unió a otros usuarios de la red social para presentar una demanda colectiva por la discriminación que sufren debido a la herramienta de anuncios que utiliza la plataforma.*
>
> *Los demandantes afirman que Facebook permite a los anunciantes discriminar por edad y género a la hora de ofrecer publicidad de ciertos servicios financieros, tales como cuentas bancarias, seguros, inversiones o préstamos, ya que este tipo de anuncios no le aparecen a mujeres y personas mayores con la misma frecuencia que al resto de los usuarios. Según la demanda, Facebook persiste en este tipo de discriminación, a pesar de que la compañía aseguró hace unos meses que tomaría medidas al respecto.*
>
> *No es la primera vez que la red social es criticada por este motivo. El pasado mes de marzo, el Gobierno federal acusó a la compañía por discriminación en la publicidad relacionada con la vivienda. "Facebook está discriminando a las personas en base a quiénes son y dónde viven", aseguró el secretario del Departamento de Vivienda y Desarrollo Urbano, Ben Carson, en un comunicado* (Pinto, 2019).

Este caso nos muestra apenas la punta del *iceberg* de las consecuencias de no ser conscientes de nuestra huella digital, especialmente en el perfil que construimos sobre nosotros en contextos sociales y profesionales (por ejemplo, en plataformas como *LinkedIn*). La falta de control y el desconocimiento sobre el impacto que pueden tener nuestras acciones y palabras en el mundo virtual, con repercusiones en

el mundo real, pueden tener consecuencias diversas como lo hemos referido en el presente artículo.

Esto plantea un desafío adicional para naciones como México, donde aún no se reconocen derechos como el derecho al olvido en Internet, a diferencia de lo que ocurre en la Unión Europea, donde se ha delineado una especie de frontera digital para definir la competencia legal en casos de afectación por información personal o profesional compartida en línea que ya no se considere de interés público y cuya permanencia en los motores de búsqueda de Internet cause un perjuicio mayor que el beneficio de tener conocimiento sobre dicho evento, como ocurrió en el caso de Mario Costeja en 2014 (caso "Costeja"), el cual marcó el inicio del derecho al olvido en Internet. Según Verónica Alarcón, "dice que reciben solicitudes de este tipo a diario y que acumulan miles desde sus inicios en 2010. Google ha recibido peticiones para retirar más de 4 millones de enlaces y ha quitado hasta el momento 1.642.170, según su último informe de transparencia" (Alarcón en Gonzalo, 2021).

La sentencia que dictó el Tribunal de Justicia de la Unión Europea para el caso "Costeja" permitió comprender la importancia del derecho al olvido en Internet, al señalar "que la actividad de los motores de búsqueda es diferente e independiente a la que realizan los editores de las páginas *web* indexadas y tiene un efecto "multiplicador", que puede causar daño adicional y distinto al que pueden ocasionar las publicaciones hechas en las páginas originales" (Quijano, 2022, 181).

En el caso de México, lo más cercano al derecho al olvido en Internet, judicialmente hablando, es el que involucró a un abogado que demandó

al motor de búsqueda Google. El abogado resultó favorecido en la sentencia de un juicio que tardó ocho años en concluirse, condenando a Google a pagar 5.000 millones de pesos mexicanos (cfr. Expansión, 2023).

4. Derecho a la protección de datos personales en Internet

A lo largo del presente artículo, hemos explorado la relación entre la privacidad y la protección de datos personales, derechos que se han visto infringidos debido al avance tecnológico sin una regulación ética y de derechos humanos adecuada. Es imperativo avanzar hacia una normativa específica para el entorno digital, donde gran parte de nuestra vida cotidiana —incluyendo aspectos laborales, educativos, sociales, políticos, comerciales, financieros, de salud y de prestación de servicios públicos— tiene lugar en la actualidad.

La mayoría de los trámites administrativos se realizan inicialmente a través de páginas web o de aplicaciones móviles, desde la obtención de pasaportes y visas de entrada para algún país, hasta la contratación de servicios financieros o de entretenimiento.

La legislación actual en materia de protección de datos personales obliga tanto al sector público como al privado a tomar medidas que garanticen el adecuado tratamiento de la información personal, situación cada vez más compleja dada la evolución tecnológica y los riesgos asociados. Esta legislación establece principios fundamentales, como la licitud, consentimiento, información, calidad, finalidad, lealtad,

proporcionalidad y responsabilidad, los cuales deben ser observados para garantizar el tratamiento adecuado de los datos personales.

En el caso específico de México, el consentimiento debe obtenerse de manera expresa, principalmente aplicable al tratamiento de datos personales considerados sensibles, como los relacionados con la salud, los financieros, datos biométricos o aquellos que puedan ser utilizados para realizar una perfilación del titular de los datos personales. Por otro lado, el consentimiento tácito se aplica cuando no se requiere una manifestación expresa, siendo suficiente con que el titular no se oponga al tratamiento. Este último tipo de consentimiento es común en los servicios en línea, aunque en algunos casos se puede encontrar un consentimiento expreso forzado, donde se condiciona la prestación del servicio a la aceptación de ciertos tratamientos de datos, sin posibilidad de oponerse inicialmente. En estas situaciones, se nos impulsa a ejercer nuestro derecho de oposición o cancelación para limitar o negar la continuidad en el tratamiento de nuestros datos personales.

La legislación en materia de protección de datos vigente en México ha sido considerada por propios Comisionados que integran el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como obsoleta ante los desafíos que representan los avances tecnológicos, debiendo tener presente que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares no ha sido objeto de reformas desde su promulgación en 2010 (cfr. Román, 2024).

La situación actual en Internet y en cualquier servicio que requiera la entrega de datos personales plantea desafíos. A pesar de la obligación de contar con un aviso de privacidad y de limitar la solicitud de datos a lo estrictamente necesario, existe una falta de cultura en revisar estos avisos, resaltando que no todos los sujetos obligados cuentan con dicho documento. En ocasiones, la extensión y redacción de estos pueden ser estrategias para evitar su lectura, lo que lleva a que las personas acepten el tratamiento de sus datos sin comprender completamente su finalidad, o bien, se condicione el servicio a la entrega de datos que no son necesarios para su prestación.

Esta problemática se agrava en las redes sociales, donde compartimos información personal creyendo estar seguros. Aunque mostramos ciertos niveles de confianza en línea, es paradójico que aceptemos a desconocidos en nuestras redes sociales, incluso sin conocerlos, con el fin de aparentar cierta popularidad, situación que en nuestra vida real no realizamos con tanta facilidad, particularmente compartir información personal con extraños que nos encontramos en la calle.

Además de lo mencionado, existen otras obligaciones para estos dos sectores en el tratamiento de los datos personales, entre los cuales está la de informar sobre las medidas de seguridad implementadas para proteger nuestra información, lo cual requiere de una considerable inversión económica y de recursos humanos especializados para asegurar que los sistemas estén debidamente actualizados y para

reducir significativamente las vulnerabilidades a robos cibernéticos de datos personales, tal como ya ha sucedido.

Las vulnerabilidades mencionadas representan un gran riesgo para la sociedad y, en consecuencia, para los gobiernos. Recientemente, en México se ha registrado el robo de datos personales de periodistas que asisten a las conferencias de prensa conocidas como “Mañaneras”, llevadas a cabo por el Presidente de la República. Algunos de estos periodistas son considerados incómodos o incluso adversarios para el Gobierno debido a sus preguntas críticas. Es importante destacar que México es uno de los países más peligrosos para los periodistas, quienes enfrentan amenazas, desapariciones, secuestros y homicidios. Esta situación pone en peligro la integridad de los periodistas y de sus familias, y hasta el momento no se conocen las medidas tomadas por el gobierno para proteger a los afectados.

Para atender este tipo de situaciones, México cuenta con un organismo constitucional autónomo denominado INAI. Este organismo tiene la responsabilidad de garantizar la eficacia y protección de derechos fundamentales como el derecho a la información, el derecho a la libertad de expresión, el derecho a la privacidad y el derecho a la protección de datos personales. Es crucial que el INAI cuente con la autonomía necesaria para cumplir con su función según lo establecido en la propia Constitución Política de los Estados Unidos Mexicanos.

En este sentido, ante el caso de vulneración de datos personales de periodistas, el denominado INAI abrió una investigación al respecto:

> *El Instituto Nacional de Transparencia y Protección de Datos Personales (INAI), inició un análisis técnico sobre la eventual filtración de los datos de más de 300 periodistas que cubren las conferencias matutinas del presidente Andrés Manuel López Obrador.*
>
> *A través de su cuenta de X, aclaró que como garante de la protección de datos personales, cualquier transgresión a principios, deberes y derechos consagrados en la Ley General en la materia será investigada y resuelta conforme a sus atribuciones y al amparo de la ley.*
>
> *La organización Artículo 19 solicitó al Gobierno de la República clarificar cuáles fueron las medidas que tomó para evitar la vulneración de los datos personales que recolectó y cuáles serán las acciones preventivas para evitar que se cometan daños con esa información* (Vallejo, 2024).

Como se puede observar, existe una alta vulnerabilidad en cuanto a la protección de datos personales. En el caso mencionado, nos enfrentamos a una filtración en los sistemas de la Presidencia de la República, área estratégica del Gobierno Federal que debería contar con un sistema de mayor control en materia de ciberseguridad, considerando la naturaleza de la información que almacenan estos sistemas y su relevancia para la seguridad nacional. Esta problemática se extiende también al ámbito privado y personal, donde muchas personas no tienen la disciplina de contratar servicios de protección cibernética, como los antivirus, que también protegen contra el denominado phishing.

De acuerdo con medios informativos, “México fue el objetivo del 66 por ciento de los ciberataques dirigidos en América Latina, los cuales causaron daños que se estiman entre hasta por 5 mil millones de

dólares; a pesar de ello al menos 36 por ciento de los mexicanos no usan antivirus" (Calderón, 2023).

Este panorama hace necesario repensar nuestra interacción en Internet y ser conscientes de los riesgos asociados. Es fundamental considerar que nuestras acciones en línea pueden tener consecuencias jurídicas tanto para nosotros como para terceros. Es necesario promover una cultura de protección de datos personales y utilizar responsablemente todos los dispositivos electrónicos, especialmente en un entorno donde la tecnología, como la Inteligencia Artificial Generativa, está en constante evolución y puede causar daños irreparables si se utiliza incorrectamente. La Unión Europea ya dio los primeros pasos para una regulación en materia de Inteligencia Artificial (cfr. Kaplan, 2024), labor que deberán realizar a la brevedad los demás países para no dejar desprotegidos a sus ciudadanos e incluso desprotegidos los propios sistemas del Estado.

Ante este escenario es evidente la necesidad de reformar nuestro marco legal para adaptarlo a una realidad donde la interacción virtual es cada vez más frecuente. Un estudio realizado por la Universidad Nacional Autónoma de México reveló que "los mexicanos destinan una cuarta parte del día —aproximadamente seis horas— al entretenimiento en redes sociodigitales, además, debido a ellos prefieren informarse por medio de estas plataformas" (EFE, 2023), a su vez, el investigar de la Universidad Nacional Autónoma de México, Luis Ángel Hurtado Razo señaló que "con el avance tecnológico han surgido las redes sociodigitales o social 'network', que ocurren en un espacio público

digital, en el cual interactuamos con otros "y al hacerlo modificamos nuestro comportamiento, que pueda ser para beneficio o perjuicio de la comunidad" (EFE, 2023).

La cuestión a analizar no debe limitarse al tiempo que pasamos en línea, sino a cómo interactuamos y qué información compartimos. Cada clic deja una huella digital, lo que nos obliga a repensar nuestra relación con la tecnología y promover una cultura de protección de datos personales en todos los ámbitos de nuestra vida en línea. Esta información está inicialmente al alcance de plataformas como Google, que la utilizan para consolidar su posición dominante como motor de búsqueda (cfr. Hovenkamp, 2021: 1962).

Como acertadamente señala Marta Gracia, "Google tiene toda la información y es capaz de saber dónde dormimos, donde trabajamos, dónde comemos… "y somos nosotros los que le damos esa información sin ningún tipo de pudor". Los usuarios le han dado los datos a cambio de unos servicios y productos gratuitos, aunque "hay que plantearse que si algo es gratis, tú eres el producto" (Gracia, 2022).

En efecto, según el estudio "Antitrust and platform monopoly", Google Search controla el 90% de las búsquedas en Internet (cfr. Hovenkamp, 2021, 1963). Esta plataforma obtiene la mayor parte de sus ingresos a través de sus servicios publicitarios, los cuales se basan en gran medida en la información que los usuarios proporcionan al interactuar con las plataformas. La huella digital de los usuarios se convierte en un instrumento crucial para personalizar los anuncios

publicitarios, generando un interés manipulado en los usuarios mediante la explotación de sus datos personales.

La dominancia de Google como motor de búsqueda quedó demostrada en una sentencia emitida por un juez federal de los Estados Unidos de Norteamérica. En la decisión, se argumenta lo siguiente: “después de haber considerado cuidadosamente y valorado el testimonio del testigo y la evidencia, la Corte llegó a la siguiente conclusión: Google es un monopolio, y ha actuado como uno para mantener dicho monopolio”, “esto ha violado la sección 2 del Sherman Act.” (Feiner, 2024) (traducción propia).

Otro ejemplo que ilustra la fragilidad de la seguridad de nuestros datos personales y de nuestra privacidad se encuentra en la empresa *Tik Tok*, la cual ha sido objeto de acusaciones de espionaje por parte del gobierno chino, como se evidenció en Estados Unidos:

> *en Estados Unidos, le han dado un plazo a la red social para que "venda" y se separe de su empresa matriz china, si es que quiere continuar operando en el país, ello porque el gobierno estadounidense afirma que la empresa ByteDance está bajo control del gobierno chino, lo cual no solo irrumpe en las políticas de privacidad para los usuarios del vecino del norte, sino que significa un riesgo a su seguridad nacional por un posible proceso de espionaje. Sin embargo, existen otros estudios que mencionan que Tik Tok no es la única red social en recopilar nuestra información privada. Citizen Lab encontró que otras redes sociales guardan el mismo tipo de información como parte del rastro y seguimiento del comportamiento de los usuarios* (Del Río, 2023).

El 13 de marzo de 2024, la Cámara de Representantes de Estados Unidos presentó y aprobó un proyecto de Ley mediante el cual se prohíbe el uso de la plataforma *TikTok* en ese país. "El proyecto de ley prohibiría a *TikTok* en las tiendas de aplicaciones de EE.UU. a menos que la plataforma de redes sociales, utilizada por aproximadamente 170 millones de estadounidenses, se escinda de su empresa matriz china, *ByteDance*" (Foran, Fung, et.al, 2024).

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ha alertado a la sociedad sobre los riesgos que representa el uso de la plataforma *TikTok*, especialmente después de que la propia plataforma admitiera que estaba utilizando su tecnología para fines de espionaje, como en el caso de 2 periodistas de origen estadounidense y empleados de la plataforma (cfr. Del Río, 2023). El Instituto ha buscado sancionar a esta red social, y aunque *TikTok* buscó obtener un amparo contra el INAI, un juez de distrito le negó el amparo

al considerar que no existe una afectación derivada de la investigación ordenada por el INAI para detectar si la empresa estaba vulnerando los datos personales de sus usuarios (cfr. Lastiri, 2022).

La protección de nuestra identidad, imagen, honor, privacidad y seguridad, así como la de las demás personas, es un asunto que requiere la colaboración y responsabilidad de toda la sociedad para crear un entorno digital más seguro, especialmente cuando se trata de proteger a los menores de edad. Estos niños ya tienen una huella digital desde muy temprana edad, ya que sus padres, familiares o amigos suben sus primeras fotografías y videos a Internet, perdiendo el control sobre esa información. Esto los hace aún más vulnerables a situaciones como la extorsión o el secuestro, entre otras amenazas que pueden afectar su vida personal y laboral.

Además, la protección de datos debe extenderse incluso a las personas fallecidas. Recientemente, la Suprema Corte de Justicia de la Nación en México (SCJN) resolvió en el sentido del derecho de cancelación de datos personales de una persona fallecida. “Destacó que la Constitución Federal y los tratados internacionales consagran la protección de datos para garantizar el control sobre su información personal, siendo su fundamento: (i) el desarrollo de su autonomía personal; (ii) prevenir daños patrimoniales y morales; y, (iii) el justo y equitativo desarrollo de las relaciones de consumo” (SCJN, 2022). Esto cobra especial relevancia en el contexto del uso de la IAG, e incluso del Metaverso, como en los casos en China donde se utilizan datos personales, como la voz y rostro de una persona fallecida, para crear

avatares que permitan a los familiares conectarse de alguna forma con sus seres queridos fallecidos, “en un apacible cementerio del este de China, Seakoo Wu saca su teléfono, lo coloca sobre la lápida de la tumba de su hijo y mira un video donde aparece el joven fallecido…Agobiados por el dolor, Wu y su esposa se unieron al creciente número de chinos que recurren a la tecnología de IA para crear avatares de sus deudos.” (Taizhou, 2023), esperando que con los avances que se vayan logrando en el metaverso, podamos tener una vida virtual más inmersiva, sin conocer hasta el momento el impacto que tendrá en nuestra privacidad y en nuestros datos personales.

En este sentido, hemos podido examinar la relevancia de nuestra interacción en línea para poder regular, en cierta medida, nuestra privacidad. Resulta esencial contar con organismos sólidos y autónomos que salvaguarden prerrogativas como la protección de los datos personales, el derecho a la autodeterminación informativa y otros derechos que deben emerger para proteger nuestra identidad en esta nueva era digital cada vez más integrada con nuestra vida cotidiana.

5. Conclusiones

Todo lo analizado nos obliga a reconsiderar nuestra interacción diaria, especialmente en el ámbito digital. En la actualidad, nuestra vida está intrínsecamente ligada a la web, ya sea a través de dispositivos como teléfonos móviles, *smart watches*, *smart tvs* y otros dispositivos domésticos conectados a Internet, que permiten a los fabricantes

recopilar cada vez más información sobre nosotros. Desde nuestros hábitos de consumo hasta nuestro estado de salud y actividad diaria, toda esta información se convierte en datos susceptibles de comercialización. En otras palabras, nos hemos convertido en productos para ser consumidos, y la búsqueda de datos para la perfilación de los usuarios es incansable y, en algunos casos, ilegal y éticamente cuestionable.

Hoy en día, la importancia de mantener una huella digital lo más discreta posible es crucial para cualquier actividad que deseemos emprender. Ya sea buscar empleo, solicitar un préstamo bancario o una visa de viaje o trabajo, todas estas acciones pueden verse condicionadas por nuestra presencia en la web. A pesar de que el derecho a la libertad de expresión está garantizado en instrumentos internacionales y constituciones, la realidad es que las personas o algoritmos que revisan nuestros perfiles en línea pueden formar opiniones subjetivas y discriminatorias sobre nosotros basadas en nuestra actividad en redes sociales, o incluso en la información proporcionada por dispositivos como relojes inteligentes, que registran datos sobre nuestros hábitos de ejercicio, sueño, presión arterial, niveles de oxígeno y otros aspectos. Estos datos, cada vez más numerosos, son buscados por las compañías de seguros, entre otros, para condicionar la venta de sus servicios.

En este sentido, hemos observado cómo los derechos a la privacidad y a la protección de datos personales se ven afectados por nuestra huella digital, lo que termina impactando en el nivel de privacidad que podemos disfrutar y en cómo se manejan nuestros datos personales.

Los gobiernos ya no pueden depender únicamente de la autorregulación por parte de las empresas tecnológicas. Deben asumir su responsabilidad como garantes de los derechos humanos para prevenir y eliminar cualquier práctica que pueda poner en peligro estos derechos, no solo los mencionados anteriormente, sino todos los derechos reconocidos, ya que la vulneración de uno puede conducir a la violación de otro.

Derivado de todo lo analizado en el presente artículo, podemos afirmar que la hipótesis planteada se confirma en el sentido de que los algoritmos utilizados en la tecnología que usamos cotidianamente están sesgados, lo que está dando lugar a situaciones de discriminación y, por ende, a violaciones de nuestros derechos humanos, como el derecho a la privacidad, a la protección de datos personales y, por supuesto, el derecho a la autodeterminación informativa, al honor, a la imagen, entre otros derechos que se afectarán en algún momento.

Con esta investigación no se pretende señalar que la tecnología es mala por sí sola. La tecnología es maravillosa y fundamental para la gran mayoría de las actividades que realizamos en todos los sectores. La intención de este artículo mostrar que el uso inadecuado e inescrupuloso de la misma puede generar una afectación que trascienda en todos los ámbitos de nuestra vida personal, familiar, social y laboral. Es nuestra obligación informarnos para hacer uso responsable de la misma y disfrutar las ventajas que nos proporciona con el menor de los riesgos, toda vez que siempre habrá alguna situación que pueda afectarnos.

Referencias

Alarcón, Verónica en Gonzalo, Marilín (2021). El derecho al olvido: 7 años y 1.600.000 enlaces borrados después. Newtral, España, https://www.newtral.es/derecho-al-olvido-internet-enlaces/20210407/

Albarrán, Cristina (2023). ¿Sabes cuánto valen tus datos personales en Internet?. Digital 360, España. https://www.redestelecom.es/seguridad/sabes-cuanto-valen-tus-datos-personales-en-internet/

BBC Mundo (2018). Con un test de Facebook, Cambridge Analytica obtuvo información de millones de usuarios. México: Animal Político. https://www.animalpolitico.com/2018/03/como-un-test-de-personalidad-de-facebook-le-sirvio-a-cambridge-analytica-para-recolectar-informacion-privada-de-millones-de-usuarios-sin-que-lo-supieran

Calderón, Christopher (2023). Un tercio de los internautas no usan antivirus. Periódico El Financiero, México, https://www.elfinanciero.com.mx/empresas/2023/11/15/un-tercio-de-los-internautas-no-usan-antivirus/

Calle, Eduardo (2024). Taylor Swift: publicadas en X falsas imágenes pornográficas de la cantante. El Periódico, Barcelona, España, https://www.elperiodico.com/es/gente/20240130/taylor-swift-victim

a-ia-publicadas-imágenes-pornograficas-cantante-desnuda-dv-97368745

Campos Ríos, Maximiliano (2021). ¿Qué es la identidad digital y por qué está transformando al Estado?. México, INFOBAE, https://www.infobae.com/opinion/2021/07/23/que-es-la-identidad-digital-y-por-que-esta-transformando-al-estado/

Corte Interamericana de Derechos Humanos (2024). Colombia responsable internacionalmente por haber ejecutado actividades arbitrarias de inteligencia contra personas defensoras de derechos humanos, quienes también fueron víctimas de actos de violencia y de estigmatización por parte de autoridades estatales. Comunicado Corte IDH_CP-16/2024 Español, CoIDH, San José de Costa Rica.

Del Río Venegas, Norma Julieta (2023). En riesgo los datos personales y privacidad de usuarios de TikTok. Periódico El Mirador, México, https://www.periodicomirador.com/2023/04/11/en-riesgo-los-datos-personales-y-privacidad-de-usuarios-de-tik-tok/

EFE (2023). Dormir, comer... y Facebook: ¿Cuánto tiempo pasan los mexicanos en redes sociales al día?. Periódico El Financiero, México, https://www.elfinanciero.com.mx/tech/2023/06/30/dormir-comer-y-facebook-mexicanos-ocupan-25-de-su-dia-a-redes-sociales/

Expansión (2023). Corte revisará si Google tiene que pagar 5,000 MDP a mexicano. Periódico Expansión, México, https://expansion.mx/tecnologia/2023/02/16/ulrich-ritcher-vs-google-empresa-pagara-al-abogado

Feiner, Lauren (2024). Judge rules that Google 'is a monopolist' in US antitrust case. The Verge, Estados Unidos, https://www.theverge.com/2024/8/5/24155520/judge-rules-on-us-doj-v-google-antitrust-search-suit

Foran, Clare, Fung, Brian, et.al. (2024). La Cámara de Representantes aprueba un proyecto de ley que podría prohibir TikTok en Estados Unidos. CNN Español, Estados Unidos, https://cnnespanol.cnn.com/2024/03/13/camara-representantes-aprueba-ley-prohibir-tiktok-estados-unidos-trax/

Gracia, Marta (2022). Las claves del imperio Google: el poder de los datos y su simplicidad. El Independiente, España, https://www.elindependiente.com/economia/2022/05/21/las-claves-del-imperio-google-el-poder-de-los-datos-y-su-simplicidad/

Hovenkamp, Herbert J. (2021). Antitrust and Platform Monopoly. University of Pennsylvania Carey Law School. Estados Unidos, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3194&context=faculty_scholarship

Justicia Digital (2023). <<Huella digital: qué es y por qué es relevante>>. Justicia Digital, http://lajusticiadigital.com/blog/huella-digital-que-es

Kaplan, Patricia (2024). La UE aprueba una histórica ley sobre inteligencia artificial. Esto es lo que se dice. CNN, Estados Unidos, https://cnnespanol.cnn.com/video/union-europea-nueva-ley-inteligencia-artificial-cnn-dinero-tv/

Lastiri, Diana (2022). TikTok pierde amparo contra el INAI sobre uso de datos personales. Proceso, México, https://www.proceso.com.mx/nacional/2022/12/19/tiktok-pierde-amparo-contra-el-inai-sobre-uso-de-datos-personales-298936.html

López Casarín, Javier (2022). Identidad Digital, ¿qué es y por qué es tan importante?, México, Forbes. https://www.forbes.com.mx/identidad-digital-que-es-y-por-que-es-tan-importante/

Naciones Unidas. (2014). Resolución aprobada por la Asamblea General el 18 de diciembre de 2013. https://documents.un.org/doc/undoc/gen/n13/449/50/pdf/n1344950.pdf?token=I7Qcj7Fe4JJOin6IH0&fe=true

Naciones Unidas. (2020). Resolución aprobada por la Asamblea General el 16 de diciembre de 2020. https://documents.un.org/doc/undoc/gen/n20/371/79/pdf/n2037179.pdf?token=7l2oMGgOKkNMrJbk0j&fe=true

Nares Feria, Yamil (2018). La Deep web y otras cosas profundas. Animal Político, Mexico, https://www.animalpolitico.com/analisis/autores/la-ventana-indiscreta/la-deep-web-y-otras-cosas-profundas

Pineda Gómez, Hernán, Jima-González, Alexandra, et al. (2020). ¿Preparados para las fake news? Un estudio exploratorio de la comunidad universitaria del Tecnológico de Antioquia. Revista de Investigación en Administración, Contabilidad, Economía y

Sociedad, vol. 8, núm. 12, https://www.redalyc.org/journal/5518/551865938009/html/

Pinto, Teguayco (2019). Facebook afronta otra demanda por orientar sus anuncios de forma discriminatoria. El País, España, https://elpais.com/tecnologia/2019/11/13/actualidad/1573669848_630951.html?event=oklogin&event_log=oklogin

Piñar Mañas, José Luis y Recio Gayo, Miguel (2016). La privacidad en Internet. Suprema Corte de Justicia de la Nación, México, https://www.sitios.scjn.gob.mx/cec/sites/default/files/publication/documents/2019-03/07_PIÑAR%20y%20RECIO_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales.pdf

Quijano Decanini, Carmen (2022). Derecho a la privacidad en Internet. Tirant Lo Blanch, México.

Quirós-García, Elizabeth (2021). La huella digital y la protección de datos: su impacto en las culturas de alto contexto y alto control de incertidumbre en Latinoamérica. Revista InterSedes, vol. XXII, núm. 46: 169-187. https://www.redalyc.org/journal/666/66671361007/html/

Recio Gayo, Miguel (2022). La Privacidad en la Era de las Redes Sociales. INAI, México, https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/PRIVACIDADYREDES_digital.pdf

Román Vergara, Josefina en López Dóriga (2024). Joaquín. Inai urge a actualizar Ley de Protección de Datos para regular el uso de IA,

López Dóriga Digital, México, https://lopezdoriga.com/nacional/inai-urge-actualizar-ley-de-proteccion-de-datos-regular-ia/

Sánchez Cordero, Olga (2023). "Ley Ingrid" sanciona filtración de imágenes de víctimas; no es una mordaza para periodistas: Sánchez Cordero. Comunicado Número – 093, Senado de la República, México, https://comunicacionsocial.senado.gob.mx/informacion/comunicados/6779-ley-ingrid-sanciona-filtracion-de-imagenes-de-victimas-no-es-una-mordaza-para-periodistas-sanchez-cordero

Sánchez de Table, Gonzalo (2017). Derecho a la igualdad y no discriminación: la doctrina de la Suprema Corte. Revista Nexos, México, https://eljuegodelacorte.nexos.com.mx/derecho-a-la-igualdad-y-no-discriminacion-la-doctrina-de-la-suprema-corte/#:~:text=Son%20categorías%20sospechosas%20los%20criterios,civil%20o%20cualquier%20otra%20que

Secretaría de Coordinación de Producción (2021). Comercio Interior dictó una medida cautelar contra Facebook para evitar que WhatsApp acceda a información privada de los usuarios, Argentina.gob.ar, Argentina, https://www.argentina.gob.ar/noticias/comercio-interior-dicto-una-medida-cautelar-contra-facebook-para-evitar-que-whatsapp-0

Suprema Corte de Justicia de la Nación (2022). Comunicado de Prensa No. 424/2022. SCJN, México,

https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=7148

Taizhpu (2023). Dolientes chinos usan la inteligencia artificial para resucitar digitalmente a sus muertos. Francce24, Francia, https://www.france24.com/es/minuto-a-minuto/20231214-dolientes-chinos-usan-la-inteligencia-artificial-para-resucitar-digitalmente-a-sus-muertos

Thorn (2024). Youth Perspectives on Online Safety, 2023. Thorn, https://info.thorn.org/hubfs/Research/Thorn_23_YouthMonitoring_Report.pdf

UNICEF (2021). Orientación de políticas sobre el uso de la inteligencia artificial en favor de la infancia. Naciones Unidas para la Infancia, Nueva York, Estados Unidos, https://www.unicef.org/globalinsight/media/2636/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021_ES.pdf

Vallejo, Guadalupe (2024). INAI investiga “filtración” de datos de periodistas que acuden a la mañanera. Periódico Expansión, México, https://politica.expansion.mx/presidencia/2024/01/26/inai-investiga-filtracion-de-datos-de-periodistas-que-acuden-a-la-mananera