

Derecho al internet y nuevas amenazas digitales: la deuda constitucional en el Perú

*Internet access and new digital threats:
the constitutional debt in Peru*

 GIAN DIEGO JESÚS VELASCO BUSTAMANTE*

261

Resumen

El presente ensayo analiza el reconocimiento constitucional del derecho al acceso al internet en el Perú, establecido mediante la Ley 31878 y la incorporación del artículo 14-A a la Constitución Política. Este avance normativo, aunque significativo, resulta insuficiente frente a los desafíos estructurales que plantea la era digital. Por otro lado, el análisis parte de un enfoque constitucional crítico y se apoya en doctrina nacional e internacional, así como en jurisprudencia relevante, para evidenciar que el actual marco legal carece de mecanismos que aseguren un ejercicio efectivo, equitativo y seguro de este derecho fundamental. En particular, se advierten graves omisiones en cuanto a la calidad del servicio, la alfabetización digital, la inclusión territorial y la protección frente a amenazas tecnológicas emergentes como la inteligencia artificial, el Big Data, la biometría y los *deepfakes*. Asimismo, el problema central identificado es la ausencia de una visión integral de los derechos digitales, lo cual genera tensiones entre el acceso libre a internet y la protección de datos personales, dejando a los ciudadanos expuestos a riesgos no regulados. Ante ello, el ensayo propone una reconstrucción del ecosistema digital sustentada en cinco presupuestos constitucionales: interpretación integral del derecho al internet, complementariedad con la autodeterminación informativa, deber estatal de garantía, adaptación normativa frente a la innovación tecnológica

* Estudiante de derecho en la Universidad Católica Santo Toribio de Mogrovejo – Chiclayo.
Código ORCID: 0009-0005-5522-6394. Correo electrónico: gianvelascojvb@gmail.com

y equilibrio entre libertad digital y seguridad. Estas propuestas buscan consolidar un marco jurídico preventivo, transversal y actualizado, que permita ejercer una ciudadanía digital libre, protegida y plenamente compatible con los principios del Estado constitucional de derecho.

Palabras clave

internet, derechos digitales, protección de datos personales, amenazas digitales, inteligencia artificial.

Abstract

This essay examines the constitutional recognition of the right to internet access in Peru, established by Law No. 31878 and the incorporation of Article 14-A into the Political Constitution. This regulatory advance, although significant, is insufficient in the face of the structural challenges posed by the digital age. The analysis begins with a critical constitutional approach and draws on national and international doctrine, as well as relevant jurisprudence, to demonstrate that the current legal framework lacks mechanisms to ensure the effective, equitable, and secure exercise of this fundamental right. In particular, serious omissions are noted regarding the quality of service, digital literacy, territorial inclusion, and protection against emerging technological threats such as artificial intelligence, big data, biometrics, and deepfakes. The central problem identified is the absence of a comprehensive vision of digital rights, which generates tensions between free internet access and the protection of personal data, leaving citizens exposed to unregulated risks. In response, the essay proposes a reconstruction of the digital ecosystem based on five constitutional prerequisites: a comprehensive interpretation of the right to the internet, complementarity with informational self-determination, the state's duty to guarantee it, regulatory adaptation to technological innovation, and a balance between digital freedom and security. These proposals seek to consolidate a preventive, cross-cutting, and up-to-date legal framework that allows for the exercise of free, protected digital citizenship that is fully compatible with the principles of the constitutional state of law.

Key words

internet, digital rights, personal data protection, digital threats, artificial intelligence.

Sumario

I. INTRODUCCIÓN. II. EL ACCESO AL INTERNET COMO DERECHO FUNDAMENTAL EN EL MUNDO ACTUAL. III. LA FRAGILIDAD DEL DERECHO AL ACCESO AL INTERNET EN EL PERÚ Y SU VINCULACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES. IV. NUEVAS AMENAZAS DIGITALES: WORLD ID, INTELIGENCIA ARTIFICIAL Y LA VULNERABILIDAD DE LOS DATOS PERSONALES. V. HACIA UNA RECONSTRUCCIÓN CONSTITUCIONAL: INTERNET, PROTECCIÓN DE DATOS Y GARANTÍAS FRENTE A LA ERA DIGITAL. VI. PRESUPUESTOS CONSTITUCIONALES PARA ENFRENTAR LA DEUDA CONSTITUCIONAL ANTE LA ERA DIGITAL. VII. CONCLUSIONES.

I. INTRODUCCIÓN

La evolución tecnológica de la sociedad ha sido notoria con el paso de los años; vivimos en un contexto donde el internet se ha convertido en un instrumento cotidiano en la vida de las personas. Esta transformación tecnológica ha facilitado el acceso del ser humano en su relación con el Estado, acceso a bienes y servicios informáticos con el fin de facilitar el ejercicio de sus derechos. La consolidación del internet como un recurso cotidiano y estratégico en la vida contemporánea ha motivado que diversos estados reconozcan su acceso como un derecho fundamental. En el caso de Perú, este reconocimiento se formalizó recientemente mediante la Ley 31878, que incorporó el artículo 14-A a la Constitución Política, estableciendo el acceso libre al internet como un derecho de todo ciudadano. Esta reforma constitucional responde a la creciente necesidad de integrar a la ciudadanía a una esfera digital que permita el ejercicio pleno de otros derechos, como la educación, la salud, el trabajo y la libertad de expresión. No obstante, este avance normativo ha expuesto una serie de desafíos estructurales y vacíos legales que limitan la efectividad real del derecho a la conectividad en el país.

El presente informe sostiene como tesis que el reconocimiento constitucional del acceso al internet, si bien representa un progreso significativo en el desarrollo de los derechos digitales en Perú, resulta insuficiente si no se incorpora de forma integral con otros elementos esenciales del entorno digital, especialmente la protección de los datos personales. En ese sentido, se plantea que el artículo 14-A, al no prever garantías mínimas como la calidad del servicio, el desarrollo de competencias digitales o mecanismos de protección frente a amenazas tecnológicas, genera una tensión jurídica entre la conectividad libre y la privacidad digital, poniendo en riesgo derechos fundamentales de las personas usuarias.

En atención a ello, este trabajo se estructura en tres ejes centrales. En primer lugar, se examina el desarrollo progresivo del derecho al internet como derecho fundamental a nivel internacional y su incorporación en el ordenamiento jurídico peruano. En segundo lugar, se analiza la fragilidad del artículo 14-A frente a los retos que implica la protección de datos personales en un entorno digital no regulado con suficiencia. Finalmente, se abordan las nuevas amenazas tecnológicas —como la inteligencia artificial, los *deepfakes*, el big data y la biometría— que, al operar sobre la base de la libre conectividad, exponen a la ciudadanía a vulneraciones graves de su privacidad e identidad. Este panorama permite evidenciar que el Perú afronta una deuda constitucional pendiente: la reconstrucción normativa de un verdadero bloque de derechos digitales que integre acceso, protección y garantía efectiva en la era digital.

II. EL ACCESO AL INTERNET COMO DERECHO FUNDAMENTAL EN EL MUNDO ACTUAL

En la actualidad, el acceso al internet es considerado como un derecho fundamental que permite el desarrollo y garantía de otros derechos fundamentales. Fernández (2022), desde una perspectiva internacional, señala que el derecho al acceso al internet facilitaría el ejercicio real de otros derechos fundamentales, con el fin de exigir al Estado una infraestructura que permita la conexión entre todos estos derechos e invocar el cumplimiento de estos. En otras palabras, el acceso al internet contribuye al ejercicio de otros derechos como lo pueden el derecho a la educación, salud y al trabajo.

Con el paso del tiempo, diversas normas han ido tutelándose como un garante del acceso a internet hacia las personas, debido a que con el paso de los años el internet se ha ido convirtiendo en algo cotidiano para el ser humano. Para esto, Miranda (2016) menciona que: «Existe una tendencia en el ámbito constitucional y convencional que ha reconocido el acceso a internet como un derecho fundamental» (p. 2). Dando a entender que el derecho constitucional tras el contexto de esta nueva era digital vio oportuno y necesario reconocer este derecho fundamental al acceso al internet; a su vez, este autor afirma que el acceso al internet es parte de estos «nuevos derechos» ya que ha influenciado positivamente en el desarrollo de la sociedad.

En el ámbito internacional, el derecho al acceso al internet ha ido teniendo una evolución constitucional. Desde inicios del siglo XXI, diversos países del mundo han adoptado medidas para ampliar este derecho dentro de toda la población. En un informe realizado hace más de una década por el exrelator especial de la Organización de las Naciones Unidas (ONU), La Rue (2011) mencionaba que: «El internet solo puede responder a su finalidad si los Estados asumen su voluntad de elaborar políticas eficaces para obtener el acceso universal a internet» (p. 18). Señalando que se requiere una voluntad clara de los gobiernos para poder implementar políticas públicas eficaces que permitan que todas las personas puedan acceder al internet sin importar ubicación geográfica. Asimismo, este informe menciona que, en algunos países, como Estonia en el año 2000, su parlamento ya declaraba el acceso al internet como derecho humano básico. Del mismo modo, señala que en el año 2009, el Consejo Constitucional de Francia emite una importante decisión (Decisión 2009-580 DC) en donde se reconoce al internet como derecho fundamental. Sin embargo, Prince (2020), sobre dicha sentencia francesa, menciona que el tribunal «considera que el acceso al servicio de internet se encuentra subsumido en el derecho a la libertad de expresión, que

a su vez se deriva directamente de la Declaración Universal de los Derechos del Hombre del año 1789» (p. 7). Dando a entender que el tribunal francés no terminaba por considerar el acceso al internet como un nuevo derecho autónomo, sino que integra este derecho dentro de otro como lo es la libertad de expresión, siendo una herramienta clave para lograr su efectivo ejercicio.

Tras estos antecedentes, la Asamblea General de la ONU, en el año 2011, terminó por declarar el acceso al internet como derecho humano, al ser una herramienta que permite el crecimiento y desarrollo progresivo de la sociedad. Por otro lado, se pudo evidenciar cómo tribunales de países desarrollados se llegaron a pronunciar positivamente sobre este derecho al acceso al internet. Anzures (2021) nos mencionaba en como el Tribunal Federal de Alemania (BGH) llegó a considerar que: «La internet es un medio a través del cual la persona cumple ciertas obligaciones hacia el Estado, tales como el pago de servicios públicos o sus impuestos» (párr. 2). Destacando lo esencial que se ha vuelto el internet en la vida de las personas, convirtiéndose en un medio que permite ejercer otros derechos y deberes ciudadanos o así también para cumplir obligaciones legales o administrativas.

En el contexto nacional, el Estado peruano actualmente reconoce el derecho al acceso al internet, siendo este incorporado en la Constitución Política del Perú de 1993 mediante la Ley 31878 (2023): «Ley de reforma constitucional que promueve el uso de las tecnologías de la información y comunicación, y reconoce el derecho de acceso a internet libre en todo el país», siendo una ley que se publicó en el Diario Oficial El Peruano en septiembre del 2023, modificando los artículos 2.4 e incorporando el artículo 14-A dentro de la Constitución Política del Perú. En el caso del primero, la modificación consistió en la ampliación del alcance para reconocer el acceso al internet libre como un instrumento esencial para ejercer derechos también importantes como el de la libertad de información y expresión, siendo un claro ejemplo, de cómo el acceso al internet se logra inmiscuir dentro de otros derechos. Por su parte, el artículo 14-A reconoce expresamente el acceso a internet como un derecho fundamental en sentido estricto, siendo un artículo que tuvo como fin salvaguardar los problemas y carencias de la sociedad peruana que existían dentro del contexto de la pandemia del COVID-19, especialmente en zonas rurales en donde se necesitaba del acceso al internet para garantizar otro derecho fundamental, como el derecho a la educación en ese entonces.

Sin embargo, dar este reconocimiento al acceso al internet como un derecho fundamental libre para todos no significa que este sea gratuito en su totalidad; esto se puede evidenciar en otros derechos ya antes reconocidos, como el derecho a la

salud, educación, etc. Monge (2023) señala que: «En el caso de servicios públicos o de interés público, ‘libre’ significa que no habrá impedimentos o que el Estado fomentará su acceso masivo, en amparo del principio democrático» (párr. 5). En otras palabras, lo esencial del reconocimiento de un derecho reside en la capacidad y obligación que tiene el Estado para fomentarlo y garantizarlo a través del desarrollo de una infraestructura y medidas necesarias, así como la continuidad del servicio. Por lo tanto, se puede decir que el acceso a internet, al ser libre para todos, adquiere características propias de un servicio público, sin que ello signifique una prestación gratuita en todos los casos.

III. LA FRAGILIDAD DEL DERECHO AL ACCESO AL INTERNET EN EL PERÚ Y SU VINCULACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES

La incorporación del derecho al acceso al internet dentro de la Constitución Política del Perú por medio de la modificación del artículo 2.4 y la integración del artículo 14-A en dicho texto ha sido un gran avance por parte del derecho constitucional; sin embargo, aún presenta barreras significativas que comprometen la garantía efectiva de este derecho en la práctica. Es por eso que, para referirnos a este derecho, vamos a centrarnos en sentido estricto en el artículo 14-A, que, si bien garantiza el «acceso libre» a internet dentro de todo el territorio nacional, deja en el aire muchos vacíos respecto a su protección específica, generando cierta incertidumbre sobre algunos parámetros como velocidad mínima, calidad de servicio, protección contra interrupciones de internet. Para esto, el experto en derecho digital, el Dr. Iriarte (como se citó en Mendoza, 2023) menciona que:

El cierre de la brecha no solo parte de la conectividad sino del desarrollo de capacidades para poder utilizar la conectividad a la cual se tiene acceso. El cambio normativo realizado a la constitución deja en el aire el tema del desarrollo de capacidades. (párr. 7).

Es decir, la reforma constitucional que integra este nuevo derecho se enfoca únicamente en garantizar la disponibilidad de internet en toda la nación, pero no define la calidad de acceso ni las capacidades que tiene la población para acceder al internet. Por ejemplo, una persona que habita en una zona rural puede que tenga este «acceso libre» a una red wifi pública, pero si no sabe usar plataformas digitales, si no tiene dispositivos adecuados o si la conexión es lenta, su derecho no se está ejerciendo plenamente. En otras palabras, muchas poblaciones del Perú no han logrado desarrollar las suficientes competencias digitales, formación ni recursos adecuados para acceder al internet, quedando como un derecho incompleto.

Por otro lado, el artículo 14-A no contempla los riesgos que sobrelleva dar un acceso libre al internet en relación al derecho a la protección de datos personales (Derecho a la autodeterminación informativa) regulado en el artículo 2, inciso 6 de la Constitución. Esta omisión constitucional es especialmente grave debido que ingresar a internet implica un sin número de tratamiento de datos personales, que muchas veces son expuestos sin un consentimiento claro y previo. El Tribunal Constitucional (TC) (2007), en la sentencia recaída dentro del Expediente 04739-2007-HD, en el fundamento 2 señala que: «El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos» (p. 2). Dando a entender que el individuo tiene ese derecho de poder controlar el uso de sus datos personales y nadie puede usarlos sin su consentimiento. Lo mencionado posee relevancia debido a que actualmente, al acceder a la red, una página web recolecta tus datos mediante cookies, inteligencia artificial, big data, formularios, redes sociales, etc., vulnerando el derecho a la autodeterminación informativa y otros que se encuentran conexos como los de la imagen, honor e intimidad.

Asimismo, la última modificatoria del reglamento de la Ley de Protección de Datos Personales (LPDP) N°. 29733 (2024), aprobado por el Decreto Supremo 016-2024, específicamente en el artículo 86, habla sobre el derecho de oposición al tratamiento de los datos personales y en el numeral 5 señala que: «Cuando los datos personales son tratados en internet, el ejercicio de derecho de oposición puede incluir la desindexación de los datos personales» (p. 17). En otras palabras, toda persona que accede a internet puede oponerse al tratamiento de sus datos personales y solicitar que se dejen de procesar estos. Sin embargo, el artículo 14-A, al garantizar el internet como un «acceso libre» a este, no prevé medidas de control sobre estos datos privados que se vulneran al acceder a la red, dejando a los ciudadanos expuestos a ser víctimas de delitos informáticos como la vigilancia digital indebida, el robo de información o el uso no autorizado de sus datos. De este modo, se crea una paradoja en donde se pone en evidencia la tensión entre el derecho al acceso libre al internet y la necesidad de proteger los datos personales, especialmente en tiempos de esta nueva era digital, en donde la conectividad sin garantías puede convertirse en una vía de vulneración de otros derechos fundamentales. Ahora bien, esta controversia solo existe cuando estos dos derechos se asimilan por separado y no integralmente, es por eso que resulta necesario comprender que ambos derechos deben abordarse en conjunto, con el fin de asegurar mayor garantía de estos dentro de su ejercicio.

El acceso a internet y la protección de datos personales (PDP) deben interpretarse como componentes de un bloque integrado de derechos digitales. Manani (2023; parafraseando a Peña-Pérez, 2021) sostiene que los derechos digitales se entienden como: «un conjunto de prerrogativas y libertades fundamentales que las personas tienen en el entorno digital» (p. 3). Dicho de otro modo, esto implica que la tensión abordada entre el derecho al acceso a internet y a la PDP no debería existir en nuestro ordenamiento jurídico, puesto que en la práctica no son independientes, siendo componentes interrelacionados dentro de un solo conjunto normativo. Aguilar (2024), tras un análisis estadístico (Rho de Spearman 0,615) realizado señala que: «Existe una relación significativa entre la protección de datos personales y los derechos digitales en el Perú. Este hallazgo sugiere la importancia de considerar la protección de datos como un elemento crucial en la garantía y promoción de los derechos digitales en el entorno peruano» (p. 16). Reafirmando así la tesis de que no puede hablarse de un acceso libre a internet si no se garantiza en conjunto de derechos digitales (como es el caso de la PDP) para la tutela adecuada de los datos personales.

La configuración de un bloque de derechos digitales dentro de nuestro ordenamiento jurídico permitiría establecer un marco normativo coherente entre los derechos como el acceso al internet y la protección de datos personales, evitando todo tipo de tensión y contradicción jurídica frente a los riesgos que existen actualmente. A su vez, se busca que contribuyan a un mismo objetivo, como es el de garantizar que las personas tengan la facultad de poder ejercer plenamente sus derechos fundamentales en el entorno digital.

IV. NUEVAS AMENAZAS DIGITALES: WORLD ID, INTELIGENCIA ARTIFICIAL Y LA VULNERABILIDAD DE LOS DATOS PERSONALES

La nueva era digital presenta nuevos desafíos para la protección de datos personales que necesitan ser abordados ante las nuevas amenazas que aparecen; el reconocimiento del derecho al acceso libre al internet, tal como se mencionó anteriormente, trae consigo algunos debates con respecto a su protección frente a tecnologías emergentes que procesan información personal sin control alguno. Escribano (citado por Mubarak, 2020) afirma que:

La facilidad con la que se accede a internet, su uso a edades cada vez más tempranas, la rapidez con la que se difunde la información y el escaso control que tenemos de nuestros datos, entre otros factores, hacen que internet se configure como un marco idóneo para la lesión de nuestros derechos. (p. 2)

Dando a entender que un acceso libre a internet es un facilitador de un entorno en el que se recopilan cantidades inmensas de datos personales, llevando a grandes peligros ante las nuevas amenazas que se encuentran presentes en el mundo digital de hoy en día.

Al respecto, Olivos (2018) advierte que «la protección de la privacidad nace como una respuesta a un problema real [...], el tratamiento masivo de los datos personales [...] constituían una amenaza al sistema de derechos fundamentales, haciendo vulnerables a las personas» (p. 2). A pesar que esta reflexión surge en un contexto general sobre privacidad, resulta plenamente aplicable a la realidad actual del entorno digital, dado que el acceso a internet, cuando no se encuentra acompañado de adecuados mecanismos de protección, genera precisamente ese tratamiento masivo e incontrolado de datos personales.

El globo empresarial peruano ya se encuentra adoptando estas tecnologías como la inteligencia artificial, big data, biometría. Sin embargo, aún presentan dificultades para mitigar riesgos que estos sistemas pueden ocasionar. Andina (2025) reporta que el 55 % de empresas aún enfrentan obstáculos frente a los riesgos de ciberseguridad; aquella situación resulta crítica si se considera que estas tecnologías empleadas en la actualidad, sin una protección adecuada, pueden manipular información altamente sensible sin una supervisión adecuada, revelando así una deficiencia estructural en las garantías que da el Estado para la protección de los derechos digitales al acceder a internet.

1. Los riesgos del uso indiscriminado de la inteligencia artificial

La inteligencia artificial (IA) representa una de las amenazas más significativas y estructurales para la protección de datos personales en el contexto del acceso libre a internet. Morales (2021), miembro del Comité de Protección de Datos Personales de World Compliance Association Capítulo Perú señala que: «La protección de los datos personales se ve desafiada por el rápido desarrollo y el veloz despliegue de la IA pues su utilización implica necesariamente el tratamiento de datos masivos, dentro de los cuales se incluyen diferentes categorías de datos personales» (párr. 1). En otras palabras, señala que los sistemas de IA requieren de grandes cantidades de datos para funcionar eficazmente, generando riesgos sin precedentes para la privacidad de los usuarios. Asimismo, el problema se agrava cuando estos sistemas operan dentro de un entorno de «acceso libre» a internet, tal como lo menciona el artículo 14-A de nuestra carta madre; no existiendo una protección específica ante los riesgos que pueden tener estos sistemas al acceder a internet.

En el contexto de los avances normativos, el poder legislativo aprobó el Reglamento de la Ley 31814 (2023): «Ley que promueve el uso ético y responsable de la Inteligencia Artificial en favor del desarrollo económico y social del país». Este reglamento reconoce expresamente la necesidad de garantizar principios básicos como la privacidad, la protección de datos personales y la autodeterminación informativa, todo esto frente a los desafíos que plantea la inteligencia artificial en nuestra sociedad contemporánea. Sin embargo, no aborda por completo los riesgos estructurales que implica la IA, como el tratamiento masivo de datos, la creación de identidades sintéticas o la generación de contenidos falsos, fenómenos que ya están ocurriendo en el Perú.

En esa misma línea, en el año 2025 se publica la Ley 32314 (2025): «Ley que modifica el Código Penal, Decreto Legislativo 635, y la Ley 30096, Ley de delitos informáticos, para incluir el uso de la inteligencia artificial en la comisión de delitos». Integrando dentro del Código Penal un agravante dentro de los delitos informáticos que sean cometidos dando uso de inteligencia artificial o tecnologías análogas, el juez tiene la facultad de incrementar la pena hasta en un tercio por encima del máximo legal permitido. Esta nueva disposición, si bien reconoce los nuevos peligros que puede ocasionar la IA en su uso ilícito, actúa solo de forma reactiva, no estableciendo mecanismos preventivos que den garantías de privacidad ante los riesgos que estos nuevos sistemas traen como consecuencias.

Esta situación ha llevado a que diversos especialistas analicen las consecuencias jurídicas que podría tener este fenómeno de la IA en los derechos fundamentales de las personas. Roel, Chocano & Salazar (2025) advierten que los riesgos que puede ocasionar la IA pueden vulnerar los derechos a la imagen, autodeterminación informativa y a la identidad. Del mismo modo, señalan que de acuerdo a Marr (2023), los riesgos pueden estar vinculados a la preocupación por la privacidad, la seguridad, desinformación y manipulación de la IA. Estas amenazas, además de exponer a los usuarios a perder el control de sus propios datos, pueden distorsionar su reputación, así como ser influyente dentro de la toma de decisiones sociales o políticas usando información falsa.

a) La proliferación malintencionada de los deepfakes

Una manifestación de los riesgos que puede ocasionar la IA en la actualidad, son los llamados *deepfakes*, los cuales, tal como lo menciona García-Ull (2021), consiste en: «un vídeo hiperrealista manipulado digitalmente para representar a personas que dicen o hacen cosas que en realidad nunca sucedieron» (p. 1). Cabe aclarar que los *deepfakes* no solo son manipulaciones hechas a base de videos, sino

que también puede incluir imágenes y audios trucados. Una prueba en como la IA en la actualidad, si bien pueden tener aplicaciones legítimas, en muchos casos es usada con fines ilícitos como suplantación de identidad, difamación o generación de contenido falso que afecte la imagen y reputación de personas. Según la empresa de ciberseguridad Karpesky (2024), el 57 % de los peruanos desconocen qué es *deepfake*, alertando que existe una gran cantidad de cibercriminales usando sistemas de IA para crear imágenes engañosas, aumentando los riesgos asociados por *deepfakes*.

En el Perú y el mundo se ha evidenciado cómo los *deepfakes*, además de representar una herramienta de manipulación audiovisual, también son una amenaza directa a la dignidad e intimidad de las personas. A nivel internacional, uno de los casos más alarmantes fue informado por el diario El País (como lo citan en Fernandes, Fernández, Molero y Pérez, 2025), en donde se utilizó un *deepfake* de la princesa Leonor para cometer estafas virtuales a través de la red social TikTok. La estafa consistía en que usuarios recibían un video falso de la princesa Leonor, en donde se les anunciaba haber ganado una gran cantidad de dinero, pero para ganarlos debían realizar un depósito previo, lo cual era totalmente falso, puesto que después estos ciberdelincuentes desaparecían. Este caso evidencia que la tecnología *deepfake* no solo constituye un riesgo a la imagen personal, sino que se ha convertido en un instrumento de fácil manipulación para la comisión de delitos digitales. De acuerdo al Diario Infobae (2025), un caso alarmante ocurrió en junio del 2025, cuando la Policía Nacional del Perú (PNP) detuvo en la ciudad de Arequipa a un sujeto que había creado más de 50 videos pornográficos falsos utilizando inteligencia artificial (*deepfake*), suplantando los rostros de mujeres sin su consentimiento. Una clara muestra de que la IA, en manos equivocadas, puede ocasionar gran cantidad de riesgos y vulnerar derechos fundamentales de las personas.

Es también una realidad que hay casos en donde la IA es usada para estafas telefónicas. De acuerdo con la BBC (2023), se informó que: «Ahora, la tecnología para crear un audio falso, una copia realista de la voz de una persona, se está volviendo cada vez más común» (párr. 5). De esta manera, ciberdelincuentes usan la IA para imitar la voz de personas y realizar estafas. Lo mencionado es algo muy preocupante, puesto que para copiar estas voces se necesita un amplio contenido de grabaciones de voz de la persona, siendo realizadas sin un consentimiento previo, vulnerando derechos autónomos de la persona como la intimidad, la voz y al honor de las personas. Es por esto que tanto el Perú como el resto del mundo enfrentan el reto urgente que consiste establecer un marco legal que responda eficazmente al uso malicioso de estas herramientas tecnológicas y proteja a los ciudadanos frente a estas formas modernas de manipulación y estafa digital.

La proliferación de los *deepfakes* plantea un desafío urgente por parte del sistema legal, no solo por el daño que pueden causar, sino por la complejidad para identificar a los responsables. Loret de Mola (citado por Torres, 2025) señala que: «Para poner una denuncia ante la Autoridad Nacional de Datos Personales (la imagen o video es un dato personal), hay que identificar al autor o responsable del *deepfake*: puede ser al creador del software o quien haya elaborado el video. Pero muchas veces identificarlos es complejo debido al uso de la IA» (p. 5). Evidenciando que nuestro ordenamiento jurídico se encuentra muy limitado para responder legalmente de forma eficaz ante estas nuevas formas de vulneración digital de datos personales. Sobre esto, Palao (citado por Torres, 2025) también opina: «Creo que todavía no tenemos peritos capacitados para llegar al trasfondo del delito. Se pueden iniciar las investigaciones, a veces hasta tienes la trazabilidad de las cuentas, pero cuando los IP están en otro país, se vuelve complicado» (p. 3). En otras palabras, esta dificultad se ve agravada por la falta de especialistas informáticos expertos en inteligencia artificial y en cibercriminalidad.

b) El peligro del Big Data en el mundo actual

En la era digital, otro de los grandes peligros para la privacidad es la irrupción desmedida del actual sistema llamado Big Data. De acuerdo con González (2023): «El Big Data se ha convertido en una herramienta clave para empresas, gobiernos y organizaciones en todo el mundo, ya que permite el análisis de grandes cantidades de información para obtener conocimientos y tomar decisiones informadas» (p. 2). Es decir, este nuevo sistema se entiende como un tratamiento automatizado de grandes volúmenes de información personal. Sin embargo, en la gran mayoría de los casos, esta recopilación de datos se realiza sin el consentimiento de las personas titulares. Una definición más amplia de este nuevo sistema la da el Parlamento Europeo (citado por Cotino-Hueso, 2019) señalando que:

Se refiere a la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos). (p. 7)

Se puede observar que estas prácticas terminan generando patrones y perfiles conductuales que en muchos casos son dirigidos por inteligencia artificial y siendo utilizados con fines comerciales, políticos o de vigilancia, sin embargo, indirectamente atentan contra la privacidad de las personas, dado que almacenan gran cantidad de su información personal sin su debida autorización.

Existen una gran variedad de empresas en el mundo que usan este tipo de sistemas informáticos con diversos fines, ya sea desarrollo de productos, marketing, servicios, etc. Sin embargo, algunas recopilan información de forma ilegal e ilegítimamente, sin un previo consentimiento de los usuarios. Sobre esto, The Guardian (citado por González, 2023) nos da un caso paradigmático en donde la empresa Cambridge Analytica, en el año 2018, fue descubierta obteniendo ilícitamente datos de millones de usuarios de la red social Facebook sin su consentimiento. Demostrando en cómo estas empresas irrumpen en la privacidad de las personas, siendo una amenaza al derecho de autodeterminación informativa y al ejercicio pleno de los derechos digitales.

2. La biometría y el proyecto WorldID: Riesgos para la privacidad e identidad

La biometría digital en la actualidad representa una de las mayores amenazas sofisticadas y permanentes contra la protección de datos personales en la era digital contemporánea. Lacruz (2025) menciona que: «Se trata de la utilización de sistemas inteligentes que, a través de videocámaras, reconocen los rasgos faciales de las personas y, a partir de estos, la identidad de cada persona en particular» (p.11). Dicho de otro modo, esta tecnología convierte características únicas de las personas en identificadores digitales permanentes. No obstante, el peligro radica en que, a diferencia de otros tipos de información personal, estos datos (las huellas dactilares, el reconocimiento facial, el iris, y la voz) no pueden ser remplazados, puesto que son únicos e inmutables en la persona.

Del mismo modo, Lacruz (2025) también afirma que: «Los sistemas de reconocimiento de personas por sus datos biométricos son invasivos por sí mismos e impactan directamente en la protección de datos personales prescrita en el artículo 16 del Tratado de Funcionamiento de la Unión Europea» (p. 11). Siendo una afirmación crucial, puesto que evidencia cómo la biometría convierte rasgos físicos únicos en claves digitales permanentes que son imposibles de modificar. De esta manera, se expone a los usuarios que forman parte de estos sistemas a cualquier tipo de filtración, vigilancia masiva, suplantación de identidad e incluso discriminación algorítmica.

En el ámbito nacional peruano se puede evidenciar cómo las empresas desde hace un par de años han ido implementando este sistema de biometría. De acuerdo con EyNG (2025), el Perú desde el año 2023 ha crecido un 50 % en el uso de herramientas biométricas como el reconocimiento facial y la lectura de huellas dactilares. Este crecimiento, si bien representa un avance en eficiencia y seguridad para diversos servicios, también implica un nuevo frente de vulnerabilidad hacia la protección de datos personales.

La creciente implementación de tecnologías biométricas en el Perú y Latinoamérica refleja una clara tendencia hacia la digitalización de los procesos de verificación de identidad, tanto en el sector público como privado. Según Hernández (2023), en el Estudio de Innovación de Visa & Americas Market Intelligence 2022, el 70 % de las organizaciones en la región ya utilizaba biometría, predominando principalmente técnicas como el reconocimiento facial (63 %), la huella dactilar (43 %) y el reconocimiento de voz (12 %). No obstante, este avance, a pesar de ser prometedor en términos de eficiencia y seguridad, exige con urgencia el desarrollo e implementación de marcos regulatorios robustos que garanticen la protección efectiva de los datos personales.

Ahora bien, uno de los casos más controversiales que se han ido evidenciando en el Perú y el mundo con respecto a la biometría es el de la empresa Tools for Humanity, conocido como *WorldID* a nivel mundial. En el Perú, la empresa inició sus actividades en el año 2024 tras el lanzamiento del proyecto *WorldCoin*. (Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, 2024). Este sistema consiste en un escaneo facial y de iris de personas a través de un dispositivo llamado Orb a cambio de adquirir dinero en criptomonedas. Su funcionamiento consiste en la sincronización de este dispositivo al teléfono de las personas, brindando un código único por usuario y que nadie más posee. (Vera, 2024)

Asimismo, de acuerdo al Diario la República (2024), en la ciudad de Lima, Perú, esta empresa cuenta con alrededor de 6 sedes, ofreciendo el monto de 10 criptomonedas valoradas aproximadamente en doscientos nuevos soles a cambio de un escaneo de retina. También, se menciona que, en países como España, Portugal y Kenia, esta empresa ha sido vetada por los riesgos de seguridad y transparencia que conlleva. Sobre esto, Cenas (citado por el Diario la República, 2024), ingeniero de sistemas especializado en inteligencia artificial, menciona lo siguiente: «La principal preocupación radica en que lo que ofrece Worldcoin, que es una identidad única a nivel mundial. Sabemos que el iris es algo que no se puede homologar y que no podrías encontrar un iris idéntico al tuyo» (párr. 5). Además, señala que esto puede sobrellevar riesgos como suplantación de identidad y robo de cuentas bancarias.

La ausencia de transparencia y las fallas éticas en el proceso de consentimiento informado en proyectos como World ID representan una amenaza directa a la autodeterminación informativa y a la dignidad de las personas, especialmente cuando se trata de datos biométricos inmodificables como el escaneo del iris. Además, el creciente uso de estas tecnologías por parte de entidades privadas sin suficiente fiscalización puede derivar en una asimetría de poder, donde las perso-

nas terminan cediendo su identidad a cambio de servicios o beneficios, sin plena conciencia de las implicancias de esa cesión. Barona (2024) señala que:

Las dudas éticas y de transparencia del consentimiento han llevado a cuestionar esta acción empresarial, que comporta la recopilación de datos biométricos sensibles, sin garantías respecto de un posible uso indebido y la protección de la información personal, amén del carácter irreversible del intercambio de datos a cambio de criptomonedas, aun cuando la empresa ha manifestado en diversos momentos que cualquier persona puede revocar el consentimiento sobre sus datos biométricos. (p.28)

Dando a entender que existe un gran riesgo estructural dentro de este sistema biométrico al transformar una necesidad económica en un contrato desigual, en donde la persona entrega datos de carácter muy sensible a cambio de una compensación, sin comprender realmente las consecuencias que podría traer. Barona (2024) también expresa su preocupación al constatar sobre casos de menores de edad que se han sometido a este proceso.

Un caso preocupante se presentó en Chile, donde un padre de familia presentó un recurso de protección ante la Corte de Apelaciones de Santiago contra la empresa encargada del sistema biométrico WorldCoin, alegando que escanearon el iris de su hija menor de edad sin un consentimiento ni autorización de sus apoderados. La corte lo declaró admisible el recurso, aun así, rechazó la orden de no innovar, puesto que la empresa alegó que este sistema es más exacto que la huella dactilar y reconocimiento facial, no recopilando datos personales. Sin embargo, el medio de investigación periodístico CIPER pudo constatar que: «las personas que acceden al escaneo de su iris, se les solicita nombre, correo electrónico, número telefónico y cuenta bancaria». (De Marval, 2024, párr. 1). Este caso ocurrido en territorio chileno evidencia de forma concreta los riesgos que puede implicar la implementación de tecnologías biométricas en la recolección de datos sumamente sensibles sin los debidos estándares legales, técnicos y éticos.

Este tipo de situaciones no son aisladas. En diversas partes del mundo, especialmente en países de Latinoamérica, se viene cuestionando la falta de regulación específica con respecto a este tipo de tecnologías que recopilan datos personales (IA, Big Data, sistemas biométricos). La ausencia de legislación clara y el escaso control estatal sobre el tratamiento de esta información han facilitado la expansión de proyectos que comprometen la privacidad de millones de ciudadanos, muchas veces sin que estos comprendan el verdadero alcance de su consentimiento. En este escenario, es indispensable analizar cómo estos riesgos también se están manifestando dentro de las fronteras del Perú.

V. HACIA UNA RECONSTRUCCIÓN CONSTITUCIONAL: INTERNET, PROTECCIÓN DE DATOS Y GARANTÍAS FRENTE A LA ERA DIGITAL

En el marco constitucional del Perú, podemos decir que el reconocimiento del «acceso libre» a internet ha creado un vacío normativo que permite la proliferación de amenazas digitales como la inteligencia artificial, el Big Data y la biometría digital, las cuales operan sin control adecuado procesando masivamente datos personales y vulnerando derechos fundamentales. Estas tecnologías, que van desde manipulación y tratamiento excesivo de datos por parte de algoritmos de inteligencia artificial, hasta sistemas biométricos como WorldID que comercializan la identidad física, evidencian la urgente necesidad de que el Estado peruano desarrolle marcos regulatorios integrales que protejan efectivamente los datos personales y garanticen el ejercicio pleno de los derechos digitales en esta nueva era tecnológica. El Estado peruano tiene la obligación y el deber constitucional de establecer límites y de garantizar transparencia ante los vacíos legales existentes con respecto a la protección de datos personales que se vulneran al acceder a internet, conforme al artículo 14- A, artículo 2 inciso 6 de la Constitución y la Ley 29733 – Ley de Protección de Datos Personales.

276

Para ello, se hace necesario formular una serie de presupuestos constitucionales mínimos, desde los cuales el Estado pueda diseñar políticas públicas, normas jurídicas y mecanismos de control eficaces que garanticen el respeto a la privacidad, la autodeterminación informativa y el acceso libre y seguro a internet como verdaderas garantías fundamentales.

VI. PRESUPUESTOS CONSTITUCIONALES PARA ENFRENTAR LA DEUDA CONSTITUCIONAL ANTE LA ERA DIGITAL

1. Presupuesto de interpretación integral del derecho al acceso a internet:

En primer lugar, como mencionamos anteriormente, existe la necesidad de una interpretación integral del derecho al acceso a internet «libre», el cual se encuentra reconocido en el artículo 14-A de la Constitución Política del Perú. Si bien la Ley 31878 (2023) lo incorporó como un derecho fundamental de toda persona dentro de nuestra carta madre, sigue permaneciendo una irregularidad dentro de su interpretación que exige comprender este derecho no solo como una prestación de conectividad, sino también como un derecho complejo en el que se necesita por parte del Estado dar garantías de calidad, seguridad y protección efectiva. Por otro lado, esta nueva y mejorada interpretación integral debe superar la visión de

un «acceso libre» para abarcar dimensiones también importantes como la culturización digital, la calidad del servicio, la protección frente a las nuevas amenazas digitales y el desarrollo de capacidades ciudadanas para el ejercicio pleno de este derecho en la era digital.

2. Presupuesto de integralidad y complementariedad con la protección de datos personales:

En la sociedad digital, para que una persona pueda ejercer efectivamente el derecho al acceso al internet es necesario que este derecho se encuentre conexo con el de protección de los datos personales o también llamado a la autodeterminación informativa. Ambos derechos están profundamente interconectados, puesto que inherentemente forman parte de un bloque digital de derechos fundamentales que debe ser reconocido por la Constitución Política del Perú. La conexión a internet implica, necesariamente, la exposición a plataformas, aplicaciones y servicios que recogen, procesan y analizan datos personales. Si el uso de internet no está acompañado de garantías mínimas sobre la privacidad, la seguridad y el control de la información personal, se configura una vulneración estructural de derechos. Esta complementariedad exige políticas públicas y marcos normativos articulados donde el internet no solo sea un vehículo de acceso, sino también un entorno regulado y seguro para el ciudadano digital.

277

3. Presupuesto de obligación estatal de garantía y protección

El Estado al garantizar el acceso libre al internet, tiene que la obligación positiva de dar medidas para su ejercicio seguro y protegido ante las nuevas amenazas digitales que abundan en la actualidad. Estas medidas van más allá de una provisión tecnológica a través de la inversión pública y privada del Estado tal como lo menciona el Artículo 14-A, sino que también implica el deber estatal de desarrollar marcos regulatorios preventivos y sancionadores que garanticen la protección de los ciudadanos al acceder a la red. En ese sentido, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (Citado por Cotino-Hueso, 2019) sirve como un referente comparado, dado que promueve y apuesta por el uso de mecanismos preventivos y proactivos en vez de solo reactivos, de modo que la privacidad se integre desde el inicio de tratamiento de datos personales. Es decir, este reglamento invita a no esperar que ocurra una violación a la privacidad para que recién el Estado actúe. Desde el momento en el que se crea una página web, sistema, software o inteligencia artificial, ya se deben incluir medidas de privacidad. Dando a entender que no se trata solo de reparar

violaciones, sino de evitarlas estructuralmente mediante diseños tecnológicos que respeten los derechos digitales de las personas. De este modo, la reconstrucción constitucional peruana no puede limitarse a solo proclamar derechos digitales, sino que debe adoptar incorporar una cultura jurídica de prevención tecnológica, donde se pueda proteger con efectividad los derechos digitales de los usuarios al acceder libremente a internet.

4. **Presupuesto de adaptación normativa ante las nuevas tecnologías**

El reconocimiento constitucional del derecho al acceso al internet busca una adaptación normativa permanente que permita al ordenamiento jurídico responder de manera eficaz a los desafíos generados por el avance acelerado de las tecnologías digitales. Esta exigencia conlleva la implementación de marcos legales flexibles y actualizables que regulen fenómenos como los algoritmos, la inteligencia artificial, el Big Data, la biometría o los *deepfakes*, incluyendo estándares éticos y mecanismos técnicos manteniendo siempre como núcleo la protección de la dignidad humana y los derechos fundamentales en el entorno digital.

VII. CONCLUSIONES

En conclusión, el reconocimiento constitucional del derecho al acceso al internet en el Perú, si bien constituye un avance jurídico relevante, resulta insuficiente para garantizar su ejercicio real y efectivo. La incorporación del artículo 14-A a la Constitución y la promulgación de la Ley 31878 han dejado sin resolver aspectos esenciales como la calidad del servicio, la continuidad del acceso, la equidad territorial y la alfabetización digital. Esta omisión evidencia que no basta con el reconocimiento formal del derecho, sino que es necesario un enfoque operativo que asegure su aplicación plena en condiciones de igualdad. El Estado debe asumir un rol activo en la implementación de políticas públicas que cierren la brecha digital existente.

El acceso a internet no puede ser concebido como un derecho autónomo aislado, sino como parte de un bloque de derechos digitales interconectados, en el cual la protección de datos personales, la privacidad y la seguridad digital son condiciones necesarias para su ejercicio efectivo. La coexistencia de estos derechos exige una lectura integral e indivisible, donde el libre acceso a la red no signifique la exposición a riesgos estructurales. La omisión de garantías mínimas frente al tratamiento de datos genera una vulneración directa a la autodeterminación informativa. Por tanto, la construcción de un entorno digital justo demanda marcos normativos articulados que aborden esta interdependencia.

La expansión de tecnologías emergentes como la inteligencia artificial, el Big Data, los *deepfakes* y los sistemas biométricos ha generado nuevas amenazas a los derechos fundamentales que no han sido adecuadamente enfrentadas por el ordenamiento jurídico peruano. Estas herramientas, en manos de actores sin control, pueden vulnerar la intimidad, la identidad digital, el honor y hasta la seguridad personal de los ciudadanos. Frente a ello, el enfoque normativo no puede ser reactivo, sino preventivo. Se requiere una legislación anticipatoria y especializada que regule estas tecnologías con enfoque ético, técnico y de derechos humanos, garantizando protección efectiva en un entorno cada vez más automatizado.

La realidad digital exige una reconstrucción constitucional del ecosistema de derechos en el Perú que supere el enfoque declarativo actual y avance hacia un modelo que combine acceso libre, protección, actualización normativa y seguridad jurídica. Esta transformación debe basarse en cinco presupuestos esenciales: interpretación integral del derecho al internet, complementariedad con la protección de datos personales, deber estatal de garantía, adaptación normativa frente a la innovación tecnológica y equilibrio entre libertad digital y seguridad. Solo mediante este enfoque estructural será posible consolidar una ciudadanía digital plena, protegida y participativa, alineada con los principios constitucionales y los desafíos del siglo XXI.

BIBLIOGRAFÍA

- Aguilar, J. V. (2024). *La protección de datos personales y su relación con los derechos digitales en la legislación peruana* [Tesis de pregrado] Universidad Nacional Mayor de San Marcos, Facultad de Derecho y Ciencia Política, Escuela Profesional de Derecho. Repositorio institucional Cybertesis UNMSM. <https://hdl.handle.net/20.500.12672/23685>
- Alva, G. W. (2023). *Reforma constitucional. Incorporan acceso a internet como derecho fundamental en Perú*. LP Derecho. <https://lpderecho.pe/reforma-constitucional-incorporan-acceso-internet-derecho-fundamental-peru/>
- Andina. (2025). *Más del 50 % de empresas en Perú cuenta con una estrategia de transformación digital* [Nota de prensa]. Agencia Peruana de Noticias Andina. <https://andina.pe/agencia/noticia-ac/noticia-mas-del-50-empresas-peru-cuenta-una-estrategia-transformacion-digital-1023167.aspx>
- Anzures, J. J. (2021). *Naturaleza jurídica y funciones del derecho humano a Internet*. *Boletín Mexicano De Derecho Comparado*, 1(158), 521–552. <https://doi.org/10.22201/ijj.24484873e.2020.158.15628>

- Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos. (2024). *MINJUSDH supervisa la recopilación de datos personales por Worldcoin* [Nota de prensa]. Gobierno del Perú. <https://www.gob.pe/institucion/anpd/noticias/965752-minjurdh-supervisa-la-recopilacion-de-datos-personales-por-worldcoin>
- Barona, S. (2024). *Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale. Actualidad jurídica iberoamericana*, 21, 298-331. <https://revista-aji.com/tecnologia-biometrica-y-datos-biometricos-bondades-y-peligros-no-todo-vale/>
- Buckley, O. (2023). *Inteligencia Artificial: el cada vez más frecuente uso de voces familiares clonadas para realizar estafas telefónicas (y cómo protegerse)*. *BBC News Mundo*. <https://www.bbc.com/mundo/articles/cz9q41r80n4o>
- Consejo Constitucional Francés. (2009). *Décision N° 2009580 DC – Loi favorisant la diffusion et la protection de la création sur internet* [Decisión]. *Journal officiel de la République française*. <https://www.conseil-constitutionnel.fr/es/decision/2009/2009580DC.htm>
- De Marval, V. (2024). *Datos personales a cambio de criptomonedas: padre presentó recurso porque escanearon el iris de su hija menor de edad*. *CIPER Chile*. <https://www.ciperchile.cl/2024/03/22/datos-personales-a-cambio-de-criptomonedas-padre-presento-recurso-porque-escanearon-el-iris-de-su-hija-menor-de-edad/>
- Decreto Supremo N.º 0162024JUS (2024) – *Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales* [PDF]. *Diario El Peruano*. <https://img.lpderecho.pe/wp-content/uploads/2024/11/Decreto-Supremo-016-2024-JUS-LPDerecho.pdf>
- Fernandes, A., Fernández, D., Molero, D., & Pérez, M. Á. (2025). *Deepfakes: Riesgos, casos reales y desafíos en la era de la IA* [Informe]. Observatorio de Deepfake, ISMS Forum. <https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf>
- Fernández, E. G. (2022). *Consideración del acceso a internet como un derecho humano: avances y perspectivas*. *Anales de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata*, 19(52), 117. <https://doi.org/10.24215/25916386e117>
- González, M. (2023). *El lado oscuro del Big Data como un problema social*. *Serie Científica De La Universidad De Las Ciencias Informáticas*, 16(9), 1-27. <https://publicaciones.uci.cu/index.php/serie/article/view/1421>

- Hernández, E. (2023). *Beneficios de la biometría digital para las empresas. AméricaEconomía*. <https://www.americaeconomia.com/analisis-y-opinion/beneficios-de-la-biometria-digital-para-las-empresas>
- Cotino-Hueso, L. (2019). *Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho. Revista general de Derecho administrativo*, 50, 1-37.
- Infobae. (2025). *Cae en Arequipa sujeto que creaba videos sexuales con IA: tenía más de 50 deepfakes de mujeres sin su consentimiento. Infobae Perú*. <https://www.infobae.com/peru/2025/06/19/cae-en-arequipa-creador-de-pornografia-con-ia-tenia-mas-de-50-deepfakes-sexuales-de-mujeres/>
- La Rue, F. (2011). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (A/HRC/17/27). Naciones Unidas*. <https://www.acnur.org/fileadmin/Documentos/BDL/2015/10048.pdf>
- Lacruz, M. L. (2025). *Los sistemas inteligentes de identificación y reconocimiento biométrico y los derechos humanos. Revista Peruana De Derecho Constitucional*, (16), 69–102. <https://revista.tc.gob.pe/index.php/revista/article/view/437>
- Mananí, M. F. (2023). *Derechos digitales de los grupos vulnerables en Perú: Un análisis integral [Artículo]. Chornancap. Revista Jurídica del Ilustre Colegio de Abogados de Lambayeque*, 1(2), 1–20. <https://doi.org/10.61542/rjch.45>
- Mendoza, M. (2023). *El cierre de la brecha no solo parte de la conectividad sino del desarrollo de capacidades – Dr. Erick Iriarte, CEO de eBIZ | Especial Ley de Acceso a Internet como Derecho. eBIZ.pe*. <https://ebiz.pe/noticias/especial-sobre-la-ley-de-acceso-a-internet-como-derecho-erick-iriarte/>
- Miranda, H. (2016). *El acceso a Internet como derecho fundamental. Revista Jurídica IUS Doctrina*, 9(15). <https://revistas.ucr.ac.cr/index.php/iusdoctrina/article/view/27476>
- Monge, G. J. (2023). *Reforma constitucional: ¿qué significa que el acceso “libre” a internet sea un derecho fundamental? Echeconpar*. <https://www.echeconpar.com.pe/publicaciones-reforma-constitucional-que-significa-que-el-acceso-libre-a-internet-sea-un-derecho-fundamental.html>
- Morales, A. (2020). *El impacto de la inteligencia artificial en la protección de datos personales. World Compliance Association*. <https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccion-de-datos-personales.html>

- Mubarak, L. (2020). *El Internet, el Big Data y el tratamiento de datos personales. Advocatus*, (036), 205-223. <https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/4800>
- Olivos, M. (2018). *La protección de la privacidad como objeto de tutela en el ordenamiento jurídico peruano. IUS: Revista De investigación De La Facultad De Derecho*, 8(1), 47-67. <https://doi.org/10.35383/ius.v1i1.38>
- Prince, Á. C. (2020). *El acceso a Internet como derecho fundamental: perspectivas internacionales. Revista Justicia & Derecho*, 3(1), 1–19. <https://revistas.uaautonoma.cl/index.php/rjyd/article/view/456>
- Redacción Gestión. (2024). *Ciberdelincuentes utilizan deepfakes de figuras públicas para estafar a los usuarios* [Artículo de tecnología]. *Gestión*. <https://gestion.pe/tecnologia/ciberdelincuentes-utilizan-deepfakes-de-figuras-publicas-para-estafar-a-los-usuarios-kaspersky-ciberseguridad-noticia/>
- Roel, L. A., Chocano, E. J., & Salazar, P. M. (2025). *Las nuevas tecnologías y el daño al derecho a la autodeterminación informativa y derechos conexos. La IA como una nueva amenaza para los derechos fundamentales. Revista Peruana De Derecho Constitucional*, (16), 159–191. <https://revista.tc.gob.pe/index.php/revista/article/view/440>
- Torres, A. L. (2025). *El área gris de las denuncias contra el deepfake que también afecta a empresas en Perú. G de Gestión*.