Derechos digitales: un marco integral para la gobernanza y la educación en la era de la información

Digital rights: a comprehensive framework for governance and education in the information age

Autores: Idarmis Knight Soto, Diogo Clemente Neto, Secundino Arce Mendieta, Federico Sánchez Riaño

DOI: https://doi.org/10.19053/uptc.16923936.v23.n46.2025.20647

Para citar este artículo:

Knight Soto, I., Clemente Neto, D., Arce Mendieta, S., & Sánchez Riaño, F. (2025). Derechos digitales: un marco integral para la gobernanza y la educación en la era de la información. *Derecho y Realidad, 23* (46), 131-150

DERECHOS DIGITALES: UN MARCO INTEGRAL PARA LA GOBERNANZA Y LA EDUCACIÓN EN LA ERA DE LA INFORMACIÓN*

Digital Rights: A Comprehensive Framework for Governance and Education in the Information Age

Direitos digitais: um marco abrangente para a governança e a educação na era da informação

Idarmis Knight Soto
Profesora Titular. Universidad de Ciego de Ávila. Máximo Gómez.
ORCID: 0000-0003-4713-7488
idarmisknightsoto@gmail.com

Diogo Clemente Neto
Estudiante de Doctorado Universidad OMI Centro de Investigación. Campus México.
ORCID 0009-0009-1390-458X

Secundino Arce Mendieta
Profesor Instructor Universidad Ciego de Ávila. Máximo Gómez Báez.
ORCID: 0009-0001-8234-2324
tomarce.totin@gmail.com

Federico Sánchez Riaño
Doctor en comunicación de la Universidad Nacional de la Plata.
ORCID: 0000-0001-5935-4143
cotidianocreativo@gmail.com

Recepción: Octubre 18 de 2025
Aceptación: Noviembre 17 de 2025

RESUMEN

Este artículo propone un marco integrado para comprender, proteger y promover los derechos digitales en un contexto de acelerada transformación tecnológica y creciente interconexión global. Partimos de la tesis de que la protección efectiva de los derechos digitales requiere una articulación tripartita entre (i) gobernanza normativa, (ii) educación crítica y (iii) participación ciudadana, sin la que los marcos regulatorios resultarán insuficientes frente al dinamismo tecnológico y las asimetrías de poder que caracterizan el ecosistema digital contemporáneo.

La era digital exige una nueva generación de derechos asentados conceptualmente sobre un soporte virtual donde la corporalidad se transforma para dar paso a una estructura de

* Artículo de reflexión

derechos que debe garantizar la seguridad de la persona frente al tratamiento de datos y la arquitectura matemática de los algoritmos. A través de un análisis doctrinal, normativo y comparado, complementado con el estudio de casos emblemáticos, el trabajo conecta preocupaciones jurídicas, sociopolíticas y pedagógicas para promover una ciudadanía digital informada y protegida frente a abusos, vigilancia desproporcionada y discriminación algorítmica, garantizando equidad, transparencia y rendición de cuentas.

PALABRAS CLAVE

Derechos digitales; gobernanza algorítmica; alfabetización digital crítica; protección de datos; inteligencia artificial; ciudadanía digital.

ABSTRACT

This article proposes an integrated framework to understand, protect, and promote digital rights in a context of accelerated technological transformation and increasing global interconnection. We begin from the thesis that the effective protection of digital rights requires a tripartite articulation among (i) normative governance, (ii) critical education, and (iii) citizen participation. Without this articulation, regulatory frameworks will remain insufficient in the face of technological dynamism and power asymmetries that characterize the contemporary digital ecosystem.

The digital age demands a new generation of rights, conceptually grounded in a virtual environment where corporeality is transformed, giving rise to a rights structure that must ensure personal security regarding data processing and the mathematical architecture of algorithms. Through doctrinal, normative, and comparative analysis, complemented by the study of emblematic cases, this work connects legal, sociopolitical, and pedagogical concerns to promote an informed digital citizenship protected against abuses, disproportionate surveillance, and algorithmic discrimination, ensuring equity, transparency, and accountability.

KEYWORDS

Digital rights; algorithmic governance; critical digital literacy; data protection; artificial intelligence; digital citizenship.

RESUMO

Este artigo propõe um marco integrado para compreender, proteger e promover os direitos digitais em um contexto de acelerada transformação tecnológica e crescente interconexão global. Parte-se da tese de que a proteção efetiva dos direitos digitais requer uma articulação tripartite entre (i) governança normativa, (ii) educação crítica e (iii) participação cidadã, sem a qual os marcos regulatórios se mostram insuficientes diante do dinamismo tecnológico e das assimetrias de poder que caracterizam o ecossistema digital contemporâneo.

A era digital exige uma nova geração de direitos assentados conceitualmente sobre um suporte virtual, no qual a corporalidade se transforma para dar lugar a uma estrutura de direitos que deve garantir a segurança da pessoa frente ao tratamento de dados e à arquitetura matemática dos algoritmos. Por meio de uma análise doutrinária, normativa e comparada, complementada pelo estudo de casos emblemáticos, o trabalho articula preocupações jurídicas, sociopolíticas e pedagógicas para promover uma cidadania digital informada e protegida contra abusos, vigilância desproporcional e discriminação algorítmica, assegurando equidade, transparência e prestação de contas.

PALAVRAS-CHAVE

Direitos digitais; governança algorítmica; alfabetização digital crítica; proteção de dados; inteligência artificial; cidadania digital.

INTRODUCTION

La revolución digital ha transformado radicalmente las condiciones de existencia humana en el siglo XXI. Las tecnologías de la información y la comunicación no constituyen meras herramientas instrumentales, sino que configuran un

nuevo entorno ontológico —lo que Floridi (2020) denomina la "infosfera"— donde se desarrollan dimensiones fundamentales de la vida personal, social, económica y política. En este contexto, los derechos digitales emergen como una extensión lógica e ineludible de la dignidad humana, reclamando un reconocimiento específico que trasciende la aplicación analógica de categorías jurídicas tradicionales.

En ese sentido, el Consejo de Derechos Humanos de las Naciones Unidas reafirmó, en 2016, que los mismos derechos que las personas tienen en el mundo no virtual deben protegerse en el mundo digital (Nitsche & Hairsine, 2016). Sin embargo, esta declaración de principios, aunque valiosa, resulta insuficiente para abordar la complejidad de los desafíos contemporáneos. La arquitectura técnica de Internet, el funcionamiento opaco de los algoritmos de aprendizaje automático, la concentración oligopólica de las plataformas digitales y la economía extractiva de datos personales plantean problemas cualitativamente nuevos que exigen respuestas normativas, institucionales y educativas igualmente innovadoras.

La tesis central de este trabajo sostiene que la protección efectiva de los derechos digitales no puede descansar exclusivamente en marcos regulatorios —por sofisticados que estos sean (o parezcan)—, sino que requiere una articulación tripartita entre gobernanza normativa, educación crítica y participación ciudadana. Sin esta triple dimensión, los instrumentos jurídicos corren el riesgo de ser ineficaces frente al dinamismo tecnológico, las asimetrías informativas y la captura regulatoria por intereses corporativos. Como advierte Zuboff (2019), el *capitalismo de vigilancia* no solo extrae datos, sino que moldea comportamientos y erosiona las condiciones mismas de la autonomía que los derechos pretenden proteger.

Los derechos digitales comprenden tanto la actualización de derechos tradicionales en el entorno digital —privacidad, libertad de expresión, acceso a la información— como el reconocimiento de derechos emergentes que responden a desafíos específicos de la era tecnológica: el derecho de acceso universal a Internet, la protección frente a decisiones automatizadas, el derecho a la desconexión digital, la protección contra la desinformación algorítmica y el derecho a la explicabilidad de los sistemas de inteligencia artificial (Barrio, 2021; Mantelero, 2022).

Según la conceptualización de Cova-Fernández (2019), estos derechos están vinculados con un ecosistema tecnológico que incluye Internet; las TIC; el Big Data; la computación en la nube; la inteligencia artificial; el Internet de las cosas y los procesos telemáticos. Su adecuada protección debe —y requiere— promover la inclusión digital y el humanismo tecnológico, entendiendo que la tecnología debe servir al desarrollo integral del ser humano y no a su subordinación. Byung-Chul Han, 2012, en su obra *La sociedad del cansancio*, ha dejado claras las consecuencias de esta inversión.

Este artículo se estructura en cinco secciones principales. La primera examina los fundamentos normativos de la privacidad y la protección de datos. La segunda analiza los desafíos que la inteligencia artificial plantea a los derechos humanos. La tercera aborda la gobernanza y legitimidad del ecosistema digital. La cuarta desarrolla el papel de la educación digital crítica como condición de posibilidad para el ejercicio efectivo de los derechos. La quinta ofrece un análisis comparado de experiencias regulatorias y casos emblemáticos. Las conclusiones sintetizan las propuestas normativas y pedagógicas derivadas del análisis.

1. Privacidad y protección de datos: consentimiento informado, minimización de datos, finalidad, seguridad por diseño y derechos de acceso, rectificación y supresión

La privacidad constituye un pilar esencial de los derechos humanos, vinculada directamente con la autonomía individual y

la dignidad humana (Westin, 1967; Solove, 2021). Sin embargo, su conceptualización ha experimentado transformaciones sustanciales en el entorno digital. Mientras que la noción clásica de privacidad enfatizaba el "derecho a ser dejado solo" (Warren & Brandeis, 1890), las condiciones contemporáneas exigen una reconceptualización que incorpore dimensiones informacionales, contextuales y relacionales.

Nissenbaum (2010) propone el concepto de *integridad contextual* para comprender la privacidad en entornos digitales. Según este enfoque, las expectativas de privacidad no son absolutas sino contextualmente determinadas: la información que compartimos legítimamente en un contexto (médico, educativo, comercial) no debería fluir hacia otros contextos sin nuestro conocimiento y consentimiento. Esta perspectiva resulta particularmente relevante para evaluar las prácticas de las plataformas digitales que, muchas veces, descontextualizan la información personal y la comercializan para fines no anticipados por los usuarios.

La monetización de los datos personales ha alcanzado dimensiones impensables hasta hace poco. Como documenta Zuboff (2019), el capitalismo de vigilancia se sustenta en la extracción masiva de *excedente conductual* —datos sobre comportamientos, preferencias, relaciones y movimientos— que alimentan modelos predictivos comercializados en *mercados de futuros conductuales*. Este modelo de negocio, que subyace a las principales plataformas digitales, plantea amenazas estructurales a la autonomía individual que trascienden las violaciones puntuales de privacidad.

Lo anterior quiere decir que, más allá de la transgresión normativa, nos enfrentamos a toda una forma de producción del otro, a partir de la necesidad de un mercado voraz que solo busca expandirse y controlar nichos de mercado; nichos en los que acabamos incluidos sin que lo queramos ni sepamos.

Por otro lado. el marco normativo contemporáneo de protección de datos se articula en torno a principios fundamentales que —si bien con variaciones jurisdiccionales—, conforman un consenso internacional emergente.

El consentimiento informado constituye la piedra angular de la legitimidad del tratamiento de datos personales. Para ser válido, debe ser libre, específico, informado e inequívoco, permitiendo a las personas ejercer control significativo sobre su información y comprender las finalidades, destinatarios y plazos del tratamiento (RGPD, 2016, art. 7). Sin embargo, la práctica revela limitaciones estructurales: las políticas de privacidad son extensas, técnicamente complejas e intencionalmente oscuras; las opciones se presentan como binarias (aceptar o no usar el servicio); y la fatiga del consentimiento erosiona la atención de los usuarios (Solove, 2013). Por ello, el consentimiento debe complementarse con salvaguardas objetivas que no dependan exclusivamente de la vigilancia individual.

El principio de minimización establece que deben recogerse únicamente los datos estrictamente necesarios para cumplir una finalidad legítima, evitando la recopilación excesiva, especulativa o residual. Este principio no solo protege a los titulares, sino que facilita la responsabilidad organizacional al reducir los riesgos de seguridad y las superficies de ataque. Su implementación requiere una arquitectura de datos basada en la necesidad demostrable, políticas de conservación temporalmente limitadas y mecanismos de anonimización efectiva (Cavoukian, 2012).

La limitación de finalidad exige que los datos se recojan para propósitos determinados, explícitos y legítimos, sin que puedan tratarse ulteriormente de manera incompatible con dichos fines. Este principio enfrenta tensiones significativas con las prácticas de Big Data y aprendizaje automático, donde el valor de los datos frecuentemente emerge de usos no anticipados en el momento de la recolección (Mayer-Schönberger & Cukier, 2013).

La seguridad por diseño (privacy by design), conceptualizada por Cavoukian (2012), implica incorporar salvaguardas desde las primeras fases de desarrollo de productos y servicios. Este enfoque proactivo —en contraposición a la remediación reactiva— exige la aplicación

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

de medidas técnicas: cifrado robusto, control granular de accesos, registros de auditoría, evaluaciones de impacto y protocolos de eliminación segura. El RGPD europeo codificó este principio al exigir "protección de datos desde el diseño y por defecto" (art. 25).

Se debe destacar que los marcos normativos contemporáneos reconocen un conjunto de derechos que empoderan a las personas frente al tratamiento de sus datos.

El derecho de acceso permite conocer qué datos personales se procesan, con qué finalidades, a qué destinatarios se comunican y durante cuánto tiempo se conservarán. Este derecho constituye la condición de posibilidad para el ejercicio de los demás derechos, pues sin conocimiento no hay control.

El derecho de rectificación faculta a solicitar la corrección de datos inexactos o incompletos, protegiendo la integridad informacional de la persona y previniendo decisiones basadas en información errónea.

El derecho de supresión —conocido como "derecho al olvido" tras la sentencia Google Spain del TJUE (2014)— permite exigir la eliminación de datos cuando ya no sean necesarios para los fines que motivaron su tratamiento, cuando se retire el consentimiento o cuando el tratamiento sea ilícito (Torres, 2017). Este derecho, sin embargo, debe ponderarse con otros intereses legítimos como la libertad de información y la preservación de registros históricos.

El derecho a la portabilidad representa una innovación significativa que permite recibir los datos personales en formato estructurado y transferirlos a otro responsable, reduciendo los costos de cambio entre servicios y promoviendo la competencia en mercados digitales (De Hert et al., 2018).

Para la efectividad de estos derechos se requieren procedimientos accesibles, interfaces comprensibles y plazos razonables de respuesta, respaldados por mecanismos técnicos que aseguren la supresión integral de la información y sus copias (Knight et al., 2024).

2. Inteligencia artificial y derechos humanos: transparencia, trazabilidad, no discriminación, salvaguardas y mecanismos de reparación

La inteligencia artificial —entendida como sistemas computacionales capaces de realizar tareas que típicamente requieren inteligencia humana— está reconfigurando las dinámicas de decisión, control y poder en prácticamente todos los ámbitos de la vida social (Floridi & Cowls, 2021). A diferencia de tecnologías anteriores, los sistemas de IA pueden operar con limitada intervención humana, lo que exige su diseño bajo un enfoque de derechos desde su concepción, conocido como *human rights by design* (Knight & Delgado, 2025, p. 74). Además, estos sistemas aprenden de datos históricos que incorporan sesgos sociales y producen resultados cuya lógica resulta opaca incluso para sus desarrolladores.

Esta opacidad plantea un desafío fundamental para el Estado de Derecho: ¿cómo pueden los ciudadanos impugnar decisiones que les afectan si no comprenden —ni pueden comprender— cómo se tomaron? ¿Cómo pueden los tribunales ejercer control jurisdiccional sobre sistemas cuyo funcionamiento es técnicamente inaccesible? ¿Cómo pueden los legisladores regular tecnologías cuyas capacidades evolucionan más rápido que los procesos normativos? Como advierte Binns (2018), los debates sobre equidad algorítmica no pueden resolverse únicamente con soluciones técnicas, pues involucran concepciones normativas en disputa sobre justicia distributiva, igualdad de oportunidades y no discriminación.

La transparencia constituye la base de la rendición de cuentas en sistemas automatizados y comprende múltiples dimensiones: la existencia misma del tratamiento, las fuentes de datos, la lógica del procesamiento y las consecuencias previstas (Goodman & Flaxman, 2017; OECD, 2022). Los objetivos, supuestos y criterios de decisión deben ser comprensibles y, cuando corresponda, sujetos a revisión por autoridades o evaluadores independientes.

En el marco europeo, el Reglamento General de Protección de Datos reconoce el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado que produzcan efectos jurídicos o afecten significativamente de modo similar (art. 22), así como el derecho a obtener información significativa sobre la lógica aplicada (arts. 13-15). No obstante, la implementación práctica enfrenta obstáculos técnicos —como la complejidad de los modelos de aprendizaje profundo—, comerciales —como la protección del secreto empresarial— y epistemológicos —como los límites de la explicabilidad *post hoc* (Doshi-Velez & Kim, 2017)—.

La trazabilidad de las decisiones algorítmicas resulta crucial para reconstruir y auditar cada fase del procesamiento, desde la recolección de datos hasta la generación de resultados. Permite detectar sesgos, errores y atribuir responsabilidades en ámbitos de alto impacto como justicia penal, educación, empleo o acceso al crédito (OECD, 2022; Goodman & Flaxman, 2017).

Los sistemas de IA pueden perpetuar, amplificar o incluso crear nuevas formas de discriminación. Los sesgos pueden introducirse en múltiples etapas: en los datos de entrenamiento que reflejan desigualdades históricas, en variables proxy que correlacionan con categorías protegidas, en funciones objetivo que optimizan métricas sesgadas o en la aplicación diferencial de modelos en contextos heterogéneos (Barocas, Hardt & Narayanan, 2023). El caso COMPAS en Estados Unidos ilustra estos riesgos: una investigación de ProPublica (2016) reveló tasas de error significativamente dispares por raza, lo que abrió un debate académico sobre concepciones de equidad e incompatibilidades matemáticas (Kleinberg et al., 2017).

La prevención de la discriminación algorítmica requiere auditorías previas al despliegue, evaluaciones de impacto, diversidad en los equipos de desarrollo y mecanismos de monitoreo continuo. La Ley de Inteligencia Artificial de la Unión Europea (European Commission, 2024) establece salvaguardas diferenciadas según niveles de riesgo, prohibiendo sistemas que manipulen comportamientos o exploten vulnerabilidades, y exigiendo supervisión humana significativa (*meaningful human oversight*) y mecanismos de explicabilidad por diseño y por defecto.

La explicabilidad y la interoperabilidad son condiciones esenciales para la protección de derechos. Aunque algunas técnicas de aprendizaje profundo presentan limitaciones interpretativas, debe garantizarse una comprensión razonable de cómo se toman las decisiones y qué datos influyen en ellas, especialmente en sectores sensibles como salud, educación o administración pública (Doshi-Velez & Kim, 2017). Ello sostiene derechos como la información, la impugnación y la reparación.

Los mecanismos de reparación frente a decisiones automatizadas deben ser accesibles, efectivos y oportunos. Incluyen la revisión humana, la corrección de errores de datos, la posibilidad de impugnar resultados injustos y la compensación cuando se acredite la vulneración de derechos (Knight, 2015, p. 10).

Asimismo, la protección de la privacidad en IA exige adaptar principios tradicionales —consentimiento, minimización, finalidad legítima y seguridad por diseño— a entornos de aprendizaje automático, reconocimiento facial y procesamiento masivo de datos. Una gobernanza responsable debe garantizar que las personas conserven control sobre su información y que los sistemas operen dentro de límites éticos y jurídicos bien definidos.

Las brechas regulatorias en materia de derechos digitales revelan un desafío estructural: la tecnología avanza más rápido que la legislación, lo que genera riesgos de exclusión, vigilancia indebida y erosión de la confianza pública (Hugo, 2023, p. 19; Renda, 2023).

En síntesis, la integración de los derechos humanos en el diseño y la aplicación de la IA exige un enfoque sistémico basado en transparencia, trazabilidad, no discriminación, salvaguardas y reparación. Este modelo debe expresarse en normas claras, gobernanza ética, responsabilidad corporativa y participación cívica, para aprovechar el potencial

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

transformador de la IA sin sacrificar derechos fundamentales ni profundizar desigualdades sociales.

Las salvaguardas frente a la IA abarcan medidas técnicas y organizativas que deben integrarse por diseño y por defecto en el ciclo de vida de los sistemas. Incluyen la supervisión humana significativa, la explicabilidad de las decisiones, la documentación exhaustiva, las pruebas de robustez y los mecanismos de desactivación (European Commission, 2024). La supervisión humana no debe reducirse a una formalidad ritual —el mero "sello de goma" que valida automáticamente las recomendaciones algorítmicas— sino constituir una instancia de revisión genuina, con capacidad efectiva de modificar, rechazar o complementar los resultados automatizados. Para ello, los operadores deben contar con información comprensible, tiempo suficiente, formación adecuada e incentivos institucionales que favorezcan el escrutinio crítico (Green & Chen, 2019).

Los mecanismos de reparación frente a decisiones automatizadas deben ser accesibles, efectivos y oportunos. Comprenden la notificación del uso de sistemas automatizados, la posibilidad de solicitar revisión humana, la corrección de errores en los datos o en el modelo, la impugnación de resultados discriminatorios y la compensación cuando se verifique daño (Knight, 2015; Kaminski, 2019). Su efectividad depende, además, de condiciones institucionales frecuentemente ausentes: la existencia de autoridades con competencia técnica y recursos para investigar reclamaciones, la inversión de la carga probatoria cuando existe opacidad algorítmica, la disponibilidad de remedios colectivos para daños difusos pero sistemáticos y la existencia de sanciones disuasorias para los responsables.

3. Gobernanza y legitimidad: marco normativo, proporcionalidad, supervisión independiente y recursos judiciales efectivos

La gobernanza tecnológica contemporánea enfrenta un desfase estructural: la velocidad del cambio tecnológico supera sistemáticamente la capacidad de respuesta de los procesos legislativos tradicionales (Marchetti, 2022). Cuando las normas finalmente se aprueban, las tecnologías que pretendían regular han evolucionado, las empresas han desarrollado estrategias de evasión y los daños que se buscaba prevenir ya se han materializado. Esta brecha afecta la coherencia y la actualización normativa, generando vacíos que permiten prácticas lesivas como la explotación de datos, la manipulación algorítmica o la discriminación automatizada (Bonilla-Morejón, 2023; Fernández & Díaz Lafuente, 2022).

Estos vacíos se manifiestan particularmente en ámbitos como las criptomonedas y finanzas descentralizadas, los sistemas generativos de IA, las interfaces cerebro-computadora, los deepfakes y la desinformación sintética, o las tecnologías de vigilancia biométrica masiva. La ausencia de marcos normativos actualizados genera riesgos de exclusión, vigilancia indebida y erosión de la confianza pública (Hugo, 2023; Renda, 2023).

Frente a este desafío, algunos autores proponen modelos de regulación ágil o experimentalista que permitan ajustes iterativos mediante sandboxes regulatorios, cláusulas de revisión obligatoria y participación continua de actores relevantes (Marchetti, 2022). Otros subrayan la importancia de regulaciones basadas en principios lo suficientemente abstractos para adaptarse a desarrollos imprevistos, complementadas con estándares técnicos flexibles.

El principio de proporcionalidad se erige como piedra angular de la legitimidad regulatoria en materia tecnológica. Toda medida que restrinja derechos fundamentales —incluidas restricciones al tratamiento de datos o al despliegue de sistemas de IA— debe superar un test de idoneidad, necesidad y proporcionalidad en sentido estricto. Este principio no es solo un instrumento técnico-jurídico: también orienta la acción pública hacia un equilibrio entre innovación y protección de derechos.

Su aplicación rigurosa exige evaluaciones de impacto en derechos humanos (EIDH) antes

de la adopción de políticas o tecnologías de amplio alcance. Tales evaluaciones deben identificar efectos adversos potenciales, especialmente sobre grupos vulnerables, prever mecanismos de mitigación y establecer revisiones periódicas. La práctica de evaluación ex ante y ex post contribuye a la transparencia y responsabilidad de las decisiones regulatorias (Mantelero, 2022).

La jurisprudencia del Tribunal Europeo de Derechos Humanos ha aportado criterios operativos sobre proporcionalidad aplicados a la vigilancia digital. En Big Brother Watch v. Reino Unido (2021), el TEDH sostuvo que los programas de vigilancia masiva requieren autorización judicial previa, supervisión independiente y salvaguardas específicas para proteger derechos como el privilegio profesional de periodistas y abogados.

La supervisión independiente constituye un pilar esencial de la gobernanza tecnológica democrática. Los organismos de control —autoridades de protección de datos, agencias de competencia o reguladores sectoriales— deben contar con autonomía funcional, resources adecuados y acceso irrestricto a la información relevante. Su legitimidad exige mandatos claros, competencias para realizar auditorías algorítmicas, verificar políticas de protección de datos, evaluar equidad en decisiones automatizadas y emitir sanciones o correcciones vinculantes.

El modelo de las autoridades de protección de datos, consolidado tras el RGPD, ofrece lecciones valiosas pero también evidencia limitaciones: recursos insuficientes frente a actores globales, dificultades de coordinación transfronteriza y riesgos de captura regulatoria. El Comité Europeo de Protección de Datos ha intentado paliar estas brechas mediante mecanismos de coherencia, aunque persisten divergencias significativas entre autoridades nacionales.

Para el ámbito específico de la IA, se están desarrollando nuevos modelos institucionales. La Ley de IA europea crea la Oficina Europea de IA y prevé autoridades nacionales de supervisión con facultades para realizar auditorías, acceder a código fuente y ordenar la retirada de sistemas no conformes. La efectividad de esta arquitectura institucional dependerá de la dotación de recursos, la independencia real y la voluntad de enforcement.

Los recursos judiciales efectivos resultan indispensables para la protección de derechos en entornos tecnológicos. Las personas deben contar con vías accesibles para impugnar decisiones algorítmicas, reclamar vulneraciones de privacidad y obtener reparación por daños digitales. Sin embargo, la litigación individual enfrenta obstáculos estructurales: asimetrías informativas, costos elevados, dificultades probatorias derivadas de la opacidad técnica y efectos difusos que desalientan la acción individual. En este contexto, son cruciales los mecanismos de tutela colectiva —acciones de clase, legitimación de organizaciones de consumidores o acciones de interés público— que permitan agregar reclamaciones y distribuir costos.

A ello se suma el desafío de la especialización judicial. Los conflictos digitales involucran cuestiones técnicas que exceden la formación tradicional de jueces y abogados. Algunas jurisdicciones han creado tribunales especializados o incorporado peritos de oficio, pero la brecha entre complejidad tecnológica y capacidad institucional persiste. La reparación debe ser integral, abarcando tanto daños materiales y morales como los costos derivados de mitigar impactos tecnológicos adversos.

La legitimidad de la gobernanza tecnológica no depende únicamente de su arquitectura normativa e institucional: requiere procesos inclusivos de deliberación. La participación activa de la sociedad civil, la academia, las comunidades afectadas y el sector privado en la definición de normas y estándares reduce asimetrías de poder y fortalece la legitimidad democrática. Este enfoque colaborativo resulta indispensable en un entorno donde las decisiones regulatorias tienen consecuencias sociales amplias y distribuidas.

La transparencia regulatoria desempeña una función estratégica. Publicar los fundamentos de las políticas, criterios de decisión, análisis de riesgo y evaluaciones de

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

impacto fomenta la comprensión ciudadana, habilita el escrutinio independiente y fortalece la confianza pública. Sin embargo, la transparencia debe gestionarse equilibrando la protección de secretos industriales y la seguridad comercial sin sacrificar el derecho ciudadano a la información.

La naturaleza transfronteriza de los flujos de datos y de las operaciones de las plataformas digitales reclama respuestas coordinadas que trasciendan las jurisdicciones nacionales. Persisten divergencias profundas entre modelos regulatorios: el enfoque europeo basado en derechos fundamentales, el modelo estadounidense de autorregulación sectorial, el paradigma chino de soberanía digital y control estatal, y las aproximaciones emergentes en América Latina, África e India. Esta fragmentación facilita estrategias de arbitraje jurisdiccional, incrementa la incertidumbre jurídica y alimenta carreras regulatorias hacia estándares mínimos.

Los esfuerzos de armonización —como el antiguo Privacy Shield declarado inválido en Schrems II, las cláusulas contractuales tipo, el Convenio 108+ o los trabajos de la OCDE y UNESCO en IA— representan avances parciales. Una gobernanza global efectiva exigiría mecanismos de reconocimiento mutuo basados en equivalencia sustantiva que, sin imponer uniformidad, garanticen estándares mínimos de protección coherentes con los derechos humanos.

4. Educación digital crítica: fundamentos, modelos y propuestas

Si los derechos digitales constituyen una extensión de los derechos humanos en el entorno tecnológico, la alfabetización digital crítica representa la condición de posibilidad para su ejercicio efectivo. Sin las competencias necesarias para comprender el funcionamiento del ecosistema digital, identificar riesgos, proteger la privacidad y participar informadamente en procesos deliberativos, los ciudadanos quedan reducidos a usuarios pasivos cuyo consentimiento es formal pero no sustantivo.

La alfabetización digital excede ampliamente las competencias instrumentales —saber usar dispositivos, navegar por internet, operar aplicaciones—. Como argumenta Buckingham (2019), requiere una dimensión crítica que permita comprender las condiciones de producción de los contenidos digitales, los modelos de negocio de las plataformas, los sesgos de los algoritmos de recomendación y las técnicas de persuasión y manipulación empleadas en el diseño de interfaces.

Hobbs (2020) propone un marco de alfabetización mediática que integra cinco competencias interrelacionadas: acceso (habilidades técnicas y disponibilidad de infraestructura), análisis (deconstrucción crítica de mensajes), creación (producción de contenidos), reflexión (consideración ética del propio comportamiento) y acción (participación cívica informada). Este enfoque integral supera la visión reduccionista de la alfabetización como protección defensiva frente a riesgos, para concebirla como empoderamiento para la participación democrática.

Una dimensión particularmente urgente de la educación digital contemporánea es la alfabetización algorítmica: la capacidad de comprender cómo los algoritmos median nuestra experiencia del mundo, qué datos utilizan, qué criterios optimizan y qué consecuencias producen (Kitchin, 2017).

Los algoritmos de las plataformas digitales no son meros intermediarios neutrales que facilitan la conexión entre usuarios y contenidos. Son sistemas de curación activa que seleccionan, ordenan, filtran y recomiendan información según criterios diseñados para maximizar engagement, tiempo de uso y, en última instancia, ingresos publicitarios. Estos sistemas crean "burbujas de filtro" que limitan la exposición a perspectivas diversas (Pariser, 2011) y pueden amplificar contenidos sensacionalistas, polarizantes o desinformativos que generan mayor reacción emocional (Vosoughi et al., 2018).

La alfabetización algorítmica debe incluir conocimientos básicos sobre cómo funcionan los sistemas de recomendación, los motores de búsqueda y la publicidad programática;

habilidades para identificar contenido promocionado o patrocinado; conciencia de la personalización y sus efectos en la diversidad informativa; y capacidad para ajustar configuraciones de privacidad y preferencias algorítmicas. Esto no requiere formación técnica avanzada, sino una comprensión conceptual accesible de los principios básicos.

La proliferación de desinformación —información falsa difundida con intención de engañar— y misinformación —información errónea difundida sin intención deliberada— constituye uno de los desafíos más apremiantes del ecosistema informativo contemporáneo. Las tecnologías generativas de IA han amplificado exponencialmente este problema al permitir la creación de contenido sintético convincente (deepfakes de video, audio clonado, textos generados) a bajo costo y escala masiva.

La respuesta educativa no puede limitarse al fact-checking reactivo —verificar afirmaciones específicas— sino que debe desarrollar lo que Wineburg y McGrew (2019) denominan "lectura lateral": la práctica de verificar fuentes consultando información externa sobre su credibilidad, en lugar de evaluar el contenido aisladamente. Los estudios empíricos muestran que los verificadores profesionales emplean sistemáticamente esta estrategia, mientras que los ciudadanos comunes —e incluso académicos— tienden a evaluar la credibilidad basándose en características superficiales del contenido.

La educación contra la desinformación debe también abordar las dimensiones afectivas y sociales del fenómeno. La difusión de información falsa frecuentemente responde a necesidades de pertenencia grupal, confirmación de creencias previas o expresión de identidades políticas (Marwick, 2018). Las intervenciones puramente cognitivas resultan insuficientes si no consideran estas motivaciones sociales y emocionales.

Ética digital y responsabilidad en entornos conectados

La educación digital debe incorporar una dimensión ética que prepare a las personas para navegar los dilemas morales específicos del entorno digital: cuestiones de privacidad propia y ajena, el equilibrio entre libertad de expresión y discurso de odio, la responsabilidad en la difusión de información, el respeto a la propiedad intelectual, el comportamiento en comunidades virtuales y las implicaciones del rastro digital permanente (Floridi, 2020).

Esta formación ética no debe adoptar un enfoque prescriptivo de reglas rígidas, sino desarrollar capacidades de deliberación moral que permitan a las personas evaluar situaciones complejas, considerar perspectivas múltiples y tomar decisiones reflexivas. El objetivo es formar agentes morales autónomos capaces de aplicar principios éticos a contextos novedosos e imprevistos, no meros seguidores de normas predefinidas.

Un área de especial relevancia es la educación sobre las consecuencias del comportamiento digital para terceros: cómo las decisiones individuales de compartir información pueden afectar la privacidad de otros, cómo la participación en ciertos servicios contribuye a ecosistemas extractivos de datos, o cómo las interacciones online pueden causar daños psicológicos reales. La ética digital debe cultivar la conciencia de que las acciones en el espacio virtual tienen efectos tangibles en el mundo material.

A continuación revisaremos algunos modelos comparados de educación digital, en cuanto las experiencias internacionales ofrecen diversas posibilidades de integración de la alfabetización digital en los sistemas educativos:

Finlandia representa un caso paradigmático de integración transversal de la alfabetización mediática desde la educación básica. El currículo finlandés no trata la alfabetización digital como una asignatura separada sino como una competencia transversal que permea todas las áreas de conocimiento. Los docentes reciben formación específica para incorporar el análisis crítico de medios en sus disciplinas, y existe una colaboración estructurada entre escuelas, bibliotecas públicas y organizaciones

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

de verificación de hechos (Kupiainen et al., 2019).

Estonia, pionera mundial en gobierno electrónico, ha desarrollado un programa integral de ciudadanía digital que comienza en la educación primaria. El currículo incluye fundamentos de programación, seguridad informática, protección de datos personales y funcionamiento de servicios digitales públicos. La experiencia estonia demuestra que la familiaridad temprana con servicios digitales gubernamentales puede fomentar tanto competencias técnicas como confianza institucional (Kalvet, 2012).

Corea del Sur ha implementado un enfoque que combina la alfabetización digital con la educación socioemocional, reconociendo los problemas de ciberacoso, adicción digital y presión social en redes. El programa incluye formación para padres y madres, reconociendo que la alfabetización digital es un desafío intergeneracional que no puede abordarse únicamente en el espacio escolar.

En América Latina, experiencias como el Plan Ceibal en Uruguay o el programa Educ. ar en Argentina han enfatizado el acceso universal a dispositivos y conectividad como precondición de la alfabetización digital. Sin embargo, como señala Lugo (2016), la dotación de infraestructura debe complementarse con transformaciones pedagógicas profundas para evitar que la tecnología reproduzca prácticas educativas tradicionales. Las evaluaciones de estos programas revelan que el acceso material, aunque necesario, resulta insuficiente sin formación docente, contenidos adaptados y acompañamiento pedagógico.

A partir del análisis precedente, proponemos una agenda educativa articulada en torno a los siguientes ejes:

Integración curricular transversal: La alfabetización digital no debe relegarse a una asignatura específica sino integrarse en todas las áreas del conocimiento. La historia puede abordar la propaganda y la manipulación informativa; las ciencias naturales pueden examinar la comunicación científica y el negacionismo; la educación cívica puede analizar la participación política digital; las matemáticas pueden introducir nociones básicas de probabilidad y estadística necesarias para comprender el funcionamiento algorítmico.

Formación docente especializada: Los programas de formación inicial y continua del profesorado deben incorporar competencias de alfabetización digital crítica. Los docentes necesitan no solo habilidades instrumentales, sino comprensión conceptual del ecosistema digital y metodologías para desarrollar pensamiento crítico en sus estudiantes. Esto debe involucrar la crítica a la manera en la que se deben integrar en la educación las diversas tecnologías, a partir de estudios que demuestran que sus bondades son cuestionables, especialmente en la atención y formación de alteridad (Sánchez, 2025).

Educación intergeneracional: Los programas deben dirigirse también a adultos y personas mayores, frecuentemente más vulnerables a la desinformación y con menores recursos para proteger su privacidad. Las bibliotecas públicas, los centros comunitarios y las organizaciones de la sociedad civil pueden desempeñar roles cruciales en esta formación.

Colaboración público-privada responsable: Las empresas tecnológicas deben asumir responsabilidades educativas mediante el diseño de interfaces más transparentes, herramientas de alfabetización mediática integradas en sus plataformas, y financiación de investigación y programas educativos independientes —no controlados por sus intereses comerciales—.

Investigación y evaluación continua: Las políticas de alfabetización digital deben sustentarse en evidencia empírica sobre la efectividad de diferentes intervenciones y adaptarse a la evolución del ecosistema tecnológico. Se requieren métricas que trasciendan las habilidades instrumentales para evaluar competencias críticas y comportamientos informados.

Análisis comparado: casos emblemáticos y experiencias regulatorias

Las sentencias *Schrems I* (2015) y *Schrems II* (2020) del Tribunal de Justicia de la Unión Europea constituyen hitos fundamentales en la jurisprudencia sobre derechos digitales. Originadas en la demanda individual de Max Schrems contra la transferencia de sus datos de Facebook a Estados Unidos, estas sentencias invalidaron sucesivamente los marcos jurídicos que legitimaban dichas transferencias —el Safe Harbor y el Privacy Shield— por considerar que la legislación estadounidense de vigilancia no ofrecía protección equivalente al derecho europeo.

El razonamiento del TJUE es particularmente significativo: los programas de vigilancia masiva estadounidenses (revelados por Snowden en 2013) vulneraban el contenido esencial de los derechos fundamentales a la privacidad y la protección de datos reconocidos en la Carta de los Derechos Fundamentales de la UE, al no limitar las injerencias a lo estrictamente necesario ni garantizar tutela judicial efectiva a los afectados europeos.

Las implicaciones de *Schrems II* trascienden las relaciones UE-EEUU. La sentencia establece que la equivalencia en protección de datos constituye un requisito sustantivo —no meramente formal— para las transferencias internacionales, lo que afecta potencialmente a cualquier jurisdicción con programas de vigilancia extensivos. Además, impone obligaciones de verificación activa a los exportadores de datos, quienes deben evaluar caso por caso si el ordenamiento del país destinatario ofrece protección adecuada.

El sistema de crédito social chino: un contramodelo. El sistema de crédito social implementado en China representa un modelo antitético de gobernanza digital que merece análisis por su potencial expansión y por los debates que suscita sobre los límites de la datificación de la vida social.

A diferencia de la imagen frecuentemente caricaturizada en medios occidentales, el sistema de crédito social no es un mecanismo único y centralizado sino un conjunto heterogéneo de sistemas locales y sectoriales con objetivos diversos: cumplimiento de obligaciones financieras, confianza comercial, respeto a regulaciones administrativas y comportamiento cívico (Creemers, 2018). No obstante, sus rasgos comunes plantean preocupaciones legítimas desde la perspectiva de los derechos humanos.

El sistema se caracteriza por la agregación masiva de datos de fuentes múltiples (transacciones comerciales, comportamiento online, registros administrativos, denuncias ciudadanas), la aplicación de puntuaciones que determinan acceso a servicios y oportunidades, la opacidad de los criterios de evaluación y la limitación de recursos de impugnación. Sus defensores argumentan que promueve la confianza en sociedades con instituciones formales débiles; sus críticos señalan su potencial para la vigilancia totalitaria, el conformismo social y la discriminación sistémica.

Para la reflexión sobre derechos digitales, el modelo chino ilustra los riesgos de la ausencia de límites normativos a la vigilancia estatal y la datificación del comportamiento social. También evidencia que las tecnologías de análisis de datos pueden emplearse para fines radicalmente diferentes según el marco político-institucional en que se inserten.

El Marco Civil de Internet de Brasil: un referente latinoamericano. El Marco Civil de Internet brasileño (Ley 12.965/2014) representa una experiencia significativa de regulación digital participativa en el Sur Global. Elaborado mediante un proceso innovador de consulta pública que involucró a más de 2.000 contribuciones ciudadanas, el Marco Civil establece principios, garantías, derechos y deberes para el uso de Internet en Brasil.

Entre sus disposiciones más relevantes se encuentran: la consagración de la neutralidad de la red como principio (prohibiendo discriminación de tráfico por contenido, origen o destino); la protección de la privacidad y los datos personales de los usuarios; el régimen de responsabilidad de intermediarios (protección del "puerto seguro" condicionada a respuesta

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

judicial); y la garantía de libertad de expresión como fundamento del uso de Internet.

El proceso de elaboración del Marco Civil ofrece lecciones metodológicas: la consulta pública digital permitió incorporar perspectivas diversas y generar legitimidad democrática; la participación de la comunidad técnica aportó conocimiento especializado; y la articulación de la sociedad civil logró resistir presiones de grupos de interés que buscaban regímenes más restrictivos (Souza et al., 2017).

Sin embargo, la experiencia brasileña también evidencia las limitaciones de los marcos normativos aislados. La posterior Ley General de Protección de Datos (LGPD, 2018), aunque inspirada en el RGPD europeo, enfrentó demoras en su implementación y debilitamientos durante el proceso legislativo. La efectividad de cualquier marco regulatorio depende de la voluntad política, los recursos institucionales y la capacidad de enforcement.

***Estonia: laboratorio de gobernanza digital**:* Estonia se ha convertido en referente mundial de gobierno digital tras una apuesta estratégica iniciada en los años 1990. El sistema X-Road de interoperabilidad permite que diferentes bases de datos gubernamentales se comuniquen de manera segura, ofreciendo servicios digitales integrados a ciudadanos y empresas. El 99% de los servicios públicos están disponibles en línea, incluyendo el voto electrónico, la firma digital legalmente vinculante y la residencia electrónica para no residentes.

Desde la perspectiva de los derechos digitales, el modelo estonio presenta elementos destacables: el principio de "solicitud única" (el Estado no puede pedir al ciudadano información que ya posee), la trazabilidad de accesos (los ciudadanos pueden verificar qué funcionarios accedieron a sus datos y con qué propósito), y la descentralización del almacenamiento (no existe una base de datos central única, reduciendo riesgos de seguridad y abuso).

La experiencia estonia demuestra que la digitalización gubernamental y la protección de derechos no son objetivos contradictorios sino potencialmente complementarios. La transparencia sobre el uso de datos públicos puede fortalecer la confianza ciudadana y la rendición de cuentas, siempre que existan salvaguardas técnicas y jurídicas adecuadas.

No obstante, el modelo enfrenta también críticas: la dependencia de infraestructura digital crea vulnerabilidades ante ciberataques (Estonia sufrió ataques masivos en 2007); la brecha digital puede excluir a segmentos de la población; y el éxito del modelo se benefició de condiciones específicas (población pequeña y homogénea, alta conectividad, reconstrucción institucional post-soviética) difícilmente replicables en otros contextos.

La Ley de Inteligencia Artificial de la Unión Europea. La Ley de Inteligencia Artificial de la UE (AI Act), aprobada en 2024 tras un extenso proceso de negociación, constituye el primer marco regulatorio integral para sistemas de IA en una jurisdicción importante. Su enfoque basado en riesgos clasifica los sistemas de IA en cuatro categorías con requisitos diferenciados:

Riesgo inaceptable (prohibiciones): Se prohíben sistemas de manipulación subliminal, explotación de vulnerabilidades, puntuación social generalizada por autoridades públicas, e identificación biométrica remota en tiempo real en espacios públicos (con excepciones limitadas para seguridad).

***Alto riesgo (requisitos estrictos)**:* Sistemas en áreas sensibles —identificación biométrica, infraestructuras críticas, educación, empleo, crédito, servicios públicos esenciales, justicia— deben cumplir obligaciones de gestión de riesgos, calidad de datos, documentación técnica, transparencia, supervisión humana y robustez.

Riesgo limitado (obligaciones de transparencia): Sistemas como chatbots deben informar a los usuarios que interactúan con una máquina; los deepfakes deben etiquetarse como contenido generado artificialmente.

Riesgo mínimo (uso libre): La mayoría de aplicaciones de IA no enfrentan restricciones específicas.

La AI Act incorpora también requisitos para modelos de IA de propósito general (como los grandes modelos de lenguaje), incluyendo obligaciones de documentación, transparencia sobre datos de entrenamiento y evaluación de riesgos sistémicos para los modelos más potentes.

Las críticas al AI Act provienen de direcciones opuestas: organizaciones de derechos civiles consideran excesivas las excepciones para vigilancia biométrica y señalan vacíos en la protección de migrantes y solicitantes de asilo; el sector tecnológico advierte sobre cargas regulatorias que podrían frenar la innovación europea frente a competidores estadounidenses y chinos.

6. Perspectivas desde el Sur Global: colonialismo de datos y soberanía digital

El análisis de los derechos digitales no puede prescindir de su dimensión geopolítica. La economía digital contemporánea se caracteriza por una marcada asimetría Norte-Sur: las principales plataformas digitales son estadounidenses o chinas, la infraestructura de computación en la nube se concentra en países desarrollados, y los flujos de datos masivos extraen valor de poblaciones del Sur Global para alimentar modelos entrenados y monetizados en el Norte.

Couldry y Mejias (2019) conceptualizan esta dinámica como "colonialismo de datos": una nueva forma de apropiación que, análogamente al colonialismo histórico, extrae recursos —en este caso, datos sobre la vida humana— de territorios subordinados para beneficio de centros metropolitanos, normalizando esta extracción mediante discursos de progreso tecnológico y conectividad. A diferencia de materias primas tradicionales, los datos pueden extraerse sin presencia física en el territorio, a través de infraestructuras digitales que atraviesan fronteras.

Esta perspectiva crítica no rechaza la tecnología ni la conectividad como tales, sino que cuestiona las relaciones de poder que estructuran su desarrollo y distribución (Sánchez, 2025). Plantea preguntas fundamentales: ¿Quién se beneficia de la datificación de las sociedades del Sur? ¿Qué capacidades locales se desarrollan o atrofian? ¿Cómo pueden los países periféricos participar en la gobernanza de tecnologías cuyo diseño y control residen en otros lugares?

La discusión sobre derechos digitales presupone condiciones de acceso que están lejos de ser universales. La brecha digital —entendida no solo como diferencia en conectividad sino como desigualdad multidimensional en acceso, habilidades, uso significativo y resultados— constituye un obstáculo estructural para la realización de los derechos digitales en el Sur Global.

Según datos de la Unión Internacional de Telecomunicaciones (2023), aproximadamente 2.700 millones de personas permanecen sin conexión a Internet, concentradas desproporcionadamente en países de bajos ingresos, zonas rurales, y entre mujeres, personas mayores y poblaciones indígenas. Pero incluso entre los conectados, las diferencias en calidad de conexión, costo relativo, competencias digitales y relevancia de contenidos producen experiencias radicalmente desiguales.

Los derechos digitales en contextos de alta desigualdad enfrentan una tensión constitutiva: ¿tiene sentido hablar de derecho al olvido o portabilidad de datos para poblaciones cuya preocupación primaria es obtener conectividad básica? Sin desconocer esta tensión, sostenemos que el enfoque de derechos sigue siendo valioso precisamente porque permite articular demandas de acceso como cuestiones de justicia, no meramente de política tecnológica o desarrollo económico.

Diversos países del Sur Global han articulado reivindicaciones de "soberanía digital" que buscan recuperar control sobre datos, infraestructuras y gobernanza tecnológica. Estas demandas, sin embargo, son heterogéneas y potencialmente contradictorias.

En su versión autoritaria, la soberanía digital puede servir como justificación para censura,

ISSN 1692-3936 Vol 23 Número 46 Julio - Diembre de 2025

vigilancia de disidentes y fragmentación de Internet —lo que algunos denominan "splinternet"—. En su versión democrática, puede fundamentar políticas de localización de datos que protejan a ciudadanos de vigilancia extranjera, desarrollo de capacidades tecnológicas locales, y participación significativa en instituciones de gobernanza global de Internet.

Para América Latina, la construcción de soberanía digital democrática requiere: inversión en infraestructura de conectividad y computación regional; desarrollo de talento local en tecnologías críticas; marcos regulatorios que protejan datos personales y establezcan condiciones para la competencia; participación activa en foros internacionales de gobernanza de Internet; y promoción de modelos tecnológicos alternativos basados en software libre, datos abiertos y procomún digital.

CONCLUSIONES

La protección de los derechos digitales constituye uno de los desafíos definitorios de nuestro tiempo. Como hemos argumentado a lo largo de este trabajo, este desafío no puede abordarse desde respuestas unidimensionales —ya sean puramente tecnológicas, exclusivamente jurídicas o meramente educativas— sino que requiere una articulación integral de múltiples estrategias.

Los derechos digitales deben entenderse como una extensión y actualización de los derechos humanos tradicionales, no como una categoría separada o subordinada. La privacidad, la libertad de expresión, la no discriminación y el debido proceso adquieren dimensiones específicas en el entorno digital que exigen reconocimiento normativo y garantías adaptadas, pero su fundamento permanece anclado en la dignidad humana como valor universal.

Los marcos regulatorios, aunque necesarios, resultan insuficientes por sí solos. La velocidad del cambio tecnológico, las asimetrías informativas entre reguladores y regulados, los riesgos de captura corporativa y las limitaciones de aplicación transfronteriza debilitan la eficacia de las respuestas puramente normativas. La regulación debe complementarse con mecanismos de supervisión independiente dotados de recursos y expertise, acceso efectivo a la justicia para los afectados, y participación significativa de la sociedad civil en los procesos de gobernanza.

La educación digital crítica constituye una condición de posibilidad para el ejercicio efectivo de los derechos digitales. Sin las competencias necesarias para comprender el ecosistema digital, identificar manipulaciones, proteger la privacidad y participar informadamente, los ciudadanos no pueden ejercer control significativo sobre su vida digital ni exigir rendición de cuentas a quienes detentan poder tecnológico. La alfabetización digital debe integrarse transversalmente en los sistemas educativos, extenderse a todas las generaciones y desarrollar dimensiones críticas y éticas que trasciendan las habilidades meramente instrumentales.

La perspectiva del Sur Global resulta indispensable para una comprensión completa de los derechos digitales. Las asimetrías de la economía digital internacional, la persistencia de la brecha digital y las dinámicas de extracción de datos configuran condiciones estructurales que cualquier marco de derechos debe considerar. La soberanía digital democrática —no autoritaria— representa una reivindicación legítima que debe articularse con los principios universales de derechos humanos.

La gobernanza digital debe concebirse como un proyecto ético, político y educativo de alcance global que requiere cooperación multinivel entre Estados, organismos internacionales, sector privado, academia y sociedad civil. Su legitimidad se fundamenta en la capacidad de proteger derechos, reducir desigualdades y fomentar una ciudadanía digital crítica y responsable.

En síntesis, la defensa de los derechos digitales no es únicamente una cuestión técnica o jurídica: es, ante todo, una apuesta por el fortalecimiento de la democracia, la dignidad humana y la justicia en la era de la inteligencia artificial y la interconexión global. Los desafíos son formidables, pero también

lo son las oportunidades que las tecnologías digitales ofrecen para la participación, la transparencia y el empoderamiento ciudadano. El rumbo que tomemos dependerá de las decisiones colectivas que adoptemos en los próximos años.

REFERENCIAS

» Barocas, S., Hardt, M., & Narayanan, A. (2023). *Fairness and Machine Learning: Limitations and Opportunities*. MIT Press.

» Barrio A. (2021). Génesis y desarrollo de los derechos digitales. *Revista de las Cortes Generales*, (110), 197-233.

» Barrio, A. (2021). *Derechos digitales y sociedad de la información: nuevos retos para el constitucionalismo contemporáneo*. Tirant lo Blanch.

» Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*, 149-159.

» Bonilla-Morejón, D. M. (2023). Derecho penal y políticas de seguridad en Ecuador: Análisis de la eficacia. *Revista Científica Zambos, 2*(3), 59–74. https://doi.org/10.69484/rcz/v2/n3/50

» Buckingham, D. (2019). *The Media Education Manifesto.* Polity Press.

» Cavoukian, A. (2012). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.

» Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

» Cova-Fernández, L. (2019). Los derechos digitales: fundamentos, alcance y desafíos en la sociedad de la información. *Revista Venezolana de Legislación y Jurisprudencia*, (12), 255-298.

» Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3175792

» De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34(2), 193-203.

» Derechos Digitales. (2021). Derechos Digitales expresa su preocupación ante la CIDH por aumento del uso de reconocimiento facial en la región. *Derechos Digitales*.

» Díaz Charquero, P., Vásquez, H. A., & Gemetto, J. (2021). *Flexibilidades al derecho de autor en América Latina*. Fundación Karisma.

» Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608.*

» European Commission. (2024). Regulation (EU) 2024/1689 *laying down harmonised rules on artificial intelligence (AI Act)*. Official Journal of the European Union.

» European Data Protection Board. (2021). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.*

» Fernández, E., & Díaz Lafuente, J. (2022). Los derechos digitales: ¿hacia una nueva generación de derechos humanos? Aproximaciones teóricas desde América Latina y Europa. *Revista de Estudios Socio-Jurídicos*, 61, 1–20. https://doi.org/10.17808/des.61.1942

» Floridi, L. (2020). *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities.* Oxford University Press.

» Floridi, L., & Cowls, J. (2021). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 1(1).

» Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine, 38*(3), 50-57.

» Green, B., & Chen, Y. (2019). The principles and limits of algorithm-in-the-loop decision making. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1-24.

» Han, B.-C. (2012). *La sociedad del cansancio* (A. Saratxaga Arregi, Trad.). Herder. (Obra original publicada en 2010).

» Hobbs, R. (2020). *Media Literacy in Action: Questioning the Media*. Rowman & Littlefield.

» Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government, an International Journal, 9*(2), 142-157.

» Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, 34(1), 189-218.

» Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14-29.

» Kleinberg, J., Mullainathan, S., & Raghavan, M. (2017). Inherent trade-offs in the fair determination of risk scores. *Proceedings of the 8th Innovations in Theoretical Computer Science Conference*.

» Knight, M. I. D. (2011). El daño: ¿común denominador de la responsabilidad contractual y la extracontractual? *Contribuciones a las Ciencias Sociales* (2011-08).

» Knight, M. I. D. (2012). Algunas reflexiones en torno a la legalidad, cultura jurídica y comportamiento ciudadano. *Contribuciones a las Ciencias Sociales* (2012-05).

» Knight Soto, I. (2015). La protección al derecho a la vida e integridad física del niño, niña y adolescente. *Letras Jurídicas*, (31), 95-108.

» Knight Soto, I. (2015a). Derecho y ética en la era digital: protección de la dignidad humana. *Revista Latinoamericana de Derecho y Tecnología, 3*(1), 87–102.

» Knight Soto, I. & Delgado Knight, M. (2020). El conciliador como tercero en la relación contractual: La innovación social en la práctica restaurativa de solución de conflictos. *Derechos en Acción, 14*(14), 360–360.

» Knight Soto, I., & Delgado Knight, M. (2023). El derecho de petición: una mirada a su dimensión defensiva y de participación ciudadana. *Estudios Constitucionales, 21*(1), 200–218.

» Knight Soto, I., Chacón, M. L. Q., Roque, D. M. D., & Zapata, P. R. (2024). Uniendo fronteras: cooperación internacional en la era global. *Derecho y Realidad, 22*(43), 2-31.

» Knight Soto, I., & Delgado Knight, M. I. (2023). El derecho de petición: una mirada a su dimensión defensiva y de participación ciudadana. Estudios Constitucionales, 21(1), 200–218.

» Knight Soto, I., & Delgado Knight, M. I. (2025). La inteligencia artificial en el lugar de trabajo: derechos laborales en la era de la automatización. *Revista Derecho y Realidad, 3*(3), 71–84.

» Kupiainen, R., Sintonen, S., & Suoranta, J. (2019). Educating for critical media literacy in Finland. En *The International Encyclopedia of Media Literacy* (pp. 1-13). Wiley.

» Lugo, M. T. (2016). Entornos digitales y políticas educativas: dilemas y certezas. UNESCO-IIEP.

» Mantelero, A. (2022). *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. Springer.

» Marchetti, R. (2022). *Digital Governance: New Technologies and New Challenges*. Routledge.

» Marwick, A. E. (2018). Why do people share fake news? A sociotechnical model of media effects. *Georgetown Law Technology Review, 2*(2), 474-512.

» Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.

» Mendoza-Armijos, H. E. (2023). Análisis de la protección jurídica de los derechos digitales. *Multidisciplinary Collaborative Journal*, 1(4), 13–26. https://doi.org/10.70881/mcj/v1/n4/23

» Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

» Nitsche, L., & Hairsine, K. (2016). What are digital rights? *DW Akademie.*

» OECD. (2022). *OECD Framework for the Classification of AI Systems*. OECD Publishing.

» Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.

» Renda, A. (2023). *Regulating AI: From Principles to Practice*. Centre for European Policy Studies.

» Sánchez Riaño, F. (2025). *Sembrar mi corazón en el corazón del otro: Pedagogías sentipensantes en la educación superior* [Tesis doctoral, Universidad Nacional de La Plata]. Repositorio institucional de la Universidad Nacional de La Plata. http://sedici.unlp.edu.ar/handle/10915/187025

» Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.

» Solove, D. J. (2021). *Understanding Privacy* (2nd ed.). Harvard University Press.

» Souza, C. A., Steibel, F., & Lemos, R. (2017). Notes on the creation and impacts of Brazil's Internet Bill of Rights. *The Theory and Practice of Legislation, 5*(1), 73-94.

» Torres Manrique, J. I. (2017). Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución. *Revista Misión Jurídica, 10*(13), 209–223. https://doi.org/10.25058/1794600X.16

» UNESCO. (2023). *Recommendation on the Ethics of Artificial Intelligence*. París: UNESCO.

» Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151.

» Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

» Westin, A. F. (1967). *Privacy and Freedom.* Atheneum.

» Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record*, 121(11), 1-40.

» Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.