

LA EROSIÓN DE LA SOBERANÍA DIGITAL: EL CONFLICTO ENTRE EL DERECHO INTERNACIONAL Y LA HEGEMONÍA ALGORÍTMICA

THE EROSION OF DIGITAL SOVEREIGNTY: THE CONFLICT BETWEEN INTERNATIONAL LAW AND ALGORITHMIC HEGEMONY

Quevedo Méndez, Orlando José*
Universidad de Los Andes
Venezuela

Resumen

El presente trabajo analiza la progresiva erosión de la soberanía digital de los Estados-nación frente a la hegemonía algorítmica ejercida por corporaciones tecnológicas transnacionales. A partir de un marco teórico interdisciplinario que articula la teoría clásica de la soberanía (Weber, 1921; Krasner, 1999), los estudios de internet y gobernanza digital (Mueller, 2010; DeNardis, 2014) y la teoría crítica del poder algorítmico (Zuboff, 2019; Pasquale, 2015), se argumenta que la arquitectura técnica de las plataformas digitales genera una nueva forma de dominación que trasciende las fronteras jurisdiccionales y desafía los principios fundamentales del derecho internacional público. El análisis se organiza en tres ejes: primero, se examina el concepto de soberanía digital y sus dimensiones; segundo, se describe el fenómeno de la hegemonía algorítmica y sus mecanismos de poder; tercero, se confrontan ambos campos a partir de casos jurisprudenciales y normativos representativos. Se concluye que el derecho internacional contemporáneo carece todavía de los instrumentos coercitivos y de los marcos conceptuales necesarios para regular eficazmente el poder de las arquitecturas algorítmicas, y se proponen líneas de investigación futura orientadas a la construcción de un ordenamiento jurídico digital robusto. La metodología empleada combina el análisis documental, la revisión de literatura especializada y el estudio de casos.

Palabras clave: Soberanía digital · Hegemonía algorítmica · Derecho internacional · Gobernanza de internet · Poder tecnológico.

Abstract

This paper analyzes the progressive erosion of the digital sovereignty of nation-states in the face of the algorithmic hegemony exercised by transnational technology corporations. Drawing on an interdisciplinary theoretical framework that links classical theories of sovereignty (Weber, 1921; Krasner, 1999), internet studies and digital governance (Mueller, 2010; DeNardis, 2014), and the critical theory of algorithmic power (Zuboff, 2019; Pasquale, 2015), it argues that the technical architecture of digital platforms generates a new form of domination that transcends jurisdictional boundaries and challenges the fundamental principles of public international law. The analysis is structured around three key axes: first, it examines the concept of digital sovereignty and its dimensions; second, it describes the phenomenon of algorithmic hegemony and its mechanisms of power; third, it confronts both fields through representative case law and regulatory frameworks. The paper concludes that contemporary international law still lacks the coercive instruments and conceptual frameworks required to effectively regulate the power of algorithmic architectures, and suggests future lines of research aimed at building a robust digital legal order. The methodology employed combines documentary analysis, a review of specialized literature, and case studies.

Keywords: Digital sovereignty · Algorithmic hegemony · International law · Internet governance · Technological power.

*Profesor de la Universidad de Los Andes - Venezuela. ORCID: <https://orcid.org/0009-0001-6963-8630>. Correo: orlandoq@ula.ve

Recibido: 10/01/2026 / **Aceptado:** 26/03/2026

La soberanía, entendida como el monopolio legítimo del uso de la fuerza dentro de un territorio determinado (Weber, 1921), ha sido históricamente uno de los pilares constitutivos del Estado moderno. Sin embargo, la revolución digital de las últimas tres décadas ha introducido un conjunto de dinámicas que desafían de manera sin precedentes la capacidad de los Estados para ejercer efectivamente sus funciones soberanas en el ámbito virtual. Las corporaciones que controlan las infraestructuras, los protocolos y los datos del ecosistema digital global han acumulado un poder que, en muchos aspectos, rivaliza con el de los propios Estados.

Este fenómeno adquiere especial relevancia cuando se observa que las decisiones algorítmicas —los procesos automatizados de clasificación, selección y recomendación que estas corporaciones implementan— afectan directamente la vida de miles de millones de personas, incluyendo la configuración de la opinión pública, el acceso a la información, las dinámicas del comercio internacional y, en última instancia, el ejercicio de derechos fundamentales como la libertad de expresión, la privacidad y la no discriminación.

Para comprender la profundidad de esta erosión, es imperativo analizar el sustrato cultural y sociológico en el que se despliega la hegemonía algorítmica. No nos enfrentamos únicamente a una reconfiguración técnica o a una disputa de jurisdicciones estatales, sino a una mutación fundamental en la estructura misma de la sociedad contemporánea. Como señala Byung-Chul Han, hemos transitado de la sociedad disciplinaria a una sociedad de la información dominada por la infocracia. En este nuevo régimen, el poder ya no opera principalmente mediante la coacción física o el silenciamiento, sino a través de la saturación informativa, la libre autoexposición del individuo y la canalización invisible de los flujos de datos.

Esta realidad cultural transforma las prácticas democráticas y la esfera pública en un ecosistema gobernado por un régimen

psicopolítico digital, donde los algoritmos operan de manera subrepticia sobre el plano afectivo y cognitivo de la población. Es precisamente en el corazón de esta sociedad con estas características donde se detona la necesidad de este tipo de investigaciones. En consecuencia, el estudio del derecho en el entorno virtual adquiere una urgencia crítica: el verdadero desafío para el Estado de derecho no radica solo en defender fronteras analógicas, sino en descifrar cómo la arquitectura invisible de las plataformas altera la autonomía comunicativa y debilita los cimientos de la deliberación ciudadana.

Así, la tensión entre la soberanía digital de los Estados y la hegemonía algorítmica de las grandes corporaciones tecnológicas no es meramente un conflicto técnico o económico: es, fundamentalmente, un conflicto jurídico-político de primera magnitud que el derecho internacional no ha logrado todavía procesar con la profundidad y la urgencia que su complejidad exige. Como señalan Slaughter y Burke-White (2006), el derecho internacional clásico fue diseñado para regular las relaciones entre Estados soberanos en un mundo analógico; su capacidad para adaptarse a un entorno en el que actores no estatales dominan infraestructuras críticas globales sigue siendo una cuestión profundamente debatida.

La investigación se estructura en cinco secciones además de esta introducción. En la segunda sección se desarrolla el marco teórico, articulando los conceptos de soberanía digital y hegemonía algorítmica. La tercera sección examina el derecho internacional aplicable y sus limitaciones. La cuarta sección presenta un análisis de casos concretos que ilustran las tensiones descritas. La quinta sección ofrece una discusión y propuestas de futuro. Finalmente, se presentan las conclusiones.

Marco teórico

La soberanía digital: concepto, dimensiones y debates

El concepto de soberanía digital representa una extensión del principio clásico

de soberanía hacia el dominio del ciberespacio y las tecnologías de la información y la comunicación (TIC). La soberanía digital puede definirse como la capacidad de un Estado para ejercer su autoridad efectiva sobre las infraestructuras digitales, los datos y las actividades que tienen lugar en el entorno virtual bajo su jurisdicción. Esta definición, aunque operativa, ha sido objeto de debate en la literatura especializada.

Mueller (2010), en su influyente obra *Will the Internet Fragment? Sovereignty, Thick and Thin*, distingue entre una soberanía «gruesa» (*thick sovereignty*) y una soberanía «fina» (*thin sovereignty*) en el contexto digital. La primera se refiere al control efectivo y completo sobre las infraestructuras críticas; la segunda, a la capacidad de participar en la gobernanza global del ecosistema digital y de regular el comportamiento de los actores que operan en su jurisdicción. Mueller argumenta que la internet, por su arquitectura descentralizada, tiende naturalmente hacia la erosión soberana, y que los intentos de los Estados por recuperar control total son, en gran medida, ilusorios.

En cambio, DeNardis (2014), en *The Global War for Internet Governance*, ofrece una perspectiva más matizada al señalar que la gobernanza de internet no es un dominio libre de poder estatal, sino un campo de disputa donde los Estados compiten activamente por definir las normas técnicas y jurídicas que rigen el espacio digital. Según DeNardis, la *governance gap* —la brecha entre la velocidad del cambio tecnológico y la lentitud de la elaboración normativa internacional— constituye uno de los desafíos más graves para el ordenamiento jurídico internacional contemporáneo.

Krasner (1999), en su trabajo seminal sobre la soberanía, identifica cuatro dimensiones del concepto: la soberanía doméstica (autoridad sobre el territorio), la soberanía interdependiente (control sobre los flujos transfronterizos), la soberanía internacional (reconocimiento jurídico

externo) y la soberanía westfaliana (ausencia de autoridad externa superior). Cada una de estas dimensiones se ve afectada de manera distintiva por el fenómeno digital: la doméstica, por la dificultad de regular plataformas globales desde marcos nacionales; la interdependiente, por la concentración de infraestructuras críticas en manos de pocos actores; la internacional, por la ausencia de tratados vinculantes en materia digital; y la westfaliana, por la presión de normas y estándares técnicos supranacionales.

En el ámbito latinoamericano, diversos estudios han señalado que los países del Sur Global enfrentan un déficit particularmente agudo de soberanía digital, dado que la infraestructura, los servicios y los estándares técnicos están diseñados predominantemente desde una lógica del Norte Global, lo que reproduce asimetrías de poder preexistentes en el orden internacional (Milan & Treré, 2019; Gurumurthy, 2020; Villanueva-Mansilla, 2018).

Hegemonía algorítmica: arquitectura, poder y dominación

El concepto de hegemonía algorítmica se refiere al conjunto de prácticas, estructuras y dinámicas de poder que emanan de los sistemas algorítmicos utilizados por las grandes corporaciones tecnológicas para dirigir, orientar y condicionar el comportamiento de individuos, organizaciones y Estados. Este concepto articula elementos de la teoría del poder de Foucault (1975, 1976), la economía política de la información (Schiller, 1984) y los estudios críticos sobre automatización (Braverman, 1998; Noble, 1978).

Zuboff (2019), en *The Age of Surveillance Capitalism*, ofrece el análisis más comprensivo hasta la fecha sobre este fenómeno. La autora distingue entre el «capitalismo de vigilancia» —un nuevo paradigma económico fundado en la extracción sistemática de datos conductuales de los usuarios— y las formas clásicas de capitalismo industrial. Según Zuboff, las empresas tecnológicas han logrado

lo que ninguna institución política había conseguido previamente: un control discreto y omnipresente sobre el comportamiento humano a escala global, operando fuera de todo marco de rendición de cuentas democrática. La autora acuña el concepto de «instrumentarismo» para describir esta nueva lógica de dominación, que supera tanto al marxismo clásico como al liberalismo en su capacidad de instrumentalizar la experiencia humana.

Por su parte, Pasquale (2015), en *The Black Box Society*, argumenta que las redes sociales, los motores de búsqueda y las plataformas de comercio electrónico funcionan como «cajas negras» (*black boxes*) que toman decisiones con profundas consecuencias para la vida de las personas —desde la concesión de crédito hasta la determinación de qué contenidos informativos llegan a los ciudadanos— sin que exista transparencia sobre los criterios utilizados ni mecanismos efectivos de responsabilidad jurídica. Esta opacidad algorítmica constituye, según el autor, una de las mayores amenazas para la democracia liberal contemporánea.

Van Dijck, De Waal y Poell (2018), en *The Platform Society*, analizan cómo las plataformas digitales se han convertido en infraestructuras institucionales que median cada vez más aspectos de la vida social, económica y política. Los autores identifican tres dimensiones del poder algorítmico: el poder de datos (la capacidad de recopilar, analizar y monetizar información personal), el poder de selección (la capacidad de determinar qué contenidos, productos o servicios se muestran a cada usuario) y el poder de arquitectura (la capacidad de diseñar los entornos digitales que estructuran la interacción social). Cada una de estas dimensiones erosiona, de manera específica, las prerrogativas soberanas de los Estados.

En el ámbito de la comunicación política, los trabajos de Pariser (2011) sobre las «burbujas de filtro» (*filter bubbles*) y de Benkler, Faris y Roberts (2018) sobre la «red de la ira» (*network of outrage*) han

demostrado cómo los algoritmos de las redes sociales pueden fragmentar el espacio público informativo, amplificar discursos polarizadores y, en última instancia, desestabilizar procesos electorales y la cohesión social. Estos efectos tienen implicaciones directas para la soberanía informativa de los Estados y para la capacidad de los ciudadanos de ejercer sus derechos políticos en condiciones de igualdad.

Derecho internacional y gobernanza digital: marcos normativos y limitaciones. Los derechos humanos digitales y su protección internacional

El marco normativo internacional en materia de derechos humanos digitales tiene su fundamento en la Declaración Universal de los Derechos Humanos (1948), el Pacto Internacional de Derechos Civiles y Políticos (1966) y, de manera más específica, en los Principios de UNCTAD sobre privacidad en el contexto del comercio electrónico (1996) y las Directrices de la OCDE sobre privacidad (1980, actualizadas en 2013). La Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información (Ginebra, 2003 / Túnez, 2005) reconoció explícitamente que «la libertad de comunicación y el derecho a la información constituyen un componente fundamental de la democracia» y que «la seguridad en el uso de las TIC debe garantizarse para reforzar la confianza de los usuarios» (ITU, 2005).

El Relator Especial de las Naciones Unidas para la libertad de expresión, en sus informes temáticos de 2011, 2014 y 2018, ha abordado específicamente las dimensiones digitales de la libertad de expresión, señalando que los Estados tienen la obligación positiva de garantizar que los actores privados —incluidas las corporaciones tecnológicas— respeten este derecho fundamental. El informe de 2018, presentado por David Kaye, es particularmente relevante por su análisis de la moderación de contenidos por parte de las plataformas y la necesidad de estándares de diligencia debida (*due diligence*) que las obliguen a responder ante abusos sistémicos.

Sin embargo, como señalan Roth y Nolan (2019), la implementación efectiva de estos marcos normativos enfrenta obstáculos fundamentales: la ausencia de un tratado internacional vinculante específico sobre derechos digitales, la jurisdicción extraterritorial limitada del derecho internacional de los derechos humanos, y la asimetría de poder entre los Estados —especialmente los del Sur Global— y las corporaciones tecnológicas estadounidenses. Además, el sistema de relatores especiales y órganos de tratados carece de mecanismos coercitivos, lo que reduce su capacidad de incidencia a la persuasión y la legitimación moral.

La protección de datos personales: un patchwork normativo global

En materia de protección de datos personales, el panorama normativo internacional se caracteriza por su fragmentación. La Unión Europea, con el Reglamento General de Protección de Datos (GDPR, 2016/2018), ha establecido el estándar más riguroso y comprensivo del mundo, basado en principios como la minimización de datos, la finalidad, la limitación del almacenamiento y los derechos de acceso, rectificación y supresión. El GDPR ha ejercido un efecto de «jurisdiccionalización» (*Brussels Effect*) significativo: numerosas jurisdicciones de todo el mundo han adoptado legislaciones inspiradas en sus principios (Bradford, 2020).

No obstante, la aplicación extraterritorial del GDPR enfrenta límites estructurales. En primer lugar, las grandes corporaciones tecnológicas estadounidenses han desarrollado estrategias de adaptación que, en la práctica, permiten una *compliance* selectiva. En segundo lugar, la ausencia de mecanismos de cooperación internacional efectivos de aplicación de la normativa de protección de datos dificulta la persecución efectiva de infracciones cometidas desde jurisdicciones con marcos regulatorios laxos. En tercer lugar, la concentración de la infraestructura tecnológica en un puñado de empresas

dominantes crea dependencias estructurales que los reguladores no han logrado resolver.

Fuera de la UE, la situación es igualmente fragmentada: la Ley de Privacidad del Consumidor de California (CCPA, 2018) representa un avance significativo en el derecho estadounidense, pero su alcance es limitado. En América Latina, Brasil (Lei Geral de Proteção de Dados, LGPD, 2018), Argentina (Ley de Protección de Datos Personales, 2000) y México (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010) han desarrollado marcos normativos propios, aunque su capacidad de aplicación (*enforcement*) frente a las *Big Tech* es desigual. En Asia, la Ley de Protección de la Información Personal (PIPL) de China (2021) representa un intento de afirmar la soberanía digital mediante controles estrictos sobre el flujo transfronterizo de datos, pero su tensión con los intereses de las corporaciones tecnológicas globales es un frente abierto de conflicto.

El derecho de la competencia y el poder de mercado algorítmico

El derecho de la competencia internacional ofrece otro frente de regulación. La concentración de mercado en el sector tecnológico —con empresas como Alphabet (Google), Meta (Facebook), Amazon, Apple y Microsoft que dominan simultáneamente múltiples segmentos del ecosistema digital— plantea cuestiones fundamentales sobre la aplicación de las normas *antitrust* a nivel transfronterizo. Crémer, De Montjoye y Schweitzer (2019), en un influyente informe para la Comisión Europea, identificaron tres categorías de prácticas problemáticas: las estrategias de vinculación (*tying*) que aprovechan la posición dominante en un mercado para avanzar en otros (el caso Google Shopping es paradigmático), la recopilación masiva de datos como barrera de entrada (*data as barrier to entry*), y los efectos de red que generan tendencias naturales al monopolio u oligopolio.

Las autoridades de competencia de múltiples jurisdicciones han iniciado investigaciones y procesos sancionadores contra las grandes tecnológicas: la Comisión Europea ha impuesto multas récord a Google y Meta; el Departamento de Justicia de Estados Unidos ha demandado a Google por prácticas monopolísticas en el mercado de búsqueda (2020) y a Apple por prácticas exclusivistas (2024); la Competition Commission of India ha sancionado a Google por abuso de posición dominante en el mercado de aplicaciones móviles. Sin embargo, como señala Stucke (2021), la efectividad de estas intervenciones se ve limitada por la rapidez con la que evoluciona el mercado tecnológico y por la dificultad de aplicar remedios tradicionales —como la desagregación (*divestiture*)— a empresas cuya propuesta de valor se basa precisamente en la integración vertical de múltiples servicios.

Análisis de casos: tensiones entre soberanía estatal y poder algorítmico. La eliminación de contenidos y la libertad de expresión: el caso X en Brasil

Uno de los episodios más emblemáticos de la tensión entre soberanía digital y poder algorítmico tuvo lugar en Brasil en agosto de 2024, cuando la plataforma X (anteriormente Twitter), propiedad de Elon Musk, decidió cerrar sus operaciones en el país en respuesta a las órdenes judiciales del Tribunal Supremo Federal de Brasil que exigían la eliminación de cuentas vinculadas a actividades ilegales y a la desinformación política. El ministro Alexandre de Moraes había ordenado a X que bloqueara determinadas cuentas conforme a la legislación brasileña, bajo amenaza de multas diarias. La reacción de Musk —cerrar la plataforma y desafiar la autoridad judicial— representó una muestra sin precedentes de cómo un actor corporativo privado puede ejercer presión sobre un Estado soberano amenazando con retirar un servicio del que dependen millones de ciudadanos.

Este caso ilustra varias dinámicas simultáneamente: en primer lugar, la capacidad

de las plataformas para convertirse en infraestructuras críticas cuya ausencia genera costos sociales masivos. En segundo lugar, la dificultad de los marcos jurídicos nacionales para imponer obligaciones a empresas cuya sede está en jurisdicciones remotas y cuyas decisiones operativas responden a intereses privados no sujetos a control democrático. En tercer lugar, la asimetría de recursos entre un individuo ultramillonario y un sistema judicial nacional, incluso cuando este último cuenta con mecanismos de aplicación.

Desde la perspectiva del derecho internacional, el caso reabre el debate sobre si las empresas tecnológicas de dimensión global pueden ser consideradas «actores con responsabilidades en materia de derechos humanos» conforme a los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos (2011). También plantea la cuestión de si los Estados tienen la obligación de garantizar alternativas públicas a las infraestructuras digitales privadas, como forma de preservación de la soberanía digital.

La cuestión de los centros de datos y la soberanía sobre las infraestructuras críticas

El almacenamiento y procesamiento de datos en la nube plantea cuestiones fundamentales de soberanía digital. La concentración geográfica de los centros de datos (*data centers*) en determinadas jurisdicciones —Estados Unidos, China y, en menor medida, la Unión Europea— significa que una proporción significativa de los datos generados por ciudadanos, empresas y gobiernos de todo el mundo está sujeta a las leyes de jurisdicciones extranjeras. El caso más significativo es el de la Ley CLOUD (*Clarifying Lawful Overseas Use of Data Act*) de Estados Unidos (2018), que faculta a las autoridades estadounidenses para exigir a las empresas estadounidenses la entrega de datos almacenados en cualquier parte del mundo, independientemente de las leyes de protección de datos de los países donde se encuentren físicamente.

El Tribunal de Justicia de la Unión Europea, en los asuntos *Schrems I* (C362/14, 2015) y *Schrems II* (C311/18, 2020), declaró inválido el acuerdo Privacy Shield —el mecanismo que regulaba la transferencia de datos personales de la UE a Estados Unidos— precisamente porque la legislación estadounidense no garantizaba un nivel de protección equivalente al europeo. El *Schrems II* estableció que la transferencia de datos a países terceros solo es lícita cuando el país de destino ofrece garantías adecuadas, y que las empresas deben evaluar, caso por caso, los riesgos de cada transferencia. Sin embargo, como señalan Svantesson y Polčák (2021), la realidad de la infraestructura tecnológica global —con servicios como AWS, Azure y Google Cloud que son técnicamente inseparables— hace que esta evaluación sea, en la práctica, casi imposible de llevar a cabo de manera rigurosa.

Esta situación ha impulsado políticas de «soberanía digital» en múltiples jurisdicciones. La estrategia de la nube europea (*Gaia-X*), lanzada en 2020, busca desarrollar una infraestructura de nube federada que garantice la residencia de los datos dentro de la UE. India, con su **Digital Personal Data Protection Act, 2023** (que sucedió al proyecto de ley de 2020), ha establecido requisitos de localización que obligan a las empresas a almacenar ciertos tipos de datos sensibles en servidores dentro del territorio nacional, aunque con excepciones para flujos de datos transfronterizos hacia jurisdicciones consideradas adecuadas. Rusia, con sus leyes de «internet soberana» (2019) y «almacenamiento localizado» de datos (2015), ha llevado esta lógica al extremo, generando preocupación por su compatibilidad con los estándares internacionales de libertad de expresión y acceso a la información.

Las interferencias algorítmicas en procesos electorales y la integridad democrática

La evidencia acumulada sobre el papel de los algoritmos en la amplificación de desinformación electoral constituye uno de

los casos más preocupantes de erosión de la soberanía informativa. El escándalo de Cambridge Analytica (2018), en el que se utilizaron datos de 87 millones de usuarios de Facebook para construir perfiles psicográficos y dirigir mensajes políticos personalizados durante las elecciones presidenciales de Estados Unidos en 2016 y el referéndum del Brexit, reveló hasta qué punto las plataformas digitales pueden ser instrumentalizadas para influir en procesos democráticos soberanos desde el exterior.

Bradshaw y Howard (2019), en su investigación sobre las redes de *trolls* y la desinformación a nivel global, documentaron operaciones organizadas de influencia digital en 70 países, muchas de las cuales aprovecharon las características algorítmicas de las plataformas —como los sesgos de viralización y los bucles de retroalimentación emocional— para maximizar su alcance. La responsabilidad de estos procesos es difusa: ¿recurrir al Estado cuyo proceso electoral fue interferido? ¿A la plataforma que diseñó los algoritmos de recomendación? ¿A la agencia de inteligencia del país de origen? ¿Al individuo que contrató los servicios?

El derecho internacional no ofrece, hasta la fecha, una respuesta satisfactoria a estas cuestiones. La Convención de Budapest sobre Ciberdelincuencia (2001, enmendada en 2021) aborda algunos aspectos de la criminalidad informática transfronteriza, pero no cubre específicamente la manipulación electoral mediante algoritmos. La Convención de las Naciones Unidas sobre la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (2024) tampoco ha resuelto esta laguna. En consecuencia, los Estados afectados se ven obligados a responder con herramientas legales improvisadas —desde leyes de desinformación de alcance nacional hasta regulaciones *ad hoc* sobre inteligencia artificial— cuya efectividad y compatibilidad con el derecho internacional son, en el mejor de los casos, cuestionables.

Discusión y propuestas

El análisis precedente permite identificar al menos cinco dimensiones fundamentales de la tensión entre soberanía digital y hegemonía algorítmica que requieren atención tanto de la comunidad académica como de los responsables políticos.

En primer lugar, la cuestión de la rendición de cuentas algorítmica (*algorithmic accountability*). Los marcos normativos actuales presuponen la existencia de un sujeto responsable —persona física o jurídica— cuyas decisiones pueden ser identificadas, evaluadas y, en su caso, sancionadas. Sin embargo, la opacidad de los sistemas de inteligencia artificial, particularmente los basados en aprendizaje automático (*machine learning*), dificulta radicalmente esta atribución. Como señala Diakopoulos (2016), la *accountability gap* algorítmica —la distancia entre la capacidad de predecir consecuencias y la capacidad de explicar las causas— constituye un desafío sin parangón para el derecho administrativo y penal tradicionales. La propuesta de «auditorías algorítmicas» (*algorithmic impact assessments*), análogas a las evaluaciones de impacto ambiental, comienza a ganar tracción en la Unión Europea (AI Act, 2024) y en el Reino Unido (Plan for Digital Regulation, 2024), pero su implementación práctica sigue siendo incipiente.

En segundo lugar, la reforma de la gobernanza de internet. Los modelos actuales de gobernanza —dominados por el DNS y la asignación de direcciones IP a través de ICANN (*Internet Corporation for Assigned Names and Numbers*), cuya relación con el Departamento de Comercio de Estados Unidos solo se rompió formalmente en 2016, y por estándares técnicos definidos por organismos como el IETF (*Internet Engineering Task Force*) y el W3C (*World Wide Web Consortium*)— reflejan una arquitectura de múltiples partes interesadas (*multistakeholder governance*) que, aunque preferible al control estatal exclusivo, ha demostrado ser ineficaz

para abordar las asimetrías de poder entre los actores involucrados. Kurbaliya (2019) aboga por un modelo de gobernanza que reconozca la naturaleza infraestructural de la red y la someta a los mismos principios de rendición de cuentas democrática que se aplican a otros servicios públicos.

En tercer lugar, la necesidad de un tratado internacional vinculante sobre inteligencia artificial y derechos humanos. La propuesta de la Secretaría General de las Naciones Unidas, a través del Asesor Especial sobre Inteligencia Artificial (2023), de establecer un organismo internacional de supervisión de la IA representa un avance significativo, pero enfrenta la resistencia de las grandes potencias tecnológicas —Estados Unidos y China— que controlan la mayor parte de la infraestructura y los modelos de IA. La experiencia del Organismo Internacional de Energía Atómica (OIEA) sugiere que un organismo técnico de este tipo es viable, pero su poder dependería crucialmente de la voluntad política de los Estados miembros.

En cuarto lugar, la cuestión del poder de los trabajadores del sector tecnológico. Scholz (2016) y Rosenblat (2018) han señalado que, detrás de la narrativa de la «economía de las plataformas» libre de jerarquías, existe una fuerza laboral oculta (*ghost work*) compuesta por millones de anotadores, moderadores de contenido y entrenadores de IA en el Sur Global, cuyas condiciones laborales representan una forma contemporánea de dependencia económica y colonialismo digital. Este aspecto es frecuentemente ignorado en los debates sobre soberanía digital, pero es fundamental para una comprensión integral de las relaciones de poder en el ecosistema tecnológico.

En quinto lugar, la importancia de la alfabetización algorítmica como herramienta de emancipación ciudadana. Como han señalado Dörr (2017) y Milan y Treré (2019), la capacidad de los ciudadanos para comprender, cuestionar y negociar las decisiones algorítmicas que afectan sus vidas

es una condición necesaria para la democracia digital. Las políticas públicas de educación mediática e informacional, reconocidas por la UNESCO como un derecho humano digital (2021), constituyen un complemento indispensable de la regulación normativa.

Conclusiones

El presente estudio ha argumentado que la erosión de la soberanía digital constituye uno de los fenómenos más significativos y menos atendidos por el derecho internacional contemporáneo. Las corporaciones que controlan las infraestructuras, los protocolos y los datos del ecosistema digital global han acumulado un poder que trasciende las fronteras jurisdiccionales, desafía los principios de soberanía territorial y pone en cuestión la capacidad del derecho internacional para proteger los derechos fundamentales de los ciudadanos en el entorno digital.

La confrontación entre la soberanía digital de los Estados y la hegemonía algorítmica de las grandes corporaciones tecnológicas no es un conflicto técnico, sino un conflicto político fundamental sobre la distribución del poder en la era digital. Los marcos normativos internacionales vigentes —los derechos humanos digitales, la protección de datos, el derecho de la competencia— ofrecen herramientas parciales e insuficientes para abordar esta cuestión. La fragmentación normativa, la asimetría de poder entre reguladores y regulados, la opacidad algorítmica y la ausencia de mecanismos coercitivos internacionales configuran un panorama que demanda una renovación profunda del derecho internacional público.

Las propuestas de auditoría algorítmica obligatoria, reforma de la gobernanza de internet, un tratado internacional vinculante sobre IA y derechos humanos, regulación del mercado digital desde una perspectiva de competencia, y políticas de alfabetización mediática constituyen líneas de acción complementarias que, en su conjunto, apuntan

hacia la necesidad de reconocer la soberanía digital como un derecho humano de nueva generación y de construir los mecanismos institucionales necesarios para hacerla efectiva.

Finalmente, es preciso reconocer que el debate sobre soberanía digital no puede deslindarse de las desigualdades estructurales del sistema internacional. Los países del Sur Global, que generan la mayor parte de los datos que alimentan los algoritmos de las *Big Tech* pero carecen de la infraestructura, la normativa y la capacidad de negociación para regularlas, enfrentan un déficit de soberanía particularmente agudo. Una agenda de investigación futura debe, por tanto, articular la reflexión sobre la soberanía digital con los estudios poscoloniales y la economía política internacional, para evitar que la «soberanía digital» se convierta en un discurso hegemónico más que enmascare viejas asimetrías bajo la retórica de la innovación y la conectividad universal.

Referencias bibliográficas:

- Benkler, Y., Faris, R. y Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford, United Kingdom: Oxford University Press.
- Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford, United Kingdom: Oxford University Press.
- Bradshaw, S. y Howard, P. N. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford, United Kingdom: Oxford Internet Institute.
- Braverman, H. (1998). *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. New York, United States: Monthly Review Press. (Original publicado en 1974).
- Crémer, J., De Montjoye, Y.-A. y Schweitzer, H. (2019). *Competition Policy for the Digital Era: Final Report*. Luxembourg: European Commission.

- DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, United States: Yale University Press.
- Diakopoulos, N. (2016). "Accountability in algorithmic decision-making." *Communications of the ACM*, 59(2), 56-62.
- Dörr, K. N. (2017). "Mapping the fields of fake news." *Information, Communication & Society*, 20(11), 1674-1692.
- Foucault, M. (1975). *Surveiller et punir: Naissance de la prison*. Paris: Gallimard.
- Foucault, M. (1976). *Histoire de la sexualité, vol. I: La volonté de savoir*. Paris: Gallimard.
- Gurumurthy, A. (2020). "Digital sovereignty in the global South: Revisiting the terms of the debate." *IT for Change Working Paper*, 1-20.
- Han, B.-C. (2022). *Infocracia: La digitalización y la crisis de la democracia* (I. Reguera, Trad.). Barcelona: Taurus.
- Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton, United States: Princeton University Press.
- Kurbalija, J. (2019). *An Introduction to Internet Governance*. Malta: DiploFoundation.
- Milan, S. y Treré, E. (2019). "Big data from the South(s): Beyond data universalism." *Television & New Media*, 20(4), 319-335.
- Mueller, M. L. (2010). *Will the Internet Fragment? Sovereignty, Thick and Thin*. Chichester, United Kingdom: Wiley.
- Noble, D. F. (1978). *Forces of Production: A Social History of Industrial Automation*. New York, United States: Oxford University Press.
- Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. New York, United States: Penguin Press.
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, United States: Harvard University Press.
- Rosenblat, A. (2018). *Uberland: How Algorithms Are Rewriting the Rules of Work*. Oakland, United States: University of California Press.
- Roth, B. y Nolan, J. (2019). "Data sovereignty and the challenge for international human rights law." *Data & Policy*, 1, e7.
- Schiller, D. (1984). *Who Knows: Information in the Age of the Fortune 500*. Norwood, United States: Ablex.
- Scholz, T. (2016). *Platform Cooperativism: Challenging the Corporate Sharing Economy*. Berlin: Rosa Luxemburg Stiftung.
- Slaughter, A.-M. y Burke-White, W. (2006). "The future of international law is domestic (or, The European Way of Law)." *Harvard International Law Journal*, 47(2), 327-352.
- Stucke, M. E. (2021). *Better Conflicts: The Case Against Big Tech Antitrust*. Oxford, United Kingdom: Oxford University Press.
- Svantesson, D. y Polčák, R. (2021). "Data localisation and the limits of the EU legal framework." *International Journal of Law and Information Technology*, 29(3), 215-235.
- Van Dijck, J., De Waal, T. y Poell, T. (2018). *The Platform Society: Public Values in a Connective World*. Oxford, United Kingdom: Oxford University Press.
- Villanueva-Mansilla, E. (2018). "Hacia una soberanía digital en América Latina: Discursos y prácticas." *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 19, 1-22.
- Weber, M. (1921). *Wirtschaft und Gesellschaft*. Tübingen, Germany: Mohr Siebeck. (Edición en español: *Economía y sociedad*, México: FCE, 1964).
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, United States: PublicAffairs.