

IBERIDAD DIGITAL Y TECNOPOLÍTICA: SOBERANÍA DE DATOS, INTELIGENCIA ARTIFICIAL GENERATIVA Y CIBERSEGURIDAD EN EL ESPACIO IBEROAMERICANO

DIGITAL IBERICITY AND TECHNOPOLITICS: DATA SOVEREIGNTY, GENERATIVE ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN THE IBERO-AMERICAN SPACE

Juan Pablo Mateos Abarca¹. *Universidad Complutense de Madrid. España.*

Serafín Barros Garbín². *Universidad Complutense de Madrid. España.*

Cómo citar el artículo

Mateos Abarca, Juan Pablo y Barros Garbín, Serafín (2026). Iberidad digital y tecnopolítica: soberanía de datos, inteligencia artificial generativa y ciberseguridad en el espacio iberoamericano. [Digital ibericity and technopolitics: data sovereignty, generative artificial intelligence and cybersecurity in the ibero-american space]. *Revista de Ciencias de la Comunicación e Información*, 31, 1-26. <https://doi.org/10.35742/rcci.2026.31.e357>

RESUMEN

Introducción: El presente artículo investiga la intersección entre tecnopolítica, inteligencia artificial (IA) e infraestructura digital bajo el paradigma de la Neo-Iberidad. Se analiza la capacidad de las naciones iberófonas para articular una autonomía estratégica frente a los oligopolios tecnológicos transnacionales que dominan la infraestructura lógica del siglo XXI. **Metodología:** Mediante una revisión documental sistemática y el análisis comparativo de datos del Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025, se identifican brechas críticas en supercomputación, soberanía de datos y formación avanzada en el espacio iberoamericano. **Resultados:** La soberanía digital no constituye únicamente una cuestión de autonomía normativa, sino una exigencia infraestructural que demanda la creación de bienes públicos digitales compartidos. Se constatan asimetrías estructurales significativas en capacidad de cómputo, formación doctoral especializada y producción de corpus lingüísticos propios. **Discusión:** Los resultados proponen la armonización regulatoria basada en el modelo de la AESIA y el fortalecimiento de la ciberseguridad transatlántica como ejes de defensa democrática frente a actores tecnológicos hegemónicos. **Conclusiones:** El control de la infraestructura física y lógica, y el desarrollo de

¹ Juan Pablo Mateos Abarca: Experto en Inteligencia Artificial, gestión de sistemas multimedia híbridos y herramientas digitales multimedia. Doctor acreditado por la ANECA y profesor del departamento de Periodismo y Nuevos Medios de la Facultad de Ciencias de la Información (UCM).

² Serafín Barros Garbín: Experto en información de la comunicación y herramientas digitales multimedia. Ayudante doctor y profesor del departamento de Periodismo y Nuevos Medios de la Facultad de Ciencias de la Información (UCM).



modelos lingüísticos propios en español y portugués, constituyen el primer paso ineludible para evitar que la identidad cultural iberoamericana sea colonizada por procesos de extracción masiva de datos.

Palabras clave:

Soberanía digital; tecnopolítica; inteligencia artificial generativa; Neo-Iberidad; AESIA; infraestructura digital.

ABSTRACT

Introduction: This article investigates the intersection of technopolitics, artificial intelligence (AI) and digital infrastructure under the Neo-Ibericity paradigm. It analyses the capacity of Ibero-phone nations to articulate a strategic autonomy vis-à-vis the transnational technology oligopolies that dominate the logical infrastructure of the twenty-first century. **Methodology:** Through a systematic documentary review and comparative analysis of data from the Latin American Artificial Intelligence Index (ILIA) 2025, critical gaps are identified in supercomputing, data sovereignty and advanced human capital formation. **Results:** Digital sovereignty is not merely a normative matter but an infrastructural imperative that requires the creation of shared digital public goods. Significant structural asymmetries are found in computing capacity, specialised doctoral training and the production of indigenous linguistic corpora. **Discussion:** The findings propose regulatory harmonisation based on the AESIA model and the strengthening of transatlantic cybersecurity as axes of democratic defence against hegemonic technological actors. **Conclusions:** Control over physical and logical infrastructure and the development of indigenous language models in Spanish and Portuguese are the unavoidable first step to prevent Ibero-American cultural identity from being colonised by processes of mass data extraction.

Keywords:

Digital sovereignty; technopolitics; generative artificial intelligence; Neo-Ibericity; AESIA; digital infrastructure.

1. INTRODUCCIÓN: LA GEOESTRATEGIA DE LA NEO-IBERIDAD

La geopolítica contemporánea ya no se organiza exclusivamente en torno a recursos naturales o capacidad industrial, sino alrededor de infraestructuras invisibles: centros de datos hiperescalables, redes de fibra óptica submarina, semiconductores avanzados y arquitecturas de nube. La soberanía, en consecuencia, se redefine como capacidad de decisión sobre flujos informacionales y sistemas algorítmicos (Castells, 2009).

En este escenario, el espacio iberófono —que agrupa más de seiscientos millones de hablantes de español y portugués distribuidos en Europa y América— ocupa una posición ambivalente. Por un lado, constituye una de las mayores comunidades lingüísticas del mundo, con potencial para generar economías de escala en producción científica, mercado digital y entrenamiento de modelos fundacionales multilingües.

Por otro, presenta una marcada fragmentación infraestructural y dependencia tecnológica respecto a polos hegemónicos situados principalmente en Estados Unidos y Asia oriental.

La transformación digital contemporánea ha trascendido la mera transición técnica para convertirse en una reconfiguración ontológica del poder estatal y social. Como sostiene Castells (2009) en su análisis sobre el poder de la comunicación, en la sociedad red el ejercicio del mando reside en la capacidad de programar los algoritmos y protocolos que median la realidad social. En este contexto, el espacio iberoamericano —una comunidad integrada por más de seiscientos millones de personas y una herencia lingüística compartida— se encuentra ante el desafío de no quedar relegado a ser una mera periferia de consumo masivo de datos.

La irrupción de la Inteligencia Artificial Generativa (IAG) plantea un desafío existencial: la posibilidad de una subordinación cognitiva irreversible ante modelos de pensamiento ajenos, lo que obliga a repensar las naciones no solo como unidades políticas territoriales, sino como comunidades imaginadas (Anderson, 2006) que deben defender su identidad y valores en el ciberespacio. Esta reconfiguración implica que la soberanía ya no se ejerce únicamente sobre el suelo, sino sobre el flujo de bits. Superar el solucionismo tecnológico (Morozov, 2015) requiere reconocer que detrás de cada interfaz hay una arquitectura de poder que beneficia a sus creadores originales, a menudo a expensas de la diversidad lingüística y cultural del sur global.

La Neo-Iberidad surge como un proyecto de resistencia frente a la homogeneización cultural que imponen las grandes plataformas. Según Castells y Himanen (2014), la reconstrucción del estado del bienestar en la era de la información depende de la capacidad de los estados para intervenir en la economía de la información sin asfixiar la innovación. Para Iberoamérica, esto significa crear un ecosistema donde la IA no sea una herramienta de control externo, sino un motor de desarrollo propio.

El problema de investigación que articula este trabajo puede formularse del siguiente modo: ¿es posible transformar la comunidad iberófona en una arquitectura tecnopolítica capaz de sostener soberanía digital en el ecosistema global de la inteligencia artificial generativa? La hipótesis central sostiene que la Neo-Iberidad puede operar como categoría estratégica viable siempre que se consolide una infraestructura compartida de supercomputación, se coordine la formación avanzada de capital humano y se armonicen marcos regulatorios de forma operativa y no meramente declarativa.

2. MARCO TEÓRICO: DEL CAPITALISMO DE PLATAFORMAS AL COLONIALISMO DE DATOS

La transición hacia una sociedad digital soberana exige una infraestructura robusta, modelos de lenguaje que respeten la diversidad lingüística y un marco ético que sitúe al ser humano en el centro del desarrollo algorítmico.

La relevancia de este estudio se inscribe en la necesidad de documentar cómo el espacio iberófono puede articular una respuesta propia frente a la «plataformización» de la vida social y la dependencia de infraestructuras externas. En este sentido, la tecnopolítica se presenta como la disciplina capaz de desentrañar cómo las grandes corporaciones y las telecomunicaciones definen el rumbo de las naciones, afectando la autonomía de los ciudadanos y la integridad de las democracias iberófonas.

La tecnopolítica ha dejado de ser una categoría marginal para convertirse en una tradición teórica y metodológica central en Iberoamérica, especialmente para el estudio de las protestas sociodigitales y la configuración de movimientos sociales en Internet.

El concepto abarca tanto la capacidad de las multitudes conectadas para disputar el sentido de la política a través de la apropiación tecnológica, como la dimensión de la gobernanza algorítmica y el control conductual a través de plataformas digitales. El debate sobre la soberanía digital en América Latina y España se distingue de la perspectiva del Norte Global: mientras que en Europa el discurso se centra en el control de las infraestructuras frente a proveedores externos, en el Sur Global la soberanía digital se vincula estrechamente con la resistencia al colonialismo digital y el extractivismo de datos.

La tecnopolítica se presenta como una categoría funcional que busca la convergencia cultural, científica y tecnológica entre naciones de habla española y portuguesa para reconfigurar las relaciones de poder en el entorno digital. El concepto de tecnopolítica remite a la interrelación entre tecnología y poder en contextos de transformación estructural.

Castells (2009) describió la emergencia de la sociedad red como una reorganización del poder en nodos de información estratégicos. Sin embargo, la actual fase de inteligencia artificial generativa intensifica esta lógica: los nodos no solo distribuyen información, sino que producen conocimiento sintético a escala. La emergencia de la Neo-Iberidad como un espacio de convergencia cultural, científica y tecnológica entre las naciones de habla española y portuguesa plantea una reconfiguración profunda de las relaciones de poder en el entorno digital contemporáneo.

Floridi (2014) planteó que la cuarta revolución tecnológica redefine la agencia humana en entornos informacionales, mientras que marcos internacionales como los principios de la OCDE (About the OECD AI Principles [AI Principles], s.f.) y la Recomendación de la UNESCO (UNESCO, 2021) han promovido una IA centrada en el ser humano. Sin embargo, la soberanía digital no puede reducirse a regulación ética: requiere capacidad material de implementación. Sin infraestructura propia, la regulación depende de arquitecturas técnicas externas, lo que limita su eficacia.

Desde una perspectiva comunicacional, la lengua actúa como activo estratégico en el entrenamiento de modelos de IA y en la circulación del conocimiento. La ausencia de grandes modelos entrenados prioritariamente en español y portugués refuerza dependencias cognitivas respecto a ecosistemas anglófonos. La construcción de corpus estructurados, interoperables y éticamente gobernados se convierte, por tanto, en elemento central de la soberanía digital iberófona.

El concepto de Neo-Iberidad o Iberidad Digital no se limita a una etiqueta, sino que se define como un proyecto de resistencia y autonomía estratégica para las naciones iberófonas frente a los oligopolios tecnológicos. Esta identidad se vincula con la creación de bienes públicos digitales compartidos, como infraestructuras de supercomputación y modelos lingüísticos propios (español y portugués) para evitar la "colonización" de la identidad cultural por procesos de extracción masiva de datos.

La soberanía de los datos se presenta no únicamente como un marco normativo, sino también como una necesidad infraestructural esencial en la era digital contemporánea. La resistencia frente al extractivismo de datos se entiende como una respuesta explícita al colonialismo digital y a la lógica extractivista que subyace en la captura masiva de información.

Este proceso es concebido como una forma de apropiación de la vida misma, orientada hacia la acumulación capitalista. Por tanto, el control soberano sobre los datos emerge

como una estrategia para enfrentar dinámicas de explotación. En cuanto a su materialidad, el discurso sobre la soberanía de datos se entrelaza con el concepto de soberanía tecnológica e infraestructural.

En este sentido, se subraya la importancia de controlar los flujos de información a través de infraestructuras físicas estratégicas, como los cables submarinos (por ejemplo, Ella-Link, <https://ella.link>) y las nubes soberanas, para garantizar que los datos se gestionen conforme al Reglamento General de Protección de Datos (RGPD, 2016) sin estar sujetos a jurisdicciones externas que pongan en riesgo su cumplimiento.

Asimismo, se plantea una propuesta técnica concreta: desarrollar marcos de gobernanza basados en principios de datos abiertos, acompañados de mecanismos locales robustos para la protección de la privacidad. Este enfoque busca equilibrar las asimetrías de poder generadas por las grandes corporaciones tecnológicas, conocidas como Big Tech, promoviendo un modelo más equitativo y justo en la gestión y valorización de la información.

La convergencia entre la política de los medios, la inteligencia artificial (IA) generativa y la ciberseguridad configura uno de los principales desafíos contemporáneos para la soberanía digital y la gobernanza democrática en el espacio iberófono. En el contexto de las sociedades digitalizadas, el poder ya no se ejerce únicamente mediante instituciones políticas tradicionales o estructuras mediáticas convencionales, sino también a través del control de los sistemas algorítmicos capaces de organizar la circulación de la información, modular la opinión pública y condicionar las dinámicas de interacción social. En este sentido, Castells (2009) sostiene que el poder en la sociedad red reside en la capacidad de programar las redes de comunicación y los algoritmos que determinan la percepción de la realidad social, lo que convierte a las plataformas digitales y a sus infraestructuras tecnológicas en actores centrales de la disputa política y cultural contemporánea.

Esta perspectiva adquiere especial relevancia al analizar el impacto de la IA generativa sobre la producción simbólica y los ecosistemas mediáticos. La automatización de contenidos, la personalización algorítmica y la capacidad de generar discursos sintéticos a gran escala han transformado profundamente las relaciones entre ciudadanía, información y poder. Gillespie (2018, p. 13) advierte que las grandes plataformas digitales actúan como auténticos “custodios del internet”, estableciendo criterios de moderación y visibilidad que, lejos de ser neutrales, reproducen sesgos culturales, lingüísticos y geopolíticos. En consecuencia, los algoritmos no solo organizan el acceso a la información, sino que también delimitan los márgenes de lo visible y lo legítimo dentro del espacio digital iberoamericano, afectando de manera directa a la diversidad cultural y al pluralismo comunicativo.

En este escenario, la ciberseguridad deja de ser una cuestión meramente técnica para convertirse en un componente esencial de la defensa democrática y de la soberanía digital. La creciente dependencia de infraestructuras tecnológicas extranjeras expone a los Estados y a las instituciones iberoamericanas a amenazas híbridas, campañas automatizadas de desinformación, ataques a infraestructuras críticas y procesos de manipulación algorítmica capaces de erosionar la confianza pública y la estabilidad institucional.

La ciberseguridad debe concebirse como un bien público estratégico orientado a garantizar el derecho a una vida digital segura, así como la protección de los sistemas de información y de los datos ciudadanos frente a dinámicas de vigilancia y explotación transnacional.

La problemática se intensifica al considerar la creciente opacidad de los sistemas algorítmicos. Pasquale (2015, p. 15) describe este fenómeno mediante la noción de “sociedad de la caja negra”, caracterizada por la expansión de sistemas automatizados que operan sin mecanismos suficientes de transparencia, supervisión ni rendición de cuentas. La toma de decisiones mediada por algoritmos cerrados afecta progresivamente ámbitos fundamentales de la vida social, incluyendo la comunicación pública, los servicios financieros, el acceso al empleo, la administración pública y el sistema judicial.

En el contexto iberoamericano, esta opacidad puede reproducir y amplificar desigualdades históricas, particularmente cuando herramientas predictivas o sistemas automatizados de evaluación incorporan sesgos estructurales que perjudican a comunidades vulnerables y grupos minoritarios. De este modo, la gobernanza algorítmica se convierte en un problema político y ético de primer orden, estrechamente vinculado a la protección de los derechos civiles y a la preservación de la autonomía democrática.

La relación entre política mediática, IA generativa y ciberseguridad adquiere de este modo un carácter estructural e interdependiente. Sin una soberanía tecnológica sustentada en infraestructuras propias, capacidades computacionales autónomas y sistemas de almacenamiento y procesamiento de datos bajo control regional, cualquier intento de regulación ética de la inteligencia artificial resulta limitado e insuficiente.

A su vez, sin un marco robusto de ciberseguridad, la autonomía en la gestión de los datos y la protección de los sistemas institucionales queda seriamente comprometida frente a actores corporativos y geopolíticos externos. La defensa de la soberanía digital exige, por tanto, una articulación simultánea de políticas tecnológicas, regulatorias y comunicativas capaces de responder a las nuevas formas de poder algorítmico.

En este contexto emerge con fuerza el debate sobre el colonialismo de datos, entendido como una nueva modalidad histórica de desposesión basada en la extracción masiva de información personal y colectiva. Mejías y Couldry (2019) sostienen que las dinámicas contemporáneas de captura y explotación de datos reproducen lógicas neocoloniales mediante las cuales las experiencias humanas son convertidas en recursos económicos susceptibles de procesamiento y mercantilización. La expansión de las plataformas digitales y de los sistemas de inteligencia artificial ha consolidado un modelo de acumulación basado en la apropiación sistemática de datos conductuales, consolidando relaciones de dependencia tecnológica entre el Norte y el Sur Global.

Dicha dinámica se encuentra estrechamente vinculada con lo que Zuboff (2019, p. 8) denomina “capitalismo de vigilancia”, un modelo económico sustentado en la extracción, análisis y comercialización de datos destinados a predecir e influir sobre el comportamiento humano. En el ámbito de la Neo-Iberidad, este proceso adquiere una dimensión biopolítica particularmente significativa.

Retomando las aportaciones de Foucault (2007), puede afirmarse que la gestión algorítmica de poblaciones constituye una nueva forma de biopolítica automatizada, donde los mecanismos de control ya no operan únicamente mediante instituciones disciplinarias tradicionales, sino a través de infraestructuras digitales invisibles que clasifican, priorizan y condicionan las conductas sociales. Los algoritmos funcionan de esta forma como dispositivos de regulación social capaces de moldear los discursos públicos, establecer jerarquías de visibilidad y normalizar determinadas formas de participación política y cultural dentro del espacio digital iberoamericano.

La dimensión material de este proceso resulta igualmente relevante. El desarrollo global de la inteligencia artificial depende en gran medida de formas invisibilizadas de trabajo digital, tal como señala Scholz (2016) al analizar las nuevas modalidades de explotación laboral asociadas a las plataformas tecnológicas. En numerosos países iberoamericanos, miles de trabajadores participan en tareas de etiquetación, moderación y entrenamiento de datos fundamentales para el funcionamiento de los sistemas de IA, frecuentemente en condiciones de precariedad y sin garantías laborales adecuadas. La economía digital extractivista consolida una división internacional del trabajo en la que la región aporta datos, fuerza laboral barata y recursos cognitivos, mientras que el control de las infraestructuras, las patentes y la capacidad de innovación permanece concentrado en grandes corporaciones tecnológicas extranjeras.

En consecuencia, la construcción de una auténtica soberanía digital en el espacio iberofono no puede limitarse exclusivamente a la protección de la privacidad o a la regulación técnica de los datos personales. Se trata de una cuestión profundamente política y estratégica que involucra la capacidad de las sociedades iberoamericanas para preservar su autonomía cultural, económica y democrática frente a las nuevas formas de poder algorítmico global. La articulación entre políticas mediáticas, gobernanza algorítmica y ciberseguridad constituye, por tanto, una condición indispensable para garantizar la autodeterminación tecnológica y la protección de los derechos fundamentales en la era de la inteligencia artificial generativa.

2.1. El capitalismo de plataformas y la captura de valor

La economía política de la inteligencia artificial está actualmente dominada por lo que Srnicek (2017) denomina capitalismo de plataformas. Las entidades no son simples intermediarios comerciales, sino infraestructuras básicas que extraen valor de la mediación de toda interacción humana posible. Este contexto altera profundamente la riqueza de las redes (Benkler, 2007), donde la producción social colaborativa —que en los albores de la web prometía una democratización radical del conocimiento— termina siendo capturada por procesos de centralización corporativa extrema.

En el ámbito iberofono se traduce en una precarización sistémica del trabajo digital: los trabajadores de la región operan a menudo en condiciones de mano de obra invisible (Scholz, 2016), alimentando algoritmos globales mediante tareas de etiquetado de datos y moderación de contenido carentes de protecciones laborales básicas. Para contrarrestar dicha tendencia, la región debe fomentar plataformas cooperativas que reinviertan el valor en sus propios creadores. La autonomía no es solo técnica, sino también económica: sin un modelo de negocio que respete la propiedad de los datos generados en español y portugués, la región seguirá siendo un territorio extractivo para el capital digital transnacional.

2.2. Colonialismo de datos y biopolítica algorítmica

El análisis de Mejías y Couldry (2019) sobre el colonialismo de datos revela que la captura de información no es una mera práctica comercial agresiva, sino una forma de apropiación de la vida misma para los fines de la acumulación capitalista. La colonización se manifiesta en el capitalismo de vigilancia, donde el excedente conductual de los ciudadanos es procesado para predecir, condicionar y modificar el comportamiento humano a gran escala. Desde un punto de vista de control poblacional, la tecnopolítica analizada actúa como una forma sofisticada de gobierno (Foucault, 2007), donde los algoritmos de caja negra

(Pasquale, 2015) gestionan servicios públicos esenciales sin la debida transparencia ni rendición de cuentas.

Este fenómeno se agrava cuando se considera que la «sociedad de la caja negra» (Pasquale, 2015, p. 15) oculta sesgos que penalizan desproporcionadamente a los ciudadanos iberofonos en áreas como el crédito o el empleo. Un área de preocupación crítica es la introducción de la IA en los sistemas judiciales: Pasquale (2015) advierte sobre el peligro de privatizar la justicia mediante el uso de algoritmos opacos que dictan sentencias o evalúan riesgos de reincidencia.

En América Latina, donde la brecha de acceso a la justicia es profunda, el uso de las herramientas mencionadas sin supervisión puede exacerbar prejuicios contra minorías. El AI Act (Ley de Inteligencia Artificial de la UE [AI Act], 2024) exige que cualquier sistema de IA de alto riesgo, como los de aplicación judicial, sea explicable y contemple la supervisión humana en su fase de decisión final.

La incorporación de sistemas de inteligencia artificial en el ámbito judicial plantea importantes desafíos éticos, políticos y jurídicos, especialmente en contextos caracterizados por desigualdades estructurales y fragilidad institucional. Se advierte la creciente utilización de algoritmos opacos para emitir recomendaciones judiciales, valorar riesgos de reincidencia o asistir en procesos de toma de decisiones puede conducir a una forma de “justicia automatizada” que desplaza progresivamente la deliberación humana y debilita los principios fundamentales del Estado de derecho.

Siguiendo los planteamientos de Frank Pasquale (2015), la investigación sostiene que estos sistemas de “caja negra” operan mediante mecanismos poco transparentes que dificultan comprender los criterios empleados en la toma de decisiones, así como identificar posibles sesgos incorporados en los modelos algorítmicos. La falta de explicabilidad y supervisión favorece el riesgo de privatización indirecta de la justicia, en la medida en que funciones tradicionalmente vinculadas al ámbito público quedan condicionadas por tecnologías desarrolladas y administradas por corporaciones privadas.

La problemática adquiere una dimensión particularmente crítica en el contexto latinoamericano, donde persisten profundas brechas de acceso a la justicia y elevados niveles de desigualdad social. El texto sostiene que la implementación de herramientas de inteligencia artificial sin mecanismos adecuados de control puede amplificar prejuicios históricos relacionados con factores de clase, género, raza o pertenencia étnica. Los algoritmos aprenden a partir de datos históricos que reflejan prácticas institucionales y sociales previas; como resultado, cuando dichos datos contienen patrones discriminatorios, los sistemas automatizados tienden a reproducir y legitimar esas mismas desigualdades bajo una apariencia de neutralidad técnica.

A ello se suma la persistente desigualdad de género y racial en los espacios de formación tecnológica y desarrollo de inteligencia artificial, lo que limita la diversidad de perspectivas críticas durante el diseño y entrenamiento de los propios sistemas algorítmicos.

Por todo este contexto, la regulación de los algoritmos opacos debe constituir una prioridad estratégica para los países iberoamericanos. La ausencia de mecanismos de transparencia, auditoría y control democrático podría convertir la opacidad técnica en un nuevo instrumento de exclusión social, profundizando las asimetrías existentes en lugar de corregirlas. En este marco, la cuestión no se limita únicamente a mejorar la eficiencia administrativa mediante tecnologías digitales, sino que implica garantizar que la innovación

tecnológica sea compatible con los principios de igualdad, debido proceso y protección de derechos fundamentales.

La creación de organismos especializados en auditoría algorítmica y gobernanza tecnológica permitiría fortalecer mecanismos de control público sobre tecnologías con elevado impacto social, contribuyendo a consolidar una soberanía digital basada en la transparencia, la rendición de cuentas y la protección de los derechos ciudadanos. Sin las consiguientes garantías, la automatización judicial corre el riesgo de transformar la opacidad tecnológica en una herramienta estructural de discriminación y exclusión, debilitando aún más la legitimidad democrática de las instituciones judiciales y ampliando las desigualdades existentes en la región.

La soberanía lingüística no constituye un capricho nacionalista, sino una necesidad para la preservación del pensamiento original. Gillespie (2018) avisa de que los algoritmos de moderación a menudo fallan en entender los matices del español regional o el portugués brasileño, censurando de forma injusta o permitiendo discursos de odio por ignorancia contextual. Al desarrollar modelos propios en supercomputadores locales, Iberoamérica puede garantizar que su patrimonio inmaterial no sea filtrado por los criterios de empresas cuyo objetivo prioritario es el beneficio económico. Como indica la UNESCO (2021), la IA debe promover la diversidad cultural, y esto solo es posible si las herramientas se construyen desde la propia lengua y con la participación activa de sus hablantes.

La afirmación se sustenta en la convergencia entre la fragilidad estructural de los sistemas judiciales iberoamericanos y la creciente incorporación de sistemas algorítmicos opacos en los procesos de toma de decisiones públicas. El artículo sostiene que la expansión de herramientas de inteligencia artificial aplicadas al ámbito judicial introduce riesgos significativos para la garantía efectiva de derechos fundamentales, especialmente en contextos caracterizados por desigualdades históricas y limitaciones institucionales. En este marco, la automatización de decisiones judiciales no puede interpretarse únicamente como un avance tecnológico orientado a la eficiencia administrativa, sino también como un fenómeno político y ético que afecta directamente a la legitimidad democrática de la justicia.

Frente a este escenario, se identifica al AI Act (2024) de la Unión Europea como uno de los principales marcos normativos de referencia para abordar los desafíos derivados de la gobernanza algorítmica. La normativa europea clasifica los sistemas de inteligencia artificial aplicados al ámbito judicial como tecnologías de “alto riesgo”, reconociendo el potencial impacto que las herramientas utilizadas pueden tener sobre los derechos fundamentales y las garantías procesales.

A partir de dicha jerarquía, el AI Act (2024) establece requisitos estrictos relacionados con la explicabilidad, la trazabilidad y la supervisión humana de los sistemas automatizados. El texto destaca especialmente la exigencia de que las decisiones finales permanezcan bajo control humano significativo, evitando que los algoritmos actúen como sustitutos absolutos de la deliberación judicial.

Esta investigación sostiene que la regulación de los sistemas algorítmicos opacos debe constituir una prioridad estratégica para los Estados iberoamericanos. La ausencia de mecanismos sólidos de transparencia, auditoría y rendición de cuentas podría conducir a una profundización de las asimetrías sociales existentes, consolidando formas de exclusión y discriminación mediadas tecnológicamente.

Así mismo, la cuestión no se limita únicamente a la eficiencia o innovación en la administración de justicia, sino que involucra la defensa de principios democráticos fundamentales como la igualdad ante la ley, el debido proceso y el acceso equitativo a la justicia. La incorporación de inteligencia artificial en el ámbito judicial requiere, por tanto, una gobernanza ética y regulatoria capaz de garantizar que la tecnología funcione como instrumento de fortalecimiento institucional y no como mecanismo de reproducción

3. ANÁLISIS TÉCNICO: LA INFRAESTRUCTURA COMO DESTINO

3.1. Materialidad y *cyber power*

Resulta necesario comprender que la soberanía digital no es una entelequia teórica: viaja físicamente por cables de fibra óptica enterrados en el fondo del océano. El control y la propiedad de estas rutas constituye un componente crítico del *cyber power* (Nye, 2010) en el siglo XXI. Durante décadas, la inmensa mayoría del tráfico de datos entre América Latina y la Península Ibérica dependía de nodos norteamericanos, lo que sometía la información a su jurisdicción legal y técnica. Proyectos de conectividad directa, como el cable submarino EllaLink son hitos en la autonomía estratégica que permiten que la cooperación científica en la región (OEI, 2022) se base en una ejecución técnica soberana.

La Secretaría General Iberoamericana (SEGIB, 2024) subraya que la soberanía infraestructural es la base de la soberanía política. Al evitar el tránsito por terceros países, se garantiza que el Reglamento General de Protección de Datos (RGPD, 2016) se cumpla de extremo a extremo en el corredor atlántico iberófono. Conseguir la independencia física permite reducir la latencia y hace viables aplicaciones de IA críticas en telemedicina o industria que anteriormente resultaban inviables por la dependencia de nodos distantes controlados por potencias extranjeras.

3.2. Supercomputación y modelos lingüísticos propios

El entrenamiento de modelos fundacionales de lenguaje requiere una capacidad de cómputo que debe considerarse un recurso estratégico de primer orden. Las iniciativas para el fomento de la ciencia y la transformación digital en la región (OEI, 2022) buscan romper la hegemonía anglocéntrica mediante la creación de una infraestructura de IA entrenada nativamente en español y portugués. Esto resulta vital para evitar que los custodios del internet (Gillespie, 2018) —las grandes plataformas que moderan el contenido y definen la relevancia— impongan sesgos culturales, morales y lingüísticos que erosionen la diversidad epistémica del espacio iberófono.

España ha lanzado el Proyecto ALIA, una infraestructura pública de IA orientada a desarrollar modelos de lenguaje fundacionales en castellano y en las lenguas cooficiales. ALIA se financia con fondos del Plan de Recuperación, Transformación y Resiliencia de la Unión Europea y es coordinado por el Barcelona Supercomputing Center (<https://www.bsc.es/es>), con el objetivo de que empresas, administraciones y universidades cuenten con herramientas de IA abiertas y transparentes que no obliguen a transferir datos sensibles a nubes privadas de terceros.

El entrenamiento de los modelos de la familia ALIA se realiza en el supercomputador MareNostrum 5, cuya potencia de cálculo representa la columna vertebral de esta estrategia, permitiendo procesar miles de millones de palabras para que los modelos operen originalmente en español.

En Portugal, la Agenda Nacional de Inteligencia Artificial (ANIA) 2026-2030 sigue una senda similar: el país aspira a aumentar su capacidad de computación de 60 MW en 2025 hasta entre 700 y 1.000 MW en 2030 (ANIA, 2026). El objetivo es posicionar al país como una «Gigafactory» de IA en el contexto europeo, con una inversión superior a los 400 millones de euros orientada a reducir la dependencia externa y fomentar un ecosistema de startups y pymes competitivas (Agenda Portugal IA 2030, 2026).

Por su parte, el proyecto Latam GPT (<https://www.latamgpt.org>) y CENIA (<https://cenia.cl>) —concebido como modelo público y abierto disponible a partir de junio de 2025 demuestra que el espacio iberófono puede generar sus propias herramientas de innovación aprovechando el talento local y datos soberanos, sin dependencias comerciales de terceros.

4. OBJETIVOS

A partir del análisis realizado, se proponen los siguientes objetivos de investigación:

- O1. Determinar si la Iberidad puede transformarse en una categoría tecnopolítica funcional mediante la articulación de cooperación infraestructural y armonización normativa.
- O2. Evaluar en qué medida la producción científica coordinada en español y portugués incrementa la autonomía estratégica en IA generativa.
- O3. Examinar cómo la convergencia regulatoria en protección de datos fortalece la soberanía digital regional.
- O4. Analizar la cooperación en ciberseguridad como mecanismo para reducir vulnerabilidades sistémicas derivadas de la dependencia tecnológica externa.

5. METODOLOGÍA

El presente estudio se basa en un enfoque cualitativo de carácter exploratorio y descriptivo, fundamentado en una revisión documental sistemática y un análisis comparativo de políticas públicas digitales en el espacio iberoamericano. Siguiendo los protocolos éticos de transparencia académica exigidos en la comunicación científica actual, se declara de forma expresa que, para la optimización lingüística, la corrección de estilo y la estructuración técnica de determinados epígrafes de este manuscrito se han utilizado herramientas de Inteligencia Artificial Generativa bajo supervisión humana constante.

Se garantiza, no obstante, que la autoría intelectual, el análisis crítico de los datos, la interpretación de los resultados y las conclusiones corresponden íntegramente a los firmantes del estudio.

5.1. Protocolo operativo y criterios de selección

La recolección de información se ha articulado mediante un protocolo operativo ejecutado rigurosamente entre diciembre de 2025 y febrero de 2026. La búsqueda de literatura científica y técnica se ha centralizado en las bases de datos Scopus, Web of Science (WoS) y Google Scholar, además del repositorio Dialnet para el ámbito hispanohablante. Se han utilizado cadenas de búsqueda booleanas que combinan términos clave como: (“Soberanía de datos” OR “Data Sovereignty”) AND (“Inteligencia Artificial” OR “Generative AI”) AND (“Iberidad” OR “Iberoamérica”) AND (“Ciberseguridad” OR “Cybersecurity”).

Los criterios de inclusión establecidos para la selección del corpus bibliográfico han sido: a) artículos de revistas indexadas y manuales técnicos publicados en la última década (2015-2025); b) informes y documentos oficiales de organismos internacionales, con especial atención al Índice Latinoamericano de Inteligencia Artificial (ILIA); y c) marcos normativos vigentes. Como criterio de exclusión, se descartaron comunicaciones a congresos sin revisión por pares o artículos de opinión sin base empírica contrastable. Tras una criba inicial de 92 registros identificados, el número final de fuentes primarias y secundarias que sustentan el análisis asciende a 45 documentos.

5.2. Ejes del análisis y procedimiento

El análisis se estructuró en torno a cuatro ejes metodológicos complementarios que aseguran la triangulación de la información y la validez de los resultados:

1. Revisión documental comparada de estrategias nacionales de inteligencia artificial en España, Portugal y diversos países latinoamericanos, así como de informes multilaterales sobre infraestructura digital y formación avanzada.
2. Análisis normativo de marcos regulatorios vinculados a la protección de datos y la gobernanza algorítmica, con especial atención a la Declaración de Santiago (Minciencia, 2023), el Reglamento Europeo de IA (AI Act, 2024) y el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo [RGPD], 2016).
3. Revisión bibliográfica interdisciplinar en los campos de la comunicación, el derecho digital y los estudios de gobernanza tecnológica, orientada a identificar los principales ejes de debate teórico.
4. Análisis crítico-discursivo de indicadores cuantitativos procedentes del Índice Latinoamericano de Inteligencia Artificial 2025 (ILIA, 2025), empleados como proxy para evaluar la brecha tecnológica regional.

5.3. Justificación de la muestra y corpus documental

La selección de la muestra responde a un criterio de representatividad estratégica bajo el paradigma de la “Iberidad digital”, priorizando aquellas naciones que lideran la madurez ecosistémica y la infraestructura lógica en la región. Bajo estos parámetros, el corpus de documentos institucionales primarios analizados fue el siguiente:

1. Eje Ibérico (Europa): Se analizó la arquitectura de gobernanza de la Península Ibérica como puente con la normativa europea (AI Act, 2024). Los documentos exactos examinados fueron la Estrategia Nacional de Inteligencia Artificial (Plan de Recuperación, Transformación y Resiliencia, 2023) de España y los estatutos de creación de su agencia supervisora, así como la Estrategia Nacional de Inteligência Artificial (AI Portugal 2030, 2019)
2. Eje Latinoamericano: Como muestra representativa de la región, se analizaron los planes rectores de los tres países con mayor madurez ecosistémica según el ILIA:
 - Brasil: Estratégia Brasileira de Inteligência Artificial (Ministério da Ciência, Tecnologia e Inovação, 2026).
 - Chile: Política Nacional de Inteligencia Artificial y su plan de acción.

- Colombia: Política Nacional para la Transformación Digital e Inteligencia Artificial (CONPES, 2025).

Este análisis conjunto permite verificar de manera precisa las cifras, previsiones y datos concretos sobre soberanía de datos e infraestructura incluidos en el desarrollo del texto, proporcionando una base empírica verificable para la propuesta de autonomía estratégica tecnológica.

6. RESULTADOS

Los resultados se organizan en torno a las tres dimensiones analíticas del estudio: infraestructura tecnológica, capital humano especializado y arquitectura normativa. El análisis confirma que la soberanía digital iberófona requiere superar tres obstáculos estructurales: insuficiente infraestructura de alto rendimiento, fragmentación científica y coordinación normativa limitada. Sin embargo, también revela oportunidades estratégicas derivadas de la comunidad lingüística ampliada y la convergencia jurídica.

6.1. Brechas estructurales identificadas por el ILIA 2025

A pesar de los avances en infraestructura, la Neo-Iberidad enfrenta una «trampa estructural» caracterizada por la persistencia de brechas tecnológicas profundas. El Índice Latinoamericano de Inteligencia Artificial 2025 (ILIA, 2025) revela que la región experimenta un crecimiento récord en inversión digital, pero este no se traduce necesariamente en una reducción de la desigualdad.

La brecha digital en Iberoamérica es multidimensional y se manifiesta en cuatro niveles principales:

- (1) barreras físicas y geográficas, dado que la insuficiencia de infraestructura de banda ancha fija en zonas rurales limita el acceso equitativo a las tecnologías emergentes;
- (2) brecha de especialización, manifestada en un fenómeno de «embudo» donde existe alta alfabetización general en IA pero una escasez crítica de talento especializado —en 11 de los 19 países analizados por el ILIA no existen programas de doctorado en IA—;
- (3) desigualdad de género y raza en la formación tecnológica, que excluye a mujeres y minorías étnicas, limitando la diversidad de perspectivas en el desarrollo algorítmico; y
- (4) concentración extrema del acceso al cómputo, con Brasil acaparando la mayoría de la capacidad de procesamiento de toda América Latina, lo que genera asimetrías severas dentro de la propia región.

Tabla 1. Correspondencia entre brechas del ILIA 2025 y propuestas de Neo-Iberidad

Dimensión ILIA 2025	Brecha identificada en la región	Propuesta de autonomía estratégica
Infraestructura	Déficit en nodos de supercomputación locales.	Inversión en centros de cómputo soberanos y cables directos.
Datos y algoritmos	Sesgo anglocéntrico en modelos de inteligencia artificial generativa comerciales.	Desarrollo de modelos fundacionales entrenados en español y portugués.
Gobernanza	Fragmentación regulatoria entre naciones.	Armonización normativa basada en el modelo de la Agencia Española de Supervisión de Inteligencia Artificial y el <i>Artificial Intelligence Act</i> .
Ciberseguridad	Vulnerabilidad ante amenazas híbridas externas.	Protocolos de ciberdefensa transatlántica compartida.
Capital humano	Escasez de doctores en inteligencia artificial en la mayoría de los países.	Programas doctorales regionales y movilidad científica.

Fuente: Elaboración propia a partir de datos del ILIA (2025).

6.2. Capacidades institucionales emergentes

Frente a este diagnóstico, el análisis documental revela la emergencia de capacidades institucionales relevantes. La creación de la Agencia Española de Supervisión de la IA (AE-SIA), enmarcada en el *Artificial Intelligence Act* (EU, 2024), propone un enfoque proactivo mediante *sandboxes* regulatorios que permiten la experimentación en entornos controlados. Este modelo garantiza que los sistemas tecnológicos respeten desde su diseño los principios éticos de la OCDE (AI Principles, s.f.) y las recomendaciones sobre la ética de la IA de la UNESCO (2021), al tiempo que facilita la exportación de un marco de confianza que podría ser adoptado por los países iberoamericanos.

La Declaración de Santiago (Minciencia, 2023), firmada por 20 países de la región con el apoyo de la UNESCO y la CAF, establece principios de transparencia, inclusión y sostenibilidad para el desarrollo de la IA, con especial énfasis en la gobernanza multiactoral y la protección de los neuroderechos. España ha reforzado su visión ética con el lanzamiento de un Sello de IA Ética voluntario para empresas, que garantiza que los algoritmos se apliquen de forma fiable y no discriminatoria.

El análisis de colectivos sociales en América Latina, como Atalaya Sur en Argentina o Sur-siendo en México, demuestra, además, que la soberanía digital se construye no solo desde arriba, mediante políticas públicas, sino también mediante la apropiación popular de la tecnología y la creación de redes autónomas que desafían la lógica del capital digital.

6.3. Dimensiones de la soberanía digital iberoamericana

En términos de contribución científica, el estudio aporta una visión articulada que integra dimensiones tecnológicas, organizativas y formativas, superando enfoques fragmentarios.

Asimismo, plantea la necesidad de futuras investigaciones longitudinales que evalúen el impacto real de la inteligencia artificial en la calidad informativa, la diversidad de

contenidos y la sostenibilidad económica de los medios. El análisis confirma que la soberanía digital iberófona requiere superar tres obstáculos estructurales: insuficiente infraestructura de alto rendimiento, fragmentación científica y coordinación normativa limitada. Sin embargo, también revela oportunidades estratégicas derivadas de la comunidad lingüística ampliada y la convergencia jurídica.

La Neo-Iberidad puede conceptualizarse como proyecto infraestructural orientado a la creación de consorcios de supercomputación regionales, desarrollo de modelos fundacionales en español y portugués y establecimiento de marcos regulatorios interoperables. La cooperación no implica aislamiento tecnológico, sino fortalecimiento de la capacidad negociadora colectiva frente a actores hegemónicos globales. La soberanía digital debe entenderse como autonomía relacional, no como autarquía tecnológica.

Tabla 2. Dimensiones de soberanía digital y desafíos tecnopolíticos en el espacio iberófono

Dimensión	Desafío en el espacio iberófono	Propuesta tecnopolítica
Soberanía de infraestructura	Dependencia de servicios de computación en la nube alojados fuera del territorio nacional.	Desarrollo de nubes soberanas y fortalecimiento de infraestructuras regionales de supercomputación.
Soberanía de datos	Extractivismo de datos por parte de grandes corporaciones tecnológicas (Big Tech).	Implementación de marcos de gobernanza de datos abiertos y mecanismos de protección de la privacidad local.
Soberanía lingüística	Escasez de datos de entrenamiento en español y portugués en sistemas de inteligencia artificial.	Desarrollo de modelos fundacionales propios, como el proyecto ALIA en España y ANIA en Portugal.
Soberanía tecnológica	Dependencia de software y hardware propietario desarrollado en otros países.	Fomento del software libre, el hardware abierto y modelos de cooperativismo tecnológico.

Fuente: Elaboración propia.

La relación entre soberanía digital y desafíos tecnopolíticos constituye uno de los ejes esenciales para comprender las transformaciones contemporáneas del poder en la sociedad digital. En el contexto del siglo XXI, la soberanía ya no puede limitarse únicamente al control territorial clásico ejercido por los Estados, sino que debe redefinirse como la capacidad de decisión, gestión y autonomía sobre los flujos informacionales, las infraestructuras tecnológicas y los sistemas algorítmicos que organizan la vida social, económica y política. En este contexto, la tecnopolítica emerge como un campo de análisis orientado a examinar las formas en que el poder se ejerce mediante la programación de algoritmos, protocolos digitales e infraestructuras de comunicación que median la construcción de la realidad social y condicionan los procesos de interacción colectiva.

En este marco, la soberanía digital posee una dimensión material inseparable de las infraestructuras tecnológicas que sustentan la circulación global de datos. La dependencia de redes de fibra óptica, centros de datos y plataformas controladas por actores externos sitúa a los países iberoamericanos en una posición de vulnerabilidad estratégica frente a jurisdicciones extranjeras y grandes corporaciones tecnológicas.

La infraestructura digital constituye, por tanto, una expresión concreta del poder contemporáneo, en la medida en que determina quién controla los flujos de información, las capacidades de almacenamiento y los procesos de procesamiento de datos. Frente al marco actual, el fortalecimiento de nubes soberanas, centros regionales de supercomputación y sistemas autónomos de conectividad aparece como una estrategia orientada a transformar la dependencia tecnológica en capacidad de autonomía estratégica. La construcción de infraestructuras digitales propias no responde únicamente a objetivos técnicos o económicos, sino también a la necesidad de preservar la capacidad de decisión política sobre los ecosistemas digitales de la región.

De forma complementaria, la soberanía de datos se configura como una respuesta crítica frente a las dinámicas contemporáneas de colonialismo digital. La extracción masiva de datos personales y conductuales por parte de las grandes corporaciones tecnológicas reproduce formas de apropiación que convierten la experiencia humana en un recurso explotable para la acumulación de capital. En este contexto, las dinámicas asociadas al denominado “capitalismo de vigilancia”, conceptualizado por Shoshana Zuboff (2019), evidencian cómo la información generada por los usuarios es utilizada para predecir, influir y modificar comportamientos sociales a gran escala.

La tecnopolítica contemporánea enfrenta el desafío de evitar que las sociedades iberoamericanas sean reducidas a territorios periféricos de extracción informacional al servicio de plataformas transnacionales. Como alternativa, se plantea la necesidad de desarrollar marcos de gobernanza de datos abiertos, transparentes y democráticos, capaces de garantizar la protección de la privacidad, la autonomía ciudadana y el control soberano sobre los recursos informacionales de la región.

Otra dimensión esencial de la soberanía digital se relaciona con la preservación de la diversidad lingüística y la autonomía epistemológica. La inteligencia artificial comercial dominante reproduce con frecuencia sesgos anglocéntricos que limitan la representación adecuada de los matices culturales, semánticos y contextuales propios del español y del portugués en sus múltiples variantes regionales, con el consiguiente riesgo de una creciente subordinación cognitiva respecto de modelos de pensamiento desarrollados desde perspectivas culturales ajenas a la realidad iberoamericana.

En este sentido, el desafío tecnopolítico no consiste únicamente en traducir contenidos o adaptar herramientas existentes, sino en desarrollar modelos fundacionales propios capaces de incorporar de manera nativa las particularidades lingüísticas y culturales del espacio iberófono. Iniciativas como ALIA y ANIA representan avances significativos hacia la construcción de capacidades autónomas en inteligencia artificial, orientadas a preservar el patrimonio lingüístico y evitar que los criterios culturales de plataformas extranjeras definan los marcos de producción y circulación del conocimiento.

6.4. Ciberseguridad como dimensión defensiva de la soberanía

La expansión de infraestructuras digitales amplía la superficie de ataque cibernético, convirtiendo la ciberseguridad en elemento central de la tecnopolítica contemporánea. Los gobiernos de Iberoamérica han dado pasos firmes hacia la digitalización, pero gran parte de sus sistemas públicos siguen siendo vulnerables debido a arquitecturas fragmentadas o dependientes de nubes extranjeras.

El panorama de amenazas para 2025-2026 se caracteriza por una mayor sofisticación de los ataques, que incluyen el *Ransomware-as-a-Service* (RaaS), que facilita que actores criminales lancen ataques complejos a bajo costo dirigidos a sectores críticos como la salud y la energía; la extorsión cuádruple, mediante la que los atacantes cifran datos, roban información confidencial, amenazan con publicarla y atacan a los socios comerciales de la víctima; y la vigilancia geopolítica, donde el uso de tecnologías de vigilancia extranjeras en proyectos de ciudades inteligentes puede comprometer la seguridad nacional al transferir patrones de comportamiento ciudadano a operadores externos (Morales Ramirez, 2025).

La ciberseguridad soberana exige el control sobre los activos digitales estratégicos. Esto implica no solo la implementación de herramientas técnicas, sino también el cumplimiento de estándares normativos como la Directiva NIS2 en Europa o el Esquema Nacional de Seguridad en España (Heredero del Campo, 2023). La adopción de un modelo de Seguridad de Confianza Cero (*Zero Trust*) resulta esencial para proteger terminales y servidores fuera del perímetro seguro tradicional (Gil Villa *et al.*, 2025). La utilización de productos cualificados por agencias nacionales —como el CCN en España— garantiza que la defensa de la infraestructura crítica no dependa de tecnologías con posibles vulnerabilidades de origen geopolítico.

La soberanía digital en el espacio iberofono no debe interpretarse como una estrategia de aislamiento tecnológico o repliegue autárquico, sino como una forma de “autonomía relacional” orientada a fortalecer la capacidad de negociación colectiva frente a los grandes oligopolios tecnológicos globales. La soberanía digital implica la construcción de capacidades compartidas que permitan a los países iberoamericanos reducir dependencias estructurales, proteger sus infraestructuras críticas y desarrollar modelos tecnológicos alineados con sus realidades culturales, lingüísticas y políticas. Este enfoque exige articular de manera integrada diversas dimensiones estratégicas que trascienden los enfoques fragmentarios tradicionalmente asociados a la gobernanza tecnológica.

En primer lugar, la soberanía de infraestructura constituye un componente esencial de lo que Joseph Nye (2010) denomina *cyber power*, entendido como la capacidad de influir y ejercer poder a través del control de las redes digitales y las infraestructuras de comunicación. En el contexto contemporáneo, la soberanía digital depende en gran medida del dominio material de la red, incluyendo cables submarinos, centros de datos, sistemas de almacenamiento y capacidades de computación avanzada. Infraestructuras estratégicas como EllaLink representan elementos clave para reducir la dependencia tecnológica de nodos extranjeros y fortalecer la autonomía regional en el flujo de información.

En este sentido, el fortalecimiento de nubes soberanas, centros regionales de supercomputación y capacidades propias de procesamiento de datos resulta indispensable para garantizar que estándares regulatorios como el Reglamento General de Protección de Datos puedan aplicarse de forma efectiva a lo largo de toda la cadena de circulación de información, minimizando interferencias externas y vulnerabilidades geopolíticas (Cordova Urbina *et al.*, 2025).

En segundo lugar, la soberanía de datos se plantea como una respuesta crítica frente al fenómeno del colonialismo digital. Siguiendo los planteamientos de Ulises Mejías y Nick Couldry (2019), la extracción masiva de datos constituye una nueva forma de apropiación sistemática de la experiencia humana, orientada a alimentar las dinámicas de acumulación propias del capitalismo digital contemporáneo. Dicha lógica se encuentra

estrechamente vinculada a lo que Shoshana Zuboff (2019, p. 8) conceptualiza como “capitalismo de vigilancia”, un modelo económico basado en la captura, procesamiento y monetización de datos conductuales a gran escala.

Frente a la dinámica extractivista, la propuesta tecnopolítica iberoamericana demanda el establecimiento de marcos de gobernanza de datos abiertos, transparentes y democráticos, capaces de garantizar la protección de la privacidad y evitar que la región continúe funcionando como un territorio periférico de extracción informacional al servicio del capital tecnológico transnacional.

Una tercera dimensión corresponde a la soberanía lingüística y la autonomía epistemológica. La lengua constituye una infraestructura estratégica para la preservación de la diversidad cultural y para la producción de conocimiento autónomo en entornos digitales. Tarleton Gillespie (2018, p. 13) advierte que las grandes plataformas tecnológicas, en su condición de “custodios del internet”, reproducen sesgos culturales y lingüísticos al no comprender adecuadamente los matices semánticos, contextuales y socioculturales del español y del portugués en sus múltiples variantes regionales.

Esta limitación no solo afecta la calidad de los sistemas automatizados, sino que también favorece formas de subordinación cognitiva y dependencia epistemológica respecto de modelos de inteligencia artificial entrenados desde perspectivas anglocéntricas. En este contexto, iniciativas como ALIA y ANIA adquieren una relevancia estratégica al promover el desarrollo de modelos fundacionales entrenados nativamente en lenguas ibéricas, fortaleciendo la capacidad regional para generar tecnologías coherentes con sus contextos culturales y comunicativos.

Por otra parte, la soberanía tecnológica requiere incorporar una dimensión ética orientada a garantizar que la innovación científica y técnica responda a principios democráticos y de justicia social. Frente a la creciente opacidad característica de la denominada “sociedad de la caja negra”, conceptualizada por Frank Pasquale (2015, p. 15), resulta imprescindible promover mecanismos de transparencia algorítmica, auditoría pública y desarrollo de software libre. En este sentido, la integración de la “ética de la invención”, propuesta por Sheila Jasanoff (2016), constituye un elemento prioritario para asegurar que los procesos de innovación tecnológica no se reduzcan a lógicas de eficiencia técnica o automatización indiscriminada.

El concepto se contrapone al “solucionismo tecnológico” criticado por Morozov (2015, p. 5), según el cual los problemas sociales pueden resolverse exclusivamente mediante herramientas digitales sin considerar sus implicaciones políticas, culturales y éticas. Por el contrario, la soberanía tecnológica iberoamericana debe orientarse hacia modelos de innovación comprometidos con la protección de derechos humanos, la equidad social y la participación democrática (Marzani y Pires, 2024).

El análisis desarrollado confirma que la consolidación de estas dimensiones enfrenta obstáculos estructurales significativos, entre ellos la insuficiente infraestructura de computación de alto rendimiento, la dependencia tecnológica externa y la fragmentación científica existente entre los países iberoamericanos. En este contexto, la Neo-Iberidad se proyecta como un marco estratégico de cooperación transatlántica orientado a construir capacidades tecnológicas compartidas y fortalecer mecanismos regionales de gobernanza digital.

La armonización normativa inspirada en modelos institucionales como la Agencia Española de Supervisión de la Inteligencia Artificial [AESIA], s.f.) , junto con la creación de consorcios científicos y tecnológicos regionales, aparece así como una estrategia vertebradora para defender la integridad democrática y la autonomía digital frente a la creciente concentración de poder ejercida por actores tecnológicos hegemónicos a escala global.

7. DISCUSIÓN

El análisis confirma que la soberanía digital iberófona requiere superar tres obstáculos estructurales: insuficiente infraestructura de alto rendimiento, fragmentación científica y coordinación normativa limitada. Sin embargo, también revela oportunidades estratégicas derivadas de la comunidad lingüística ampliada y la convergencia jurídica entre los países de tradición romano-germánica del espacio iberoamericano.

La Neo-Iberidad puede conceptualizarse como proyecto infraestructural orientado a tres objetivos convergentes: la creación de consorcios de supercomputación regionales, el desarrollo de modelos fundacionales en español y portugués, y el establecimiento de marcos regulatorios interoperables. La cooperación no implica aislamiento tecnológico, sino fortalecimiento de la capacidad negociadora colectiva frente a actores hegemónicos globales. La soberanía digital debe entenderse, por tanto, como autonomía relacional y no como autarquía tecnológica.

La construcción de la Neo-Iberidad digital requiere un compromiso con valores humanos inalienables. La Declaración de Santiago (Minciencia, 2023) y la AESIA representan hitos institucionales que posicionan al espacio iberófono como un referente en el uso responsable de la tecnología. La integración de la ética de la invención (Jasanoff, 2016) y la regulación de los algoritmos opacos (Pasquale, 2015) debe ser la prioridad para evitar una justicia automatizada e injusta. Esta visión aleja el análisis del pesimismo tecnodeterminista y lo sitúa en la vanguardia de una modernidad digital alternativa, donde la tecnología sirve a la comunidad y no solo al mercado.

En el ámbito del capital humano, se observa crecimiento en programas formativos en inteligencia artificial, pero con densidad doctoral insuficiente en la mayoría de los países iberoamericanos y una significativa emigración de talento hacia polos tecnológicos globales.

Para cerrar estos espacios, la cooperación internacional se vuelve esencial. La Alianza Digital UE-ALC (https://www.eeas.europa.eu/eeas/alianza-digital-eu-lac_es) apoyada por el programa Global Gateway (https://internationalpartnerships.ec.europa.eu/policies/global-gateway_es), busca movilizar inversiones sustanciales para fortalecer los sistemas de educación, investigación y conectividad segura en ambos lados del Atlántico, con el objetivo de crear vínculos que reduzcan el déficit de inversión mundial sin generar nuevas dependencias.

La ciberseguridad debe entenderse como el pilar que sostiene la integridad de la Neo-Iberidad frente a las amenazas híbridas contemporáneas. La cooperación en ciberdefensa entre España, Portugal y América Latina (SEGIB, 2024) permite el intercambio de inteligencia sobre amenazas en tiempo real, mitigando los riesgos de que actores externos erosionen la confianza en las instituciones democráticas mediante la desinformación automatizada. La SEGIB (2024) subraya que la ciberseguridad es un bien público que debe protegerse colectivamente: los países con menos recursos pueden beneficiarse del

paraguas de seguridad de los nodos más avanzados del espacio iberofono, creando una red de resiliencia que proteja el derecho de los ciudadanos a una vida digital segura.

La ciberseguridad debe ser comprendida como el elemento estructural que sostiene la integridad del proyecto de la Neo-Iberidad frente al incremento de las amenazas híbridas en el entorno digital contemporáneo. Lejos de limitarse a una dimensión meramente técnica o instrumental, se configura como una expresión concreta del *cyber power*, en la medida en que la soberanía digital contemporánea se articula a partir de la capacidad de control, gestión y protección de los activos digitales, así como de las infraestructuras y rutas de circulación de la información.

En este contexto, la cooperación en materia de ciberdefensa entre España, Portugal y América Latina, impulsada en el marco de la Secretaría General Iberoamericana, no solo facilita el intercambio de inteligencia sobre amenazas en tiempo real, sino que también se inscribe en una dinámica más amplia de disputa por el control de los flujos comunicacionales y de los entornos informacionales que configuran la esfera pública.

El planteamiento de Castells (2009) resulta especialmente relevante, en tanto que el poder contemporáneo se fundamenta en la capacidad de programar redes y algoritmos que median la construcción de la realidad social. En consecuencia, la ciberseguridad adquiere una dimensión política central al convertirse en un mecanismo de contención frente a la desinformación automatizada, la cual no solo distorsiona los procesos comunicativos, sino que también puede erosionar la legitimidad institucional y debilitar la confianza ciudadana en los sistemas democráticos. En este sentido, la protección del ecosistema digital se configura como una forma de resistencia frente a la posibilidad de que actores externos reconfiguren, mediante infraestructuras algorítmicas, las percepciones colectivas y los marcos de interpretación social.

Asimismo, desde la óptica del colonialismo de datos formulada por Mejías y Couldry (2019), la ciberseguridad puede ser interpretada como una frontera estratégica frente a las dinámicas de extracción masiva de información y vigilancia sistemática propias del capitalismo digital contemporáneo. En este marco, la propuesta de la Secretaría General Iberoamericana (SEGIB, 2024) de concebir la ciberseguridad como un bien público compartido ofrece una respuesta institucional a las asimetrías estructurales identificadas por el Índice Latinoamericano de Inteligencia Artificial, donde la concentración de capacidades tecnológicas en un número reducido de actores genera dependencias críticas y vulnerabilidades sistémicas en amplias zonas del espacio iberoamericano.

La articulación de un modelo de “paraguas de seguridad” regional permite, en este sentido, reducir dichas brechas mediante la cooperación solidaria entre Estados con distintos niveles de desarrollo tecnológico, fortaleciendo así la resiliencia colectiva sin recurrir a lógicas de dependencia externa ni a enfoques de tipo solucionista.

La soberanía tecnológica en Iberoamérica se apoya en tres pilares interconectados: las infraestructuras públicas y abiertas, concebidas como bienes públicos con gobernanza regional participativa; el acceso abierto al conocimiento, garantizado por sistemas como Latindex, Redalyc o SciELO; y la identidad y la lengua, mediante el entrenamiento de modelos de IA con datos que reflejen las problemáticas, idiomas y conocimientos propios de la región, evitando la subordinación epistemológica.

8. CONCLUSIONES

La soberanía tecnológica en Iberoamérica es un proyecto material y político que exige superar definitivamente la fase de consumo pasivo y dependiente. Como se ha analizado, el control de la infraestructura física y lógica constituye el primer paso ineludible para evitar que la vida humana sea colonizada por el capital transnacional mediante procesos de extracción masiva de datos (Mejías y Couldry, 2019).

El liderazgo institucional a través de agencias de supervisión como la AESIA (s.f.), la inversión en ciencia y educación superior (OEI, 2022) y el desarrollo de modelos de lenguaje propios, son las herramientas necesarias para construir una inteligencia artificial que respete los valores democráticos, la privacidad y la inmensa riqueza lingüística de la Neo-Iberidad.

- C1: La infraestructura y la lengua como pilares de soberanía. El control sobre la infraestructura física (cables submarinos) y lógica, sumado al desarrollo de modelos de inteligencia artificial entrenados nativamente en español y portugués, es el paso ineludible para proteger la identidad cultural iberoamericana y evitar la colonización cognitiva por parte de potencias tecnológicas externas.
- C2: La soberanía como autonomía relacional. La soberanía digital en el espacio iberoamericano no debe buscar la autarquía tecnológica, sino una "autonomía relacional" que fortalezca la capacidad negociadora colectiva mediante la armonización normativa (siguiendo modelos como la AESIA), la cooperación científica y la creación de consorcios regionales de supercomputación.
- C3: La ciberseguridad como bien público y defensa democrática. La ciberseguridad se constituye como el pilar defensivo esencial de la Neo-Iberidad, debiendo ser gestionada como un bien público compartido que proteja la integridad de las instituciones democráticas y la privacidad de los ciudadanos frente a las amenazas híbridas y el capitalismo de vigilancia.
- C4: Necesidad de una reflexión estructural y soberanía vinculada: La integración de la inteligencia artificial en el espacio iberoamericano debe trascender la mera innovación técnica para basarse en una reflexión estructural que priorice la ciberseguridad transatlántica y la autonomía epistemológica.

Solo a través de una acción coordinada podrá el espacio iberoamericano garantizar su autonomía. La integración de la ética de la invención (Jasanoff, 2016) y la regulación de los algoritmos opacos (Pasquale, 2015) debe ser la prioridad para evitar una justicia automatizada e injusta.

La lengua, tradicionalmente concebida como elemento cultural, se convierte así en infraestructura estratégica: la producción científica coordinada en español y portugués puede generar corpus propios para el entrenamiento de IA, establecer marcos éticos adaptados a contextos socioculturales específicos y reducir los sesgos culturales presentes en modelos entrenados predominantemente en inglés.

Los desafíos son inmensos —desde la ciberdelincuencia transnacional hasta la brecha de especialización—, pero el potencial de la Neo-Iberidad para transformar el panorama digital global es igualmente significativo. La colaboración entre España, Portugal e Iberoamérica, bajo principios de integridad, equidad y diversidad, es el único camino para asegurar que los frutos de la revolución digital beneficien al conjunto de la sociedad. La Neo-

Iberidad digital se proyecta, en definitiva, como un futuro compartido donde la tecnología sirve para unir culturas, proteger derechos y potenciar el desarrollo científico de los pueblos iberófonos, protegiendo la infósfera iberoamericana frente a las derivas del capitalismo de vigilancia global.

9. REFERENCIAS

- About the OECD AI Principles (s.f.). *Shaping a human-centric approach to artificial intelligence*. <https://www.oecd.org/en/topics/ai-principles.html>
- Agencia Española de Supervisión de Inteligencia Artificial. (s.f.). *Garantizando una IA ética y responsable*. Recuperado el 1 de marzo de 2026. <https://aesia.digital.gob.es/es>
- Agenda Portugal IA 2030. (12 de enero de 2026). *Portugal aprova Agenda Nacional de Inteligência Artificial com investimento até 2030*. <https://n9.cl/16em5u>
- AI Act. (13 de junio de 2024). *Ley de Inteligencia Artificial de la UE | Avances y análisis actualizados de la Ley de Inteligencia Artificial de la UE*. <https://artificialintelligenceact.eu/es/ai-act-explorer/>
- AI Portugal 2030. (31 de mayo de 2019). *Estratégia Inteligência Artificial 2030*. <https://acortar.link/6yzCFW>
- Anderson, B. R. O. (2006). *Imagined communities: Reflections on the origin and spread of nationalism*. Verso. <https://acortar.link/k1NjH3>
- ANIA. (8 de enero de 2026). *IA ao serviço da sociedade e da competitividade de Portugal*. digital.gov.pt. <https://acortar.link/9FtKY1>
- Benkler, Y. (2007). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press. [https://www.benkler.org/Benkler Wealth Of Networks.pdf](https://www.benkler.org/Benkler%20Wealth%20Of%20Networks.pdf)
- Castells, M. (2009). *Communication power*. Oxford University Press.
- Castells, M. y Himanen, P. (2014). *Reconstruir el estado del bienestar: La economía de la información y el estado red*. Alianza Editorial.
- CONPES. (28 de febrero de 2025). *Un vistazo a la política de Inteligencia Artificial CONPES 4144 y la Propiedad Intelectual*. <https://acortar.link/ce9mUp>
- Cordova Urbina, D. A., Diaz Sifuentes, S. H. y Mendoza De Los Santos, A. C. (2025). Zero Trust en la gestión de identidades y accesos en la nube: una revisión de modelos, ventajas y limitaciones. *Ingeniería Investiga*, 8. <https://doi.org/10.47796/ing.v8i00.1342>
- EU. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations. <http://data.europa.eu/eli/reg/2024/1689/oj>
- Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
- Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977-1978*. Palgrave Macmillan.

- Gil Villa, A. F., Espinoza Dávalos, S. A. y Mendoza De Los Santos, A. C. (2025). Implementación de arquitecturas Zero Trust: revisión sistemática de beneficios y desventajas. *Ingeniería Investiga*, 8, e1331. <https://doi.org/10.47796/ing.v8i00.1331>
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Herederro del Campo, C. (2023). Nueva Directiva Europea NIS 2: Un avance en la regulación de la ciberseguridad para las actuales sociedades digitalizadas modernas. *De-recho Digital e Innovación. Digital Law and Innovation Review*, (16 (abril-junio)), 5. <https://n9.cl/pzwwkzh>
- ILIA. (2025). *Índice Latinoamericano de Inteligencia Artificial 2025*. <https://hdl.handle.net/11362/82514>
- Jasanoff, S. (2016). *The ethics of invention: Technology and the human future*. W. W. Norton & Company.
- Marzani, C. F. P., y Pires, J. F. (2024). Solucionismo tecnológico: Um estudo acerca de como a ideologização da tecnologia pode trazer riscos à democracia. *Problemata*, 15(3), 109-123. <https://doi.org/10.7443/problemata.v15i3.69849>
- Mejías, U. y Couldry, N. (2019). Colonialismo de datos: Repensando la relación de los datos masivos con el sujeto contemporáneo. *Virtualis: revista de cultura digital*, 10(18), 78-97. <https://acortar.link/Mim8rH>
- Minciencia. (24 de octubre de 2023). *Chile liderará iniciativa de gobernanza de inteligencia artificial en América Latina*. <https://acortar.link/ffhV5l>
- Ministério da Ciência, Tecnologia e Inovação. (2026, 13 de enero). *Estratégia Brasileira de Inteligência Artificial*. Governo do Brasil. <https://n9.cl/154qm>
- Morales Ramirez, O. (2025). Ciberfraude: Principales métodos de ataque y estrategias para su prevención. *Ciencia Latina Revista Científica Multidisciplinar*, 9(3), 4901-4921. https://doi.org/10.37811/cl_rcm.v9i3.18122
- Morozov, E. (2015). *La locura del solucionismo tecnológico* (1ª ed). Katz.
- Nye, J. S. (2010, mayo). *Cyber power*. Harvard Kennedy School, Belfer Center for Science and International Affairs. <https://www.belfercenter.org/publication/cyber-power>
- OEI. (2022). Programa Iberoamericano de Transformación Digital en Educación. <https://short.do/WzwMAK>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Plan de Recuperación, Transformación y Resiliencia. (05 de junio de 2023). Conoce *Estrategia Nacional de Inteligencia Artificial (ENIA)*. <https://acortar.link/npTGK7>
- RGPD. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD). <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>
- Scholz, T. (2016). *Uberworked and underpaid: How workers are disrupting the digital economy*. Polity Press.
- SEGIB. (31 de julio de 2024). *Resumen de 2023 en la Memoria Anual SEGIB*. Secretaría General Iberoamericana. <https://acortar.link/hgEfAx>

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

UNESCO. (23 de noviembre de 2021). *Recommendation on the ethics of artificial intelligence*. UNESCO Publishing. Recuperado el 21 de febrero de 2026, de https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power (First trade paperback edition)*. PublicAffairs.

CONTRIBUCIONES DE AUTORES, FINANCIACIÓN Y AGRADECIMIENTOS

Conceptualización: Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Metodología:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Software:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Validación:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Análisis formal:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Curación de datos:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Preparación del borrador original:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Redacción-Revisión y Edición:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Supervisión:** Barros Garbín, Serafín. **Administración de proyectos:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín. **Todos los autores han leído y aceptado la versión publicada del manuscrito:** Mateos Abarca, Juan Pablo y Barros Garbín, Serafín.

Financiación: No ha habido financiación.

Agradecimientos: Agradecemos al I Congreso sobre la Neo-Iberidad CINIBER 2026 sus aportaciones para la realización de este trabajo.

Conflicto de intereses: No hay conflicto de intereses.

AUTORES

Juan Pablo Mateos Abarca

Universidad Complutense de Madrid, España.

Doctor en Empresa Informativa por la Universidad Complutense de Madrid (UCM) con mención Cum Laude. Actualmente es Profesor en el Departamento de Periodismo y Nuevos Medios de la Facultad de Ciencias de la Información (UCM). Acreditado como Contratado Doctor por la ANECA, su trayectoria integra la dirección de tecnología y marketing (CTO/CMO) en diversas empresas del sector editorial y digital. Es experto en Inteligencia Artificial Generativa (IAG), gestión de sistemas multimedia híbridos y herramientas digitales multimedia, con más de 25 años de experiencia como editor de prensa especializada.

juanpmat@ucm.es

Índice H: 6

Orcid ID: <https://orcid.org/0000-0002-8449-0072>

Scopus ID: <https://www.scopus.com/authid/detail.uri?authorId=57222579035>

ResearchGate: <https://www.researchgate.net/profile/Juan-Abarca-4>

Academia.edu: <https://ucm.academia.edu/JuanPabloMateosAbarca>

Google Scholar: <https://scholar.google.com/citations?user=POOcP9wAAAAJ>

Serafín Barros Garbín

Universidad Complutense de Madrid, España.

Doctor Cum Laude en Periodismo por la Universidad Complutense de Madrid, donde obtuvo el Premio Extraordinario de Doctorado. Cuenta con más de 20 años de experiencia en el sector audiovisual, en el que ha desempeñado diversas funciones en televisiones públicas. Actualmente es profesor en el Departamento de Periodismo y Nuevos Medios de la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid e integrante del grupo de investigación Observatorio de la Calidad de la Información en Televisión (OCITV).

sbarros@ucm.es

Índice H:1

Orcid ID: <https://orcid.org/0000-0002-3499-7385>

Scopus ID: <https://www.scopus.com/authid/detail.uri?authorId=59949553500>

ResearchGate: <https://www.researchgate.net/profile/Serafin-Barros>

Academia.edu: <https://ucm.academia.edu/SERAFINBARROSGARBIN>

Google Scholar: https://scholar.google.com/citations?user=_PDnN-UAAAAJ



Revista de Ciencias de la Comunicación e Información

ISSN: 2695-5016

ARTÍCULOS RELACIONADOS: (RCCI)

- Bedoya Sánchez, O. M., Pérez García, S. M., Osorio Oviedo, H. L. y Guzmán Pacheco, J. F. (2025). Inteligencia artificial y toma de decisiones en Gestión empresarial; una revisión bibliométrica de la última década. *European Public & Social Innovation Review*, 11, 1-16. <https://doi.org/10.31637/ep-sir-2026-1630>
- Braza Delgado, R. (2026). Inteligencia artificial y publicidad digital: discursos persuasivos y ciudadanía en la investigación científica. *Revista De Ciencias De La Comunicación E Información*, 31, 1-28. <https://doi.org/10.35742/rcci.2026.31.e351>
- Guerschberg, L. (2025). Impacto de la soberanía digital en poblaciones vulnerables: El rol del software libre en educación para cerrar la brecha digital. *Sapiens Discoveries International Journal (SDIJ)*, 3(1), 1. <https://dial-net.unirioja.es/servlet/articulo?codigo=10153682>
- Jacovkis, J. y Parcerisa, L. (2026). Plataformas, datificación y nueva gobernanza de la educación: Un marco analítico sobre la soberanía digital. *Revista Española de Educación Comparada*, 49, 536-554. <https://doi.org/10.5944/reec.49.2026.45462>
- Paz-Rebollo, M. A., Bonaut-Iriarte, J. y Vicent-Ibáñez, M. (2025). Deepfake Parodies, Technological Spectacle, and Digital Catharsis: The Case of Iberian Son. VISUAL REVIEW. *International Visual Culture Review Revista Internacional De Cultura Visual*, 17(7), 189-204. <https://doi.org/10.62161/revvisual.v17.5902>