Revista de Ciencias de la Comunicación e Información. 2026. Vol. 31, 1-25
ISSN 2695-5016

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

Juan Pablo Mateos Abarca: Complutense University of Madrid. Spain.

Serafín Barros Garbín: Complutense University of Madrid. Spain.

Cómo citar el artículo:
Mateos Abarca, Juan Pablo. y Barros Garbín, Serafín. (2026). Digital iberity and technopolitics: Data sovereignty, generative artificial intelligence and cybersecurity in the Ibero-American space. *Revista de Ciencias de la Comunicación e Información*, 31, 1-25. https://doi.org/10.35742/rcci.2026.31.e357

ABSTRACT

Introduction: This article investigates the intersection of technopolitics, artificial intelligence (AI) and digital infrastructure under the Neo-Iberity paradigm. This study analyzes the ability of Ibero-speaking nations to establish strategic autonomy in the face of the transnational technology oligopolies that dominate the digital infrastructure of the 21st 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, specialized doctoral training and the production of indigenous linguistic corpora. **Discussion:** The findings propose regulatory harmonization based on the AESIA model and the strengthening of transatlantic cybersecurity as axes of democratic defense against hegemonic technological players. **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 colonized by processes of mass data extraction.

Keywords:

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

CC BY NC

Received: 14/03/2026 - Accepted: 18/05/2026 - Published: 27/05/2026

1. INTRODUCTION: THE GEOSTRATEGY OF THE NEO-IBERITY

Contemporary geopolitics is no longer organized exclusively around natural resources or industrial capacity, but rather around invisible infrastructures: hyperscalable data centers, submarine fiber optic networks, advanced semiconductors, and cloud architectures. Sovereignty, consequently, is redefined as the capacity to make decisions about information flows and algorithmic systems (Castells, 2009).

In this scenario, the Ibero-speaking world —comprising more than six hundred million Spanish and Portuguese speakers across Europe and the Americas— occupies an ambivalent position. On the one hand, it constitutes one of the world's largest linguistic communities, with the potential to generate economies of scale in scientific production, the digital market, and the development of multilingual foundational models.

On the other hand, it presents a marked infrastructural fragmentation and technological dependence with respect to hegemonic poles located mainly in the United States and East Asia.

Contemporary digital transformation has transcended mere technical transition to become an ontological reconfiguration of state and social power. As Castells (2009) argues in the analysis of the power of communication, in the network society, the exercise of power resides in the ability to program the algorithms and protocols that mediate social reality. In this context, the Ibero-American space —a community comprised of more than six hundred million people with a shared linguistic heritage— faces the challenge of not being relegated to a mere periphery of mass data consumption.

The emergence of Generative Artificial Intelligence (GAI) poses an existential challenge: the possibility of irreversible cognitive subordination to foreign models of thought, which calls for rethinking nations not only as territorial political units, but as imagined communities (Anderson, 2006) that must defend their identity and values in cyberspace. This reconfiguration implies that sovereignty is no longer exercised solely over the land, but over the flow of bits. Overcoming technological solutionism (Morozov, 2015) requires recognizing that behind every interface there is a power architecture that benefits its original creators, often at the expense of the linguistic and cultural diversity of the Global South.

The Neo-Iberity emerges as a project of resistance against the cultural homogenization imposed by large platforms. According to Castells and Himanen (2014), the reconstruction of the welfare state in the information age depends on the capacity of states to intervene in the information economy without stifling innovation. For Ibero-America, this means creating an ecosystem where AI is not a tool of external control, but rather an engine of its own development.

The research problem that underpins this work can be formulated as follows: Is it possible to transform the Ibero-speaking community into a technopolitical architecture capable of sustaining digital sovereignty within the global ecosystem of generative artificial intelligence? The central hypothesis argues that Neo-Iberity can operate as a viable strategic category provided that a shared supercomputing infrastructure is consolidated, advanced human capital training is coordinated, and regulatory frameworks are harmonized operationally rather than merely declaratively.

2. THEORETICAL FRAMEWORK: FROM PLATFORM CAPITALISM TO DATA COLONIALISM

The transition to a sovereign digital society requires a robust infrastructure, language models that respect linguistic diversity, and an ethical framework that places the human being at the center of algorithmic development.

The relevance of this study lies in the need to document how the Ibero-speaking world can formulate its own response to the "platformization" of social life and dependence on external infrastructures. In this sense, technopolitics emerges as the discipline capable of unraveling how large corporations and telecommunications define the course of nations, affecting the autonomy of citizens and the integrity of Ibero-speaking democracies.

Technopolitics has evolved from a marginal category into a central theoretical and methodological tradition in Ibero-America, particularly for the study of socio-digital protests and the formation of social movements on the Internet.

The concept encompasses both the capacity of connected crowds to contest the meaning of politics through technological appropriation, and the dimension of algorithmic governance and behavioral control through digital platforms. The debate on digital sovereignty in Latin America and Spain differs from the perspective of the Global North: while in Europe the discourse focuses on the control of infrastructure against external providers, in the Global South digital sovereignty is closely linked to resistance against digital colonialism and data extractivism.

Technopolitics is presented as a functional category that seeks cultural, scientific, and technological convergence between Spanish- and Portuguese-speaking nations to reconfigure power relations in the digital environment. The concept of technopolitics refers to the interrelation between technology and power in contexts of structural transformation.

Castells (2009) described the emergence of the network society as a reorganization of power into strategic information nodes. However, the current phase of generative artificial intelligence intensifies this logic: the nodes not only distribute information but also produce synthetic knowledge at scale. The emergence of the Neo-Iberity as a space of cultural, scientific, and technological convergence between Spanish- and Portuguese-speaking nations poses a profound reconfiguration of power relations in the contemporary digital environment.

Floridi (2014) argued that the fourth technological revolution redefines human agency in informational environments, while international frameworks such as the OECD Principles (About the OECD AI Principles, n.d.) and the UNESCO Recommendation (UNESCO, 2021) have promoted human-centered AI. However, digital sovereignty cannot be reduced to ethical regulation: it requires the material capacity for implementation. Without its own infrastructure, regulation depends on external technical architectures, which limits its effectiveness.

From a communication perspective, language acts as a strategic asset in training AI models and in the circulation of knowledge. The lack of large language models trained primarily in Spanish and Portuguese reinforces cognitive dependencies on English-

speaking ecosystems. The creation of structured, interoperable, and ethically governed corpora therefore becomes a central element of Iberian digital sovereignty.

The concept of the Neo-Iberity or the Digital Iberity is not merely a label, but is defined as a project of resistance and strategic autonomy for Iberian nations in the face of technological oligopolies. This identity is linked to the creation of shared digital public goods, such as supercomputing infrastructures and distinct linguistic models (Spanish and Portuguese), to prevent the "colonization" of cultural identity through massive data extraction processes.

Data sovereignty is presented not only as a regulatory framework, but also as an essential infrastructural necessity in the contemporary digital age. Resistance to data extractivism is understood as an explicit response to digital colonialism and the extractive logic underlying the mass capture of information.

This process is conceived as a form of appropriation of life itself, geared toward capitalist accumulation. Therefore, sovereign control over data emerges as a strategy for confronting dynamics of exploitation. In terms of its materiality, the discourse on data sovereignty is intertwined with the concept of technological and infrastructural sovereignty.

In this regard, the importance of controlling information flows through strategic physical infrastructures, such as submarine cables (e.g., EllaLink, https://ella.link) and sovereign clouds, is emphasized to ensure that data is managed in accordance with the General Data Protection Regulation (RGPD[1], 2016) without being subject to external jurisdictions that could jeopardize compliance.

Furthermore, a specific technical proposal is put forward: to develop governance frameworks based on open data principles, accompanied by robust local mechanisms for privacy protection. This approach seeks to balance the power imbalances generated by large technology corporations, known as Big Tech, by promoting a more equitable and just model for the management and valuation of information.

The convergence of media politics, generative artificial intelligence (AI), and cybersecurity constitutes one of the main contemporary challenges to digital sovereignty and democratic governance in the Ibero-American world. In the context of digitized societies, power is no longer exercised solely through traditional political institutions or conventional media structures, but also through the control of algorithmic systems capable of organizing the flow of information, shaping public opinion, and conditioning the dynamics of social interaction. In this sense, Castells (2009) argues that power in the network society resides in the ability to program communication networks and the algorithms that determine the perception of social reality, making digital platforms and their technological infrastructures key players in contemporary political and cultural disputes.

This perspective becomes especially relevant when analyzing the impact of generative AI on symbolic production and media ecosystems. Content automation, algorithmic personalization, and the capacity to generate synthetic discourses on a large scale have profoundly transformed the relationships between citizens, information, and power.

[1] GDPR, in English

Gillespie (2018, p. 13) notes that large digital platforms act as true "guardians of the internet," establishing moderation and visibility criteria that, far from being neutral, reproduce cultural, linguistic, and geopolitical biases. Consequently, algorithms not only organize access to information but also define the boundaries of what is visible and legitimate within the Ibero-American digital space, directly affecting cultural diversity and communicative pluralism.

In this context, cybersecurity ceases to be a merely technical issue and becomes an essential component of democratic defense and digital sovereignty. The growing dependence on foreign technological infrastructure exposes Ibero-American states and institutions to hybrid threats, automated disinformation campaigns, attacks on critical infrastructure, and algorithmic manipulation processes capable of eroding public trust and institutional stability.

Cybersecurity should be conceived as a strategic public good aimed at guaranteeing the right to a safe digital life, as well as the protection of information systems and citizens' data against transnational surveillance and exploitation dynamics.

The problem intensifies when considering the increasing opacity of algorithmic systems. Pasquale (2015, p. 15) describes this phenomenon using the notion of the "black box society," characterized by the expansion of automated systems that operate without sufficient mechanisms for transparency, oversight, or accountability. Decision-making mediated by closed algorithms is progressively affecting fundamental areas of social life, including public communication, financial services, access to employment, public administration, and the judicial system.

In the Ibero-American context, this opacity can reproduce and amplify historical inequalities, particularly when predictive tools or automated evaluation systems incorporate structural biases that harm vulnerable communities and minority groups. Thus, algorithmic governance becomes a political and ethical problem of the first order, closely linked to the protection of civil rights and the preservation of democratic autonomy.

The relationship between media policy, generative AI, and cybersecurity thus acquires a structural and interdependent character. Without technological sovereignty based on independent infrastructure, autonomous computing capabilities, and data storage and processing systems under regional control, any attempt at ethical regulation of artificial intelligence is limited and insufficient.

In turn, without a robust cybersecurity framework, autonomy in data management and the protection of institutional systems are seriously compromised in the face of external corporate and geopolitical actors. Defending digital sovereignty therefore requires the simultaneous articulation of technological, regulatory, and communication policies capable of responding to new forms of algorithmic power.

In this context, the debate on data colonialism has emerged forcefully, understood as a new historical form of dispossession based on the massive extraction of personal and collective information. Mejías and Couldry (2019) argue that contemporary dynamics of data capture and exploitation reproduce neocolonial logics through which human experiences are transformed into economic resources susceptible to processing and commodification. The expansion of digital platforms and artificial intelligence systems

has consolidated an accumulation model based on the systematic appropriation of behavioral data, reinforcing relationships of technological dependence between the Global North and South.

This dynamic is closely linked to what Zuboff (2019, p. 8) calls "surveillance capitalism," an economic model based on the extraction, analysis, and commercialization of data intended to predict and influence human behavior. In the context of Neo-Iberity, this process takes on a particularly significant biopolitical dimension.

Drawing on Foucault's (2007) contributions, it can be argued that the algorithmic management of populations constitutes a new form of automated biopolitics, where control mechanisms no longer operate solely through traditional disciplinary institutions, but rather through invisible digital infrastructures that classify, prioritize, and condition social behaviors. Algorithms thus function as devices of social regulation capable of shaping public discourse, establishing hierarchies of visibility, and normalizing certain forms of political and cultural participation within the Ibero-American digital space.

The material dimension of this process is equally relevant. The global development of artificial intelligence depends largely on invisible forms of digital labor, as Scholz (2016) points out when analyzing the new forms of labor exploitation associated with technology platforms. In numerous Ibero-American countries, thousands of workers participate in data tagging, moderation, and training tasks that are fundamental to the functioning of AI systems, frequently under precarious conditions and without adequate labor protections. The extractivist digital economy reinforces an international division of labor in which the region provides data, a cheap labor force, and cognitive resources, while control over infrastructure, patents, and innovation capacity remains concentrated in large foreign technology corporations.

Consequently, building genuine digital sovereignty in the Ibero-speaking world cannot be limited solely to protecting privacy or technically regulating personal data. It is a profoundly political and strategic issue involving the capacity of Ibero-American societies to preserve their cultural, economic, and democratic autonomy in the face of new forms of global algorithmic power. The integration of media policies, algorithmic governance, and cybersecurity is therefore essential to guaranteeing technological self-determination and protecting fundamental rights in the era of generative artificial intelligence.

2.1. Platform Capitalism and Value Appropriation

The political economy of artificial intelligence is currently dominated by what Srnicek (2017) calls platform capitalism. These entities are not simply commercial intermediaries, but rather fundamental infrastructures that extract value from mediating every possible human interaction. This context profoundly alters the richness of networks (Benkler, 2007), where collaborative social production —which, in the early days of the web, promised a radical democratization of knowledge— ends up being co-opted by processes of extreme corporate centralization.

In the Ibero-speaking world, this leads to a systemic precarization of digital work: workers in the region often operate under conditions of invisible labor (Scholz, 2016), feeding global algorithms through data tagging and content moderation tasks lacking basic labor protections. To counteract this trend, the region must promote cooperative platforms that reinvest value in their own creators. Autonomy is not only technical but

also economic: without a business model that respects the ownership of data generated in Spanish and Portuguese, the region will remain an extractive territory for transnational digital capital.

2.2. Data Colonialism and Algorithmic Biopolitics

Mejías and Couldry's (2019) analysis of data colonialism reveals that information capture is not merely an aggressive commercial practice, but a form of appropriation of life itself for the purposes of capitalist accumulation. Colonization manifests itself in surveillance capitalism, where citizens' behavioral surplus is processed to predict, condition, and modify human behavior on a large scale. From a population control perspective, the technopolitics analyzed acts as a sophisticated form of government (Foucault, 2007), where black-box algorithms (Pasquale, 2015) manage essential public services without due transparency or accountability.

This phenomenon is exacerbated when one considers that the "black box society" (Pasquale, 2015, p. 15) conceals biases that disproportionately penalize Ibero-speaking citizens in areas such as credit and employment. A critical area of concern is the introduction of AI into judicial systems: Pasquale (2015) warns of the danger of privatizing justice through the use of unclear algorithms that issue sentences or assess the risk of recidivism.

In Latin America, where the gap in access to justice is profound, the unsupervised use of the aforementioned tools can exacerbate prejudice against minorities. The EU Artificial Intelligence Act (AI Act, 2024), requires that any high-risk AI system, such as those used in judicial enforcement, be explainable and include human oversight in its final decision-making phase.

The inclusion of artificial intelligence systems into the judicial sphere raises significant ethical, political, and legal challenges, especially in contexts characterized by structural inequalities and institutional fragility. The increasing use of opaque algorithms to issue judicial recommendations, assess recidivism risks, or assist in decision-making processes is a warning that could lead to a form of "automated justice" that progressively displaces human deliberation and weakens the fundamental principles of the rule of law.

Following Frank Pasquale's (2015) arguments, this research maintains that these "black box" systems operate through opaque mechanisms that make it difficult to understand the criteria used in decision-making, as well as to identify potential biases embedded in the algorithmic models. This lack of explainability and oversight increases the risk of indirect privatization of justice, insofar as functions traditionally linked to the public sphere become subject to technologies developed and managed by private corporations.

The problem takes on a particularly critical dimension in the Latin American context, where profound gaps in access to justice and high levels of social inequality persist. The text argues that the implementation of artificial intelligence tools without adequate control mechanisms can amplify historical biases related to class, gender, race, or ethnicity. Algorithms learn from historical data that reflects previous institutional and social practices; as a result, when such data contains discriminatory patterns, automated systems tend to reproduce and legitimize those same inequalities under a guise of technical neutrality.

In addition, there is persistent gender and racial inequality in the fields of technology education and artificial intelligence development, which limits the diversity of critical perspectives during the design and training of the algorithmic systems themselves.

Considering all of this, regulating unclear algorithms must be a strategic priority for Ibero-American countries. The absence of mechanisms for transparency, auditing, and democratic control could transform technical opacity into a new instrument of social exclusion, deepening existing inequalities instead of correcting them. In this framework, the issue is not limited to simply improving administrative efficiency through digital technologies, but also involves ensuring that technological innovation is compatible with the principles of equality, due process, and the protection of fundamental rights.

The creation of specialized bodies for algorithmic auditing and technological governance would strengthen public oversight mechanisms for technologies with high social impact, contributing to the consolidation of digital sovereignty based on transparency, accountability, and the protection of citizens' rights. Without the necessary safeguards, judicial automation risks transforming technological opacity into a structural tool of discrimination and exclusion, further weakening the democratic legitimacy of judicial institutions and exacerbating existing inequalities in the region.

Linguistic sovereignty is not a nationalist whim, but a necessity for preserving original thought. Gillespie (2018) warns that moderation algorithms often fail to understand the nuances of regional Spanish or Brazilian Portuguese, unfairly censoring or allowing hate speech due to contextual ignorance. By developing its own models on local supercomputers, Ibero-America can ensure that its intangible heritage is not filtered by the criteria of companies whose primary objective is profit. As UNESCO (2021) indicates, AI must promote cultural diversity, and this is only possible if the tools are built from within the language itself and with the active participation of its speakers.

This assertion is based on the convergence of the structural fragility of Ibero-American judicial systems and the increasing incorporation of unclear algorithmic systems into public decision-making processes. The article argues that the expansion of artificial intelligence tools applied to the judicial sphere introduces significant risks to the effective guarantee of fundamental rights, especially in contexts characterized by historical inequalities and institutional limitations. Within this framework, the automation of judicial decisions cannot be interpreted solely as a technological advancement aimed at administrative efficiency, but also as a political and ethical phenomenon that directly affects the democratic legitimacy of justice.

In this context, the European Union's AI Act (2024) is identified as one of the main regulatory frameworks for addressing the challenges arising from algorithmic governance. European legislation classifies artificial intelligence systems applied to the judicial field as "high-risk" technologies, recognizing the potential impact that the used tools can have on fundamental rights and procedural safeguards.

Based on this hierarchy, the AI Act (2024) establishes strict requirements related to the explainability, traceability, and human oversight of automated systems. The text particularly emphasizes the requirement that final decisions remain under meaningful human control, preventing algorithms from acting as absolute substitutes for judicial deliberation.

This research argues that regulating opaque algorithmic systems should be a strategic priority for Ibero-American states. The absence of robust mechanisms for transparency, auditing, and accountability could lead to a deepening of existing social inequalities, consolidating technologically mediated forms of exclusion and discrimination.

Likewise, the issue is not limited solely to efficiency or innovation in the administration of justice, but also involves the defense of fundamental democratic principles such as equality before the law, due process, and equitable access to justice. The inclusion of artificial intelligence in the judicial sphere therefore requires ethical and regulatory governance capable of ensuring that the technology functions as an instrument for institutional strengthening and not as a mechanism for perpetuating existing problems.

3. TECHNICAL ANALYSIS: INFRASTRUCTURE AS A DESTINATION

3.1. Significance and Cyber Power

It is essential to understand that digital sovereignty is not a theoretical concept: it physically travels through fiber optic cables buried on the ocean floor. Control and ownership of these routes constitute a critical component of cyber power (Nye, 2010) in the 21st century. For decades, the vast majority of data traffic between Latin America and the Iberian Peninsula depended on North American nodes, subjecting the information to their legal and technical jurisdiction. Direct connectivity projects, such as the EllaLink submarine cable, are milestones in strategic autonomy that allow scientific cooperation in the region (OEI, 2022) to be based on sovereign technical implementation.

The Ibero-American General Secretariat (SEGIB, 2024) emphasizes that infrastructural sovereignty is the foundation of political sovereignty. By avoiding transit through third countries, it ensures that the General Data Protection Regulation (RGPD, 2016) is fully implemented along the Ibero-speaking Atlantic corridor. Achieving physical independence reduces latency and enables critical AI applications in telemedicine and industry that were previously unfeasible due to dependence on distant nodes controlled by foreign powers.

3.2. Supercomputing and Proprietary Linguistic Models

Training foundational language models requires computing power that must be considered a top-priority strategic resource. Initiatives to promote science and digital transformation in the region (OEI, 2022) seek to break the Anglo-centric hegemony by creating an AI infrastructure trained natively in Spanish and Portuguese. This is vital to prevent the guardians of the internet (Gillespie, 2018) —the large platforms that moderate content and define relevance— from imposing cultural, moral, and linguistic biases that erode the epistemic diversity of the Ibero-speaking world.

Spain has launched the ALIA Project, a public AI infrastructure aimed at developing foundational language models in Spanish and its co-official languages. ALIA is funded by the European Union's Recovery, Transformation and Resilience Facility and coordinated by the Barcelona Supercomputing Center (https://www.bsc.es/es), with the goal of providing companies, public administrations, and universities with open and transparent AI tools that do not require transferring sensitive data to third-party private clouds.

The training of the ALIA family models is carried out on the MareNostrum 5 supercomputer, whose computing power represents the backbone of this strategy, allowing the processing of billions of words so that the models originally operate in Spanish.

In Portugal, the National Artificial Intelligence Agenda (ANIA) 2026-2030 follows a similar path: the country aims to increase its computing capacity from 60 MW in 2025 to between 700 and 1,000 MW in 2030 (ANIA, 2026). The goal is to position the country as an AI "Gigafactory" in the European context, with an investment of over €400 million aimed at reducing external dependence and fostering an ecosystem of competitive startups and SMEs (Agenda Portugal AI 2030[2], 2026).

Latam GPT project (https://www.latamgpt.org) and CENIA (https://cenia.cl) — conceived as a public and open model available from June 2025— demonstrates that the Ibero-speaking space can generate its own innovation tools by leveraging local talent and sovereign data, without commercial dependencies on third parties.

4. OBJECTIVES

Based on the previous analysis, the following research objectives are proposed:

• O1. To determine if the Iberity can be transformed into a functional technopolitical category through the articulation of infrastructural cooperation and regulatory harmonization.

• O2. To evaluate to what extent coordinated scientific production in Spanish and Portuguese increases strategic autonomy in generative AI.

• O3. To examine how regulatory convergence in data protection strengthens regional digital sovereignty.

• O4. To analyze cybersecurity cooperation as a mechanism to reduce systemic vulnerabilities arising from external technological dependence.

5. METHODOLOGY

This study employs a qualitative, exploratory, and descriptive approach, grounded in a systematic literature review and a comparative analysis of digital public policies in the Ibero-American region. Following the ethical protocols of academic transparency required in current scientific communication, it is expressly stated that, for linguistic optimization, style correction, and the technical structuring of certain sections of this manuscript, Generative Artificial Intelligence tools were used under constant human supervision.

However, it is guaranteed that the intellectual authorship, the critical analysis of the data, the interpretation of the results and the conclusions belong entirely to the signatories of the study.

[2] The 2030 Portugal Agenda on AI

5.1. Operating Protocol and Selection Criteria

The data collection was structured according to a rigorous operational protocol implemented between December 2025 and February 2026. The search for scientific and technical literature was centralized in the Scopus, Web of Science (WoS), and Google Scholar databases, as well as the Dialnet repository for the Spanish-speaking world. Boolean search strings were used, combining keywords such as: ("Soberanía de datos" OR "Data Sovereignty") AND ("Inteligencia Artificial" OR "Generative AI") AND ("Iberidad" OR "Iberoamérica") AND ("Ciberseguridad" OR " Cybersecurity").

The inclusion criteria established for selecting the bibliographic corpus were: a) articles from indexed journals and technical manuals published in the last decade (2015-2025); b) reports and official documents from international organizations, with special attention to the Latin American Artificial Intelligence Index (ILIA); and c) current regulatory frameworks. As an exclusion criterion, conference papers without peer review or opinion pieces without verifiable empirical support were discarded. After an initial screening of 92 identified records, the final number of primary and secondary sources supporting the analysis totaled 45 documents.

5.2. Axes of the Analysis and Procedure

The analysis was structured around four complementary methodological axes that ensure the triangulation of information and the validity of the results:

1. Comparative literature review of national artificial intelligence strategies in Spain, Portugal and various Latin American countries, as well as multilateral reports on digital infrastructure and advanced training.

2. Normative analysis of regulatory frameworks linked to data protection and algorithmic governance, with special attention to the Santiago Declaration (Minciencia, 2023), the European AI Regulation (AI Act, 2024) and the General Data Protection Regulation (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo [RGPD][3], 2016).

3. Interdisciplinary literature review in the fields of communication, digital law and technological governance studies, aimed at identifying the main axes of theoretical debate.

4. Critical-discursive analysis of quantitative indicators from the Latin American Artificial Intelligence Index 2025 (ILIA, 2025), used as a proxy to evaluate the regional technological gap.

5.3. Rationale for the Sample and Documentary Corpus

The sample selection was based on a criterion of strategic representativeness under the paradigm of the "Digital Iberity," prioritizing those nations that lead in ecosystem maturity and logical infrastructure in the region. Under these parameters, the corpus of primary institutional documents analyzed was as follows:

1. Iberian Axis (Europe): The governance architecture of the Iberian Peninsula was analyzed as a bridge to European regulations (AI Act, 2024). The specific documents

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council [GDPR]

examined were Spain's National Artificial Intelligence Strategy (Plan de Recuperación, Transformación y Resiliencia[4], 2023) and the statutes establishing its supervisory agency, as well as the National Artificial Intelligence Strategy (AI Portugal 2030, 2019).

2. Latin American Axis: As a representative sample of the region, the master plans of the three countries with the greatest ecosystem maturity according to the ILIA were analyzed:

• Brazil: Brazilian Artificial Intelligence Strategy (Ministério da Ciência, Tecnologia e Inovação[5], 2026).

• Chile: National Artificial Intelligence Policy and its action plan.

• Colombia: National Policy for Digital Transformation and Artificial Intelligence (CONPES, 2025).

This joint analysis allows for the precise verification of the figures, forecasts, and concrete data on data sovereignty and infrastructure included in the text, providing a verifiable empirical basis for the proposal of strategic technological autonomy.

6. RESULTS

The results are organized around the study's three analytical dimensions: technological infrastructure, specialized human capital, and regulatory architecture. The analysis confirms that Ibero-speaking digital sovereignty requires overcoming three structural obstacles: insufficient high-performance infrastructure, scientific fragmentation, and limited regulatory coordination. However, it also reveals strategic opportunities stemming from the expanded linguistic community and legal convergence.

6.1. Structural Gaps Identified by the ILIA 2025

Despite advances in infrastructure, the Neo-Iberity faces a “structural trap” characterized by the persistence of deep technological gaps. The Latin American Artificial Intelligence Index 2025 (ILIA, 2025) reveals that the region is experiencing record growth in digital investment, but this does not necessarily means a reduction in inequality.

The digital divide in Latin America is multidimensional and manifests itself at four main levels:

(1) physical and geographical barriers, given that the lack of fixed broadband infrastructure in rural areas limits equitable access to emerging technologies;

(2) specialization gap, manifested in a "funnel" phenomenon where there is high general AI literacy but a critical shortage of specialized talent —in 11 of the 19 countries analyzed by the ILIA there are no PhD programs in AI—;

(3) gender and racial inequality in technological training, which excludes women and ethnic minorities, limiting the diversity of perspectives in algorithmic development; and

[4] Recovery, Transformation and Resilience Plan
[5] Ministry of Science, Technology and Innovation

(4) extreme concentration of access to computing, with Brazil monopolizing most of the processing capacity in all of Latin America, which generates severe asymmetries within the region itself.

Tabla 1. *Correlation Between ILIA 2025 Gaps and Neo-Iberity Proposals.*

ILIA 2025 Dimension	Identified Gap in the Region	Proposal for Strategic Autonomy
Infrastructure	Deficit in local supercomputing nodes	Investment in sovereign data centers and direct cables.
Data and algorithms	Anglocentric bias in commercial generative artificial intelligence models	Development of foundational models trained in Spanish and Portuguese.
Governance	Regulatory fragmentation between nations	Regulatory harmonization based on the model of the **Spanish Agency for Supervision of Artificial Intelligence** and the **Artificial Intelligence Act.**
Cybersecurity	Vulnerability to external hybrid threats	Shared transatlantic cyber defense protocols
Human capital	Shortage of doctors in artificial intelligence in most countries	Regional doctoral programs and scientific mobility

Fuente: Elaborated by the authors based on data from ILIA (2025).

6.2. Emerging Institutional Capacities

In light of this diagnosis, the documentary analysis reveals the emergence of relevant institutional capabilities. The creation of the Spanish Agency for the Supervision of AI (AESIA), as part of the Artificial Intelligence Act (EU, 2024), proposes a proactive approach using regulatory sandboxes that allow experimentation in controlled environments. This model ensures that technological systems respect the OECD's ethical principles from their design stage (About the OECD AI Principles, n.d.) and UNESCO's (2021) recommendations on AI ethics, while facilitating the export of a trust framework that could be adopted by Ibero-American countries.

The Santiago Declaration (Minciencia, 2023), signed by 20 countries in the region with the support of UNESCO and CAF, establishes principles of transparency, inclusion, and sustainability for the development of AI, with special emphasis on multi-stakeholder governance and the protection of neurorights. Spain has reinforced its ethical vision with the launch of a voluntary Ethical AI Seal for companies, which guarantees that algorithms are reliably applied and without discrimination.

An analysis of social movements in Latin America —such as Atalaya Sur in Argentina and Sursiendo in Mexico— also demonstrates that digital sovereignty is built not only from the top down, through public policies, but also through the popular appropriation of

technology and the creation of autonomous networks that challenge the logic of digital capital.

6.3. Dimensions of Ibero-American Digital Sovereignty

In terms of scientific contribution, the study provides an articulated vision that integrates technological, organizational and educational dimensions, overcoming fragmented approaches.

It also raises the need for future longitudinal research to assess the real impact of artificial intelligence on information quality, content diversity, and the economic sustainability of media outlets. The analysis confirms that Ibero-speaking digital sovereignty requires overcoming three structural obstacles: insufficient high-performance infrastructure, scientific fragmentation, and limited regulatory coordination. However, it also reveals strategic opportunities arising from the expanded linguistic community and legal convergence.

The Neo-Iberity can be conceptualized as an infrastructural project aimed at creating regional supercomputing consortia, developing foundational models in Spanish and Portuguese, and establishing interoperable regulatory frameworks. Cooperation does not imply technological isolation, but rather the strengthening of collective bargaining power vis-à-vis global hegemonic players. Digital sovereignty should be understood as relational autonomy, not technological autarky.

Tabla 2. *Dimensions of Digital Sovereignty and Technopolitical Challenges in the Ibero-speaking Space.*

Dimension	Challenge in the Ibero-Speaking Space	Technopolitical Proposal
Infrastructure sovereignty	Dependence on cloud computing services hosted outside the national territory.	Development of sovereign clouds and strengthening of regional supercomputing infrastructures.
Data sovereignty	Extraction by large technology corporations (Big Tech).	Implementation of open data governance frameworks and local privacy protection mechanisms.
Linguistic sovereignty	Scarcity of training data in Spanish and Portuguese in artificial intelligence systems.	**ALIA** project in Spain and **ANIA** project in Portugal.
Technological sovereignty	Dependence on proprietary software and hardware developed in other countries.	Promotion of free software, open hardware and models of technological cooperation.

Fuente: Elaborated by the authors.

The relationship between digital sovereignty and technopolitical challenges is essential for understanding contemporary transformations of power in digital society. In the 21st century, sovereignty can no longer be limited to the traditional territorial control exercised by states; it must be redefined as the capacity for decision-making,

management, and autonomy over information flows, technological infrastructures, and algorithmic systems that organize social, economic, and political life. Within this context, technopolitics emerges as a field of analysis focused on examining how power is exercised through the programming of algorithms, digital protocols, and communication infrastructures that mediate the construction of social reality and shape processes of collective interaction.

In this context, digital sovereignty has a material dimension inseparable from the technological infrastructures that underpin the global flow of data. Dependence on fiber optic networks, data centers, and platforms controlled by external players places Ibero-American countries in a position of strategic vulnerability vis-à-vis foreign jurisdictions and large technology corporations.

Digital infrastructure, therefore, constitutes a concrete expression of contemporary power, insofar as it determines who controls information flows, storage capacity, and data processing. Given the current framework, strengthening sovereign clouds, regional supercomputing centers, and autonomous connectivity systems emerges as a strategy aimed at transforming technological dependence into strategic autonomy. Building independent digital infrastructures responds not only to technical or economic objectives but also to the need to preserve political decision-making power over the region's digital ecosystems.

Complementarily, data sovereignty emerges as a critical response to contemporary dynamics of digital colonialism. The massive extraction of personal and behavioral data by large technology corporations reproduces forms of appropriation that transform human experience into an exploitable resource for capital accumulation. In this context, the dynamics associated with what Shoshana Zuboff (2019) conceptualizes as "surveillance capitalism" demonstrate how user-generated information is used to predict, influence, and modify social behaviors on a large scale.

Contemporary technopolitics faces the challenge of preventing Ibero-American societies from being reduced to peripheral territories for information extraction at the service of transnational platforms. As an alternative, the need arises to develop open, transparent, and democratic data governance frameworks capable of guaranteeing privacy protection, citizen autonomy, and sovereign control over the region's information resources.

Another essential dimension of digital sovereignty relates to the preservation of linguistic diversity and epistemological autonomy. Dominant commercial artificial intelligence frequently reproduces Anglocentric biases that limit the adequate representation of the cultural, semantic, and contextual nuances inherent in Spanish and Portuguese in their multiple regional variants, with the consequent risk of increasing cognitive subordination to models of thought developed from cultural perspectives foreign to the Ibero-American reality.

In this sense, the technopolitical challenge lies not only in translating content or adapting existing tools, but also in developing original foundational models capable of natively incorporating the linguistic and cultural particularities of the Ibero-speaking world. Initiatives such as ALIA and ANIA represent significant progress toward building autonomous artificial intelligence capabilities, aimed at preserving linguistic heritage and preventing the cultural criteria of foreign platforms from defining the frameworks for knowledge production and dissemination.

6.4. Cybersecurity as a Defensive Dimension of Sovereignty

The expansion of digital infrastructure increases the cyber attack surface, making cybersecurity a central element of contemporary technopolitics. Governments in Latin America have taken significant steps toward digitalization, but many of their public systems remain vulnerable due to fragmented architectures or dependence on foreign cloud providers.

The threat landscape for the 2025-2026 period is characterized by more sophisticated attacks, including Ransomware-as-a-Service (RaaS), which makes it easier for criminal actors to launch complex, low-cost attacks targeting critical sectors such as health and energy; quadruple extortion, where attackers encrypt data, steal confidential information, threaten to publish it, and target the victim's business partners; and geopolitical surveillance, where the use of foreign surveillance technologies in smart city projects can compromise national security by transferring patterns of citizen behavior to external operators (Morales Ramirez, 2025).

Sovereign cybersecurity requires control over strategic digital assets. This implies not only the implementation of technical tools but also compliance with regulatory standards such as the NIS2 Directive in Europe or the National Security Framework in Spain (Heredero del Campo, 2023). Adopting a Zero Trust Security model is essential to protect terminals and servers outside the traditional secure perimeter (Gil Villa et al., 2025). The use of products qualified by national agencies —such as the CCN in Spain— ensures that the defense of critical infrastructure does not depend on technologies with potential vulnerabilities of geopolitical origin.

Digital sovereignty in the Iberian- world should not be interpreted as a strategy of technological isolation or autarkic retreat, but rather as a form of “relational autonomy” aimed at strengthening collective bargaining power against large global technology oligopolies. Digital sovereignty implies building shared capabilities that allow Ibero-American countries to reduce structural dependencies, protect their critical infrastructure, and develop technological models aligned with their cultural, linguistic, and political realities. This approach requires the integrated articulation of diverse strategic dimensions that transcend the fragmented approaches traditionally associated with technology governance.

First, infrastructure sovereignty is an essential component of what Joseph Nye (2010) calls cyber power, understood as the capacity to influence and exert power through control of digital networks and communication infrastructures. In the contemporary context, digital sovereignty depends largely on physical control of the network, including submarine cables, data centers, storage systems, and advanced computing capabilities. Strategic infrastructures like EllaLink represent key elements for reducing technological dependence on foreign nodes and strengthening regional autonomy in the flow of information.

In this sense, the strengthening of sovereign clouds, regional supercomputing centers and proprietary data processing capabilities is essential to ensure that regulatory standards such as the General Data Protection Regulation can be effectively applied throughout the entire information circulation chain, minimizing external interference and geopolitical vulnerabilities (Cordova Urbina et al., 2025).

Secondly, data sovereignty is presented as a critical response to the phenomenon of digital colonialism. Following the arguments of Ulises Mejías and Nick Couldry (2019), the massive extraction of data constitutes a new form of systematic appropriation of human experience, aimed at fueling the accumulation dynamics characteristic of contemporary digital capitalism. This logic is closely linked to what Shoshana Zuboff (2019, p. 8) conceptualizes as "surveillance capitalism," an economic model based on the large-scale capture, processing, and monetization of behavioral data.

In response to the extractivist dynamic, the Ibero-American technopolitical proposal demands the establishment of open, transparent and democratic data governance frameworks, capable of guaranteeing the protection of privacy and preventing the region from continuing to function as a peripheral territory of information extraction at the service of transnational technological capital.

A third dimension corresponds to linguistic sovereignty and epistemological autonomy. Language constitutes a strategic infrastructure for the preservation of cultural diversity and for the production of autonomous knowledge in digital environments. Tarleton Gillespie (2018, p. 13) warns that large technology platforms, in their capacity as "custodians of the internet," reproduce cultural and linguistic biases by failing to adequately understand the semantic, contextual, and sociocultural nuances of Spanish and Portuguese in their multiple regional variations.

This limitation not only affects the quality of automated systems but also fosters forms of cognitive subordination and epistemological dependence on artificial intelligence models trained from Anglocentric perspectives. In this context, initiatives such as ALIA and ANIA acquire strategic relevance by promoting the development of foundational models trained natively in Iberian languages, strengthening the regional capacity to generate technologies consistent with their cultural and communicative contexts.

Furthermore, technological sovereignty requires incorporating an ethical dimension aimed at ensuring that scientific and technical innovation adheres to democratic principles and social justice. Faced with the growing opacity characteristic of the so-called "black box society," conceptualized by Frank Pasquale (2015, p. 15), it is essential to promote mechanisms for algorithmic transparency, public auditing, and the development of free software. In this regard, the integration of the "ethics of invention," proposed by Sheila Jasanoff (2016), is a priority to ensure that technological innovation processes are not reduced to mere logics of technical efficiency or indiscriminate automation.

This concept stands in contrast to the "technological solutionism" criticized by Morozov (2015, p. 5), which posits that social problems can be solved solely through digital tools without considering their political, cultural, and ethical implications. On the contrary, Ibero-American technological sovereignty should be oriented toward innovation models committed to protecting human rights, promoting social equity, and fostering democratic participation (Marzani & Pires, 2024).

The analysis confirms that consolidating these dimensions faces significant structural obstacles, including insufficient high-performance computing infrastructure, external technological dependence, and existing scientific fragmentation among Ibero-American countries. In this context, the Neo-Iberity is projected as a strategic framework for transatlantic cooperation aimed at building shared technological capabilities and strengthening regional digital governance mechanisms.

Regulatory harmonization inspired by institutional models such as the Spanish Agency for the Supervision of Artificial Intelligence [AESIA], (n.d.), together with the creation of regional scientific and technological consortia, thus appears as a structuring strategy to defend democratic integrity and digital autonomy against the growing concentration of power exercised by hegemonic technological players on a global scale.

7. DISCUSSION

The analysis confirms that the Ibero-speaking digital sovereignty requires overcoming three structural obstacles: insufficient high-performance infrastructure, scientific fragmentation, and limited regulatory coordination. However, it also reveals strategic opportunities stemming from the expanded linguistic community and legal convergence among the Romano-Germanic countries of the Ibero-American region.

The Neo-Iberity can be conceptualized as an infrastructural project oriented toward three converging objectives: the creation of regional supercomputing consortia, the development of foundational models in Spanish and Portuguese, and the establishment of interoperable regulatory frameworks. Cooperation does not imply technological isolation, but rather the strengthening of collective negotiating power vis-à-vis global hegemonic actors. Digital sovereignty should therefore be understood as relational autonomy, not technological autarky.

Building a digital Neo-Iberian society requires a commitment to inalienable human values. The Santiago Declaration (Minciencia, 2023) and the AESIA represent institutional milestones that position the Ibero-speaking world as a benchmark for the responsible use of technology. Integrating the ethics of invention (Jasanoff, 2016) and regulating opaque algorithms (Pasquale, 2015) must be a priority to avoid an automated and unjust justice system. This vision moves the analysis away from techno-deterministic pessimism and places it at the forefront of an alternative digital modernity, where technology serves the community and not just the market.

In the area of human capital, there is growth in training programs in artificial intelligence, but with insufficient doctoral density in most Latin American countries and a significant emigration of talent towards global technological centers.

To close these gaps, international cooperation becomes essential. The EU-LAC Digital Alliance (https://www.eeas.europa.eu/eeas/alianza-digital-eu-lac_es) supported by the Global Gateway program (https://internationalpartnerships.ec.europa.eu/policies/global-gateway_es), seeks to mobilize substantial investments to strengthen education, research and secure connectivity systems on both sides of the Atlantic, with the aim of creating links that reduce the global investment gap without generating new dependencies.

Cybersecurity must be understood as the pillar that sustains the integrity of Neo- Iberia in the face of contemporary hybrid threats. Cybersecurity cooperation between Spain, Portugal, and Latin America (SEGIB, 2024) enables the exchange of real-time threat intelligence, mitigating the risks of external actors eroding trust in democratic institutions through automated disinformation. SEGIB (2024) emphasizes that cybersecurity is a public good that must be collectively protected: countries with fewer resources can benefit from the security umbrella of the most advanced nodes in the Ibero-speaking space, creating a resilience network that protects citizens' right to a secure digital life.

Cybersecurity must be understood as the structural element that sustains the integrity of the Neo-Iberian project in the face of increasing hybrid threats in the contemporary digital environment. Far from being limited to a merely technical or instrumental dimension, it is configured as a concrete expression of cyber power, insofar as contemporary digital sovereignty is articulated from the capacity to control, manage and protect digital assets, as well as the infrastructures and routes of information dissemination.

In this context, cooperation on cyber defense between Spain, Portugal and Latin America, promoted within the framework of the Ibero-American General Secretariat, not only facilitates the exchange of intelligence on threats in real time, but is also part of a broader dynamic of dispute over the control of communication flows and information environments that shape the public sphere.

Castells's (2009) argument is particularly relevant, given that contemporary power is based on the ability to program networks and algorithms that mediate the construction of social reality. Consequently, cybersecurity acquires a central political dimension by becoming a mechanism for containing automated disinformation, which not only distorts communication processes but can also erode institutional legitimacy and weaken citizens' trust in democratic systems. In this sense, protecting the digital ecosystem is configured as a form of resistance against the possibility that external actors may reconfigure collective perceptions and frameworks of social interpretation through algorithmic infrastructures.

Furthermore, from the perspective of data colonialism formulated by Mejías and Couldry (2019), cybersecurity can be interpreted as a strategic frontier against the dynamics of mass information extraction and systematic surveillance characteristic of contemporary digital capitalism. Within this framework, the proposal by the Ibero-American General Secretariat (SEGIB, 2024) to conceive of cybersecurity as a shared public good offers an institutional response to the structural asymmetries identified by the Latin American Artificial Intelligence Index, where the concentration of technological capabilities in a small number of players generates critical dependencies and systemic vulnerabilities across large areas of Ibero-America.

In this sense, the development of a regional “safety net” model makes it possible to reduce these gaps through solidarity-based cooperation among states with different levels of technological development, thereby strengthening collective resilience without resorting to a logic of external dependence or “solutionist” approaches.

Technological sovereignty in Ibero-America rests on three interconnected pillars: public and open infrastructures, conceived as public goods with participatory regional governance; open access to knowledge, guaranteed by systems such as Latindex, Redalyc or SciELO; and identity and language, through the training of AI models with data that reflect the problems, languages and knowledge of the region, avoiding epistemological subordination.

8. CONCLUSIONS

Technological sovereignty in Latin America is a material and political project that demands definitively overcoming the phase of passive and dependent consumption. As has been analyzed, control of the physical and logical infrastructure constitutes the first

essential step to prevent human life from being colonized by transnational capital through processes of massive data extraction (Mejías & Couldry, 2019).

Institutional leadership through supervisory agencies such as AESIA (n.d.), investment in science and higher education (OEI, 2022), and the development of one's own language models are the necessary tools to build an artificial intelligence that respects democratic values, privacy, and the immense linguistic richness of the Neo-Iberity.

• C1: Infrastructure and language as pillars of sovereignty. Control over physical (submarine cables) and logical infrastructure, coupled with the development of artificial intelligence models trained natively in Spanish and Portuguese, is the essential step to protect Ibero-American cultural identity and prevent cognitive colonization by external technological powers.

• C2: Sovereignty as relational autonomy. Digital sovereignty in the Ibero-speaking space should not seek technological autarky, but rather a "relational autonomy" that strengthens collective negotiating capacity through regulatory harmonization (following models such as AESIA), scientific cooperation, and the creation of regional supercomputing consortia.

• C3: Cybersecurity as a public good and democratic defense. Cybersecurity constitutes the essential defensive pillar of the Neo-Iberity, and must be managed as a shared public good that protects the integrity of democratic institutions and the privacy of citizens against hybrid threats and surveillance capitalism.

• C4: The need for structural reflection and linked sovereignty: The integration of artificial intelligence in the Ibero-American space must transcend mere technical innovation to be based on structural reflection that prioritizes transatlantic cybersecurity and epistemological autonomy.

Only through coordinated action can the Ibero-American space guarantee its autonomy. Integrating the ethics of invention (Jasanoff, 2016) and regulating opaque algorithms (Pasquale, 2015) must be a priority to avoid an automated and unjust justice system.

Language, traditionally conceived as a cultural element, thus becomes a strategic infrastructure: coordinated scientific production in Spanish and Portuguese can generate its own corpora for AI training, establish ethical frameworks adapted to specific sociocultural contexts, and reduce cultural biases present in models trained predominantly in English.

The challenges are immense —from transnational cybercrime to the skills gap— but the potential of Neo-Iberity to transform the global digital landscape is equally significant. Collaboration between Spain, Portugal, and Latin America, based on principles of integrity, equity, and diversity, is the only way to ensure that the fruits of the digital revolution benefit society as a whole. Digital Neo-Iberity is ultimately envisioned as a shared future where technology serves to unite cultures, protect rights, and foster the scientific development of Ibero-speaking peoples, safeguarding the Ibero-American infosphere from the pitfalls of global surveillance capitalism.

9. REFERENCES

About the OECD AI Principles (n.d.). *Shaping a human-centric approach to artificial intelligence.* https://www.oecd.org/en/topics/ai-principles.html

Agencia Española de Supervisión de Inteligencia Artificial. (n.d.). *Garantizando una IA ética y responsable*. Retrieved March 1, 2026. https://aesia.digital.gob.es/es

Agenda Portugal AI 2030. (2026, January 12). *Portugal aprova Agenda Nacional de Inteligência Artificial com investimento até 2030*. https://n9.cl/l6em5u

AI Act. (2024, June 13). *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. (2019, May 31). *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. (2026, January 8). *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.

Castells, M. (2009). *Communication power*. Oxford University Press.

Castells, M., & Himanen, P. (2014). *Reconstruir el estado del bienestar: La economía de la información y el estado red*. Alianza Editorial.

CONPES. (2025, February 28). *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., & 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. *Ingenieria Investiga*, 8, e1342. https://www.researchgate.net/publication/398100545_Zero_Trust_en_la_gestion_de_identidades_y_accesos_en_la_nube_Una_revision_de_modelos_ventajas_y_limitaciones

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., & 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.

Heredero del Campo, C. (2023). Nueva Directiva Europea NIS 2: Un avance en la regulación de la ciberseguridad para las actuales sociedades digitalizadas modernas. *Derecho Digital e Innovación. Digital Law and Innovation Review*, (16 (abril-junio)), 5. https://n9.cl/pzwkzh

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., & 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., & 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. (2023, October 24). *Chile liderará iniciativa de gobernanza de inteligencia artificial en América Latina.* https://acortar.link/ffhV5l

Ministério da Ciência, Tecnologia e Inovação. (2026, January 13). *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, May). *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. (2023, June 05). 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. (2024, July 31). *Resumen de 2023 en la Memoria Anual SEGIB*. Secretaría General Iberoamericana. https://acortar.link/hgEfAx

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

UNESCO. (2021, November 23). *Recommendation on the ethics of artificial intelligence. UNESCO Publishin*g. Retrieved on February 21, 2026, from 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.

Bedoya Sánchez, O. M., Pérez García, S. M., Osorio Oviedo, H. L., & 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/epsir-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://dialnet.unirioja.es/servlet/articulo?codigo=10153682

Jacovkis, J., & 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., & 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

AUTHORS' CONTRIBUTIONS, FUNDING AND ACKNOWLEDGMENTS

Conceptualization: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Methodology: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Software: Mateos Abarca, Juan Pablo. Validation: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Formal Analysis: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Data Curation: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Preparation of the Original Draft: Mateos Abarca, Juan Pablo. Drafting, Revision, and Editing: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín. Supervision: Barros Garbín, Serafín. Project Management: Mateos Abarca, Juan Pablo. All Authors Have Read and Accepted the Published Version of the Manuscript: Mateos Abarca, Juan Pablo and Barros Garbín, Serafín.

Funding: There has been no funding.

Acknowledgments: We thank the 1st Congress on Neo-Iberity CINIBER 2026 for their contributions to the completion of this work.

Conflict of interest: There is no conflict of interest.

AUTHORS

Juan Pablo Mateos Abarca
Complutense University of Madrid, Spain
Doctorate in Media Management from the Complutense University of Madrid (UCM), graduating with honors (Cum Laude). He is currently a Professor in the Department of Journalism and New Media at the Faculty of Information Sciences (UCM). Accredited as a Contracted Doctor by ANECA, his career includes positions as Chief Technology Officer (CTO) and Chief Marketing Officer (CMO) in various companies within the publishing and digital sectors. He is an expert in Generative Artificial Intelligence (GAI), hybrid multimedia systems management, and digital multimedia tools, with over 25 years of experience as an editor of specialized press.

H-index: 7
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
Complutense University of Madrid, Spain
Doctorate in Journalism (with highest honors) from the Complutense University of Madrid, where he received the Extraordinary Doctoral Prize. He has over 20 years of experience in the audiovisual sector, having held various positions in public television. He is currently a professor in the Department of Journalism and New Media at the Faculty of Information Sciences of the Complutense University of Madrid and a member of the research group Observatory of Information Quality in Television (OCITV).

H-index: 3
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

RELATED ARTICLES: (RCCI)

Bedoya Sánchez, O. M., Pérez García, S. M., Osorio Oviedo, H. L., & 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/epsir-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://dialnet.unirioja.es/servlet/articulo?codigo=10153682

Jacovkis, J., & 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., & 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