Revista científica en ciencias sociales, 7, e701202
Doi: 10.53732/rccsociales/e701202

Original Article/Artículo Original

The Exportation of the People's Republic of China's Surveillance Model: Artificial Intelligence, Social Credit, and its impact on Global Security and Human Rights

La exportación del modelo de vigilancia chino: Inteligencia Artificial, crédito social y el impacto en la seguridad global y los Derechos Humanos

Diego Sebastián Sánchez Chumpitaz[1*], Jorge Enrique Abarca Del Carpio1

[1]*Universidad San Ignacio de Loyola, School of Law, Department of International Relations. Lima, Peru.*

ABSTRACT

This study examined the consolidation and international expansion of the digital surveillance model promoted by the People's Republic of China (PRC), built on artificial intelligence (AI) and the Social Credit System (SCS). A mixed-methods approach combined documentary analysis of regulatory frameworks and technologies with quantitative modelling through the State Control Index (SCI), a linear mathematical tool. The SCI assessed the relationship between perceived security, technological deployment, and restrictions on fundamental rights across authoritarian and semi-authoritarian regimes. The findings revealed patterns of authoritarian diffusion via digital infrastructure, interstate agreements, and regulatory transfer. A steady expansion of algorithmic control was observed in fragile institutional contexts, particularly in Latin America, where the security-liberty balance has been historically unstable. In such settings, surveillance systems advanced without solid legal safeguards, reframing citizenship as an object of permanent monitoring and treating dissent as a statistical deviation. This trend undermines individual autonomy and weakens democratic stability.

Keywords: International security; human rights; artificial intelligence; surveillance; internet governance; data protection.

RESUMEN

Este estudio examinó la consolidación y expansión internacional del modelo de vigilancia digital promovido por la República Popular China (RPC), basado en inteligencia artificial (IA) y el Sistema de Crédito Social (SCS). Se aplicó un enfoque metodológico mixto que combinó análisis documental de marcos regulatorios y tecnologías con una modelación cuantitativa mediante el Índice de Control Estatal (ICE), herramienta matemática de formulación lineal. El ICE permitió evaluar la relación entre percepción de seguridad, despliegue tecnológico y restricciones a derechos fundamentales en regímenes autoritarios y semi-autoritarios. Los resultados identificaron patrones de difusión autoritaria a través de infraestructura digital, acuerdos interestatales y transferencia de normas. Se observó una expansión sostenida de dispositivos de control algorítmico en contextos institucionales frágiles, con especial énfasis en América Latina, donde el equilibrio entre seguridad y libertad ha sido históricamente inestable. La vigilancia digital se consolidó en ausencia de marcos regulatorios sólidos, transformando la ciudadanía en un objeto de monitoreo permanente y deslegitimando el disenso como desviación estadística. Este patrón compromete la autonomía individual y debilita los fundamentos democráticos.

Palabras clave: Seguridad internacional; derechos humanos; inteligencia artificial; vigilancia; gobernanza de internet; protección de datos.

How to cite/ Cómo citar:
Sánchez Chumpitaz, D. S., & Abarca Del Carpio, J. E. (2025). The Exportation of the People's Republic of China's Surveillance Model: Artificial Intelligence, Social Credit, and its Impact on Global Security and Human Rights. *Revista científica en ciencias sociales*, *7*, e701202. 10.53732/rccsociales/e701202

Managing Editor:
Chap Kau Kwan Chung
Universidad del Pacífico. Dirección de Investigación. Asunción, Paraguay
Email: wendy.kwan@upacifico.edu.py

Revisores

Myrna Ruiz Díaz
Universidad del Pacífico. Dirección de Investigación. Asunción, Paraguay
Email: myrna.ruizdiaz@upacifico.edu.py

Hernán Sutty
Universidad Americana. Facultad de Ciencias Económicas y Administrativas. Asunción, Paraguay
Email: her_su@hotmail.com

Reception date: 13/02/2025

Review date: 18/02/2025

Acceptance date: 10/03/2025

Corresponding authors:

Diego Sebastián Sánchez Chumpitaz
E-mail: diego.sanchezc@usil.pe

INTRODUCTION

This study examines the digital surveillance architecture promoted by the People's Republic of China (PRC), with particular focus on the Social Credit System (SCS) and its international projection as a replicable model of algorithmic governance. This state-controlled infrastructure, developed through artificial intelligence (AI), big data[1], facial recognition, and administrative automation, constitutes a citizen supervision regime without precedent in recent history (Creemers, 2018; Castellanos-Claramunt, 2023; Stanger et al., 2024). The technological systematization of this ecosystem extends beyond the optimization of public security and has redefined the parameters of institutional order through an authoritarian lens.

The evolution of state control mechanisms must be situated within the framework of the structural reforms launched under the Reform and Opening-up policy (**改革开放**, *Gǎigé Kāifàng*)[2]. The transition from community-based surveillance networks to large-scale digital infrastructures was consolidated through the implementation of the Golden Shield Project (**金盾工程**, *Jīndùn Gōngchéng*)[3] and the establishment of the Great Firewall of China (**防火长城**, *Fánghuǒ Chángchéng*)[4], enabling the Chinese Communist Party (CCP) to exert comprehensive control over information flows and social behavior.

The exportation of the SCS and its associated technologies has transcended the borders of the PRC. Through mechanisms such as the Belt and Road Initiative (BRI), bilateral cybersecurity agreements, and cooperation in digital infrastructure, Beijing has promoted a technopolitical design[5] aimed at institutionalizing automated surveillance systems in countries with varying degrees of democratic consolidation (Oliveira et al., 2020; Rocha Pino, 2017; Ding, 2024). This strategy has been welcomed in contexts such as Iran, Venezuela, Russia, and Nigeria, where ruling elites deploy such systems to reinforce internal control and limit accountability (Nguyen et al., 2023; Segal, 2025; Adeyeye & Grobbelaar, 2024).

The analysis is grounded in a mixed methodological strategy, combining documentary analysis of regulatory frameworks and technological platforms with an empirical assessment through the State Control Index (SCI), a tool designed to quantitatively measure the relationship between perceived security, digital surveillance, and restrictions on fundamental rights (Mozur et al., 2019; Wright, 2018). From this approach, the study seeks to contribute to the academic debate on the limits of legitimacy in digital authoritarian regimes, while problematizing the diffusion risk of these models into fragile or transitional democracies.

[1] The term *big data* refers to the large-scale processing of information to identify behavioral patterns, a practice employed by the Chinese state to implement automated systems of citizen classification (Mayer-Schönberger & Cukier, 2013).

[2] The Reform and Opening-up policy (**改革开放**, *Gǎigé Kāifàng*) was introduced by Deng Xiaoping in 1978 as a strategy for economic, institutional, and technological modernization, paving the way for the development of digital control systems.

[3] The Golden Shield Project (**金盾工程**, *Jīndùn Gōngchéng*) is a public security program launched in 2000 by the Ministry of Public Security of the PRC. It aims to integrate databases, video surveillance systems, and digital identification tools to reinforce state control through smart technologies (Creemers, 2018; Xi, 2014).

[4] The expression *Great Firewall of China* (**防火长城**, *Fánghuǒ Chángchéng*) refers to the state-run internet censorship and filtering system implemented by the Chinese government to regulate the flow of online information, forming part of its broader cyber control architecture (Feldstein, 2019; Goodman & Flaxman, 2016).

[5] The term *technopolitical design* refers to the construction of digital infrastructures that encode normative decisions and power structures, combining surveillance, administration, and coercion through algorithmic logic (Zuboff, 2019; Srivastava & Bullock, 2024).

METHODOLOGY

This study adopted a mixed-methods approach, supported by an explanatory-comparative design aimed at analyzing the transnational projection of the digital surveillance model promoted by the PRC. This approach was structured across two analytical levels: (*i*) the qualitative systematization of regulatory frameworks, technological platforms, and institutional discourses of legitimization, and (*ii*) the use of quantitative tools that enabled the modelling of the system's impact on key variables within authoritarian and semi-authoritarian contexts.

From a qualitative standpoint, documentary analysis of primary sources was conducted, including the *State Council's Approval on the Restructuring of the Interministerial Conference for the Construction of the SCS* (State Council of the PRC, 2012), alongside specialized literature on artificial intelligence, algorithmic governance, digital security, and human rights (Creemers, 2018; Feldstein, 2019; Castellanos-Claramunt, 2023). This examination enabled the identification of technopolitical dynamics related to the configuration of China's surveillance ecosystem and its mechanisms of international projection.

Within this framework, technopolitical design was understood as a structuring force of contemporary digital order. From this perspective, artificial intelligence systems were not regarded as neutral tools but rather as architectures of power embedded in regulatory frameworks, state capacities, and political rationalities (Zuboff, 2019; Stanger et al., 2024; Srivastava & Bullock, 2024). Accordingly, the SCS was conceptualized not as a purely national system but as a mechanism of sociopolitical regulation with transnational reach (Ding, 2024; Huawen, 2021; Zhang & Shaw, 2023).

In the quantitative dimension, a comparative dataset was constructed using consolidated reports (Nguyen et al., 2023; Mozur et al., 2019; Segal, 2025), which enabled the analysis of five key indicators: perceived security, degree of technological penetration, restrictions on freedom of expression, breaches of informational privacy, and documented cases of political repression. The data were organized into regional matrices to identify patterns of digital state control, distinguishing their implementation in institutionally robust regimes from those in fragile or co-opted states (Pearson et al., 2022; Oliveira et al., 2020).

The innovative component of this research lay in the formulation of the **State Control Index (ICE)**, a modelling tool that enabled the quantification of the relationship between digital surveillance, perceived security, and the degree of restriction on fundamental freedoms. The **ICE** was expressed through the following equation:

$$\boldsymbol{I_c = (\alpha \times S) + (\beta \times V) - (\gamma \times L)}$$

where $\boldsymbol{S}$ denoted perceived citizen security, $\boldsymbol{V}$ the effective reach of the implemented digital surveillance systems, and $\boldsymbol{L}$ the level of restrictions on civil rights and fundamental freedoms. The weighting coefficients $\boldsymbol{\alpha}$ (*alpha*), $\boldsymbol{\beta}$ (*beta*) and $\boldsymbol{\gamma}$ (*gamma*) were defined through multiple linear regression analysis, applying weighted estimation methods to the empirical dataset. The calibration of these weights was carried out by considering both the number of countries that had adopted Chinese surveillance technologies (Skare et al., 2024) and the magnitude of adverse impacts on sensitive sociopolitical variables (Feldstein, 2019; Nguyen et al., 2023). The index was conceived as a replicable tool for the comparative analysis of digital authoritarianism, offering a quantifiable framework grounded in the discipline of International Relations.

To empirically confirm the **SCI**, a nested case study design was adopted. Three contrasting scenarios were analyzed: (*i*) the People's Republic of China, representing a fully institutionalized model of digital surveillance; (*ii*) Nigeria, as a case of partial implementation reliant on foreign technology transfer (Adeyeye & Grobbelaar, 2024); and (*iii*) Venezuela, a

recipient of Chinese control technologies, where the authoritarian regime instrumentalized such systems amidst processes of democratic erosion (Greitens et al., 2020; Wright, 2018). This strategy responded to the principle of minimal structural variation and allowed for the evaluation of differences in efficacy, legitimacy, and social resistance to the expansion of digital control mechanisms.

The theoretical framework of the study articulated a transdisciplinary perspective that interwove elements of regime theory, algorithmic governance, critical technology studies, and digital geopolitics (Chan et al., 2024; Tuzov & Lin, 2024; Sandbrink et al., 2024). It also situated within contemporary debates on authoritarian diffusion, whereby the export of control models was legitimized through legal frameworks, strategic cooperation, and digital infrastructure deployment (Rocha Pino, 2017; Cancela-Outeda, 2024; Stanger et al., 2024).

Finally, the epistemological approach followed abductive logic, whereby inferences were constructed inductively from empirical data, aiming to theorize new configurations of power in the international domain. In this regard, the proposed methodology stood as an original contribution to the study of digital authoritarianism, its mechanisms of reproduction, and its implications for global balances of security, governance, and fundamental rights.

RESULTS

Evolution of the Surveillance Model in the People's Republic of China

The consolidation of the digital surveillance system in the PRC has evolved as a deliberate and sustained political strategy grounded in a technopolitical vision of state governance. This model is built upon a centralized normative framework, a decentralized technological infrastructure, and an algorithmic system specifically designed for population control. Rather than emerging as a reactive response to domestic insecurity, the institutionalization of this surveillance regime reflects a long-term political initiative promoted by the CCP, combining structural reform, ideological reinforcement, and an agenda of authoritarian modernization (Creemers, 2018; Xi, 2014; Feldstein, 2019; Ding, 2018).

The legal foundation was laid with the *Approval by the State Council on the Restructuring of the Interministerial Conference for the Construction of the Social Credit System* (State Council of the PRC, 2012). This policy framework established the technical, legal, and administrative basis for the SCS, designing an interinstitutional grid capable of evaluating citizens according to behavioral patterns, financial history, civic engagement, and digital interactions. The underlying rationale is one of algorithmic meritocracy, in which individual performance is transformed into input for automated administrative decision-making.

The system's evolution followed a phased development: from local pilot projects such as Rongcheng (Mozur, Kessel, & Chan, 2019) to national expansion through facial recognition, biometric monitoring, and the centralization of regional databases. Table 1 summarizes this progression, highlighting major regulatory, technological, and institutional milestones.

Table 1. *Timeline of the evolution of the surveillance model in the PRC*

Decade	Milestone	Description
2003	"Skynet" Initiative	Deployment of a nationwide video surveillance system, with over 20 million cameras installed in urban areas.
2012	Restructuring of the SCS	Establishment of the national framework for comprehensive civic evaluation under State Council Document No. 88.
2015	Implementation of scoring systems	Introduction of social credit mechanisms in pilot cities like Rongcheng, integrating legal, financial, and neighborhood-level data.

2018	Expansion via facial recognition	Extension of surveillance into public spaces using biometric identification and real-time AI.
2020	Nationwide algorithmic integration	Centralization of regional platforms into a unified national citizen monitoring system.
2022	Internationalization of the model	Export of surveillance technology to countries in Africa, Central Asia, and Latin America through bilateral agreements and corporate partnerships.

Source: Own elaboration based on State Council (2012), Creemers (2018), Ding (2018), Mozur et al. (2019), Castellanos-Claramunt (2023), and Wright (2018).

This trajectory illustrates the CCP's ability to align normative structures with technological capability, consolidating a predictive surveillance system grounded in the automated cross-analysis of personal data. This consolidation has been accompanied by a narrative that frames surveillance as a tool for social harmony and national order, thereby redefining the citizen as a subject of continuous observation and behavioral evaluation (Amoore, 2020; Zhang & Shaw, 2023; Vickers, 2022). By embedding algorithmic processing into regulatory frameworks, the system gains operational flexibility beyond individual supervision, enabling intervention in access to basic services such as healthcare, transportation, and employment (Nguyen, Lafrance, & Vu, 2023).

Impact of the SCS on Fundamental Rights

The implementation of the SCS by the PRC has significantly transformed the conditions of citizenship by merging an algorithmic surveillance model that converts individual behavior into a decisive parameter for accessing fundamental rights. This data-driven governance framework does not merely modernize public administration; it institutionalizes a political rationality centered on the continuous evaluation of the governed subject, legitimizing their inclusion in or exclusion from the system based on civic merit criteria (Creemers, 2018; Amoore, 2020; Castellanos-Claramunt, 2023).

Following the enactment of State Council Document No. 88 (2012), the legal and technological infrastructure of the SCS enabled individual and organizational scoring mechanisms through unified digital platforms, without the need for judicial intervention or traditional procedural safeguards (State Council of the PRC, 2012; Mac Síthigh & Siems, 2019). This ecosystem functions as an architecture of enforced visibility, composed of governmental databases, private corporations, digital platforms, and biometric systems that process data from financial records, judicial decisions, social media behavior, and commercial interactions.

One of the most widely referenced examples is the pilot project in the city of Rongcheng, where judicial, banking, and community-level data are combined to generate a civic score. This score determines access to public services, the ability to travel, and eligibility for financial credit.

The empirical evidence gathered shows a disproportionately adverse impact across several critical dimensions of civic life. Table 2 summarizes the perceived positive and negative effects in five key areas:

Tabla 2. *Impact of the SCS on society*

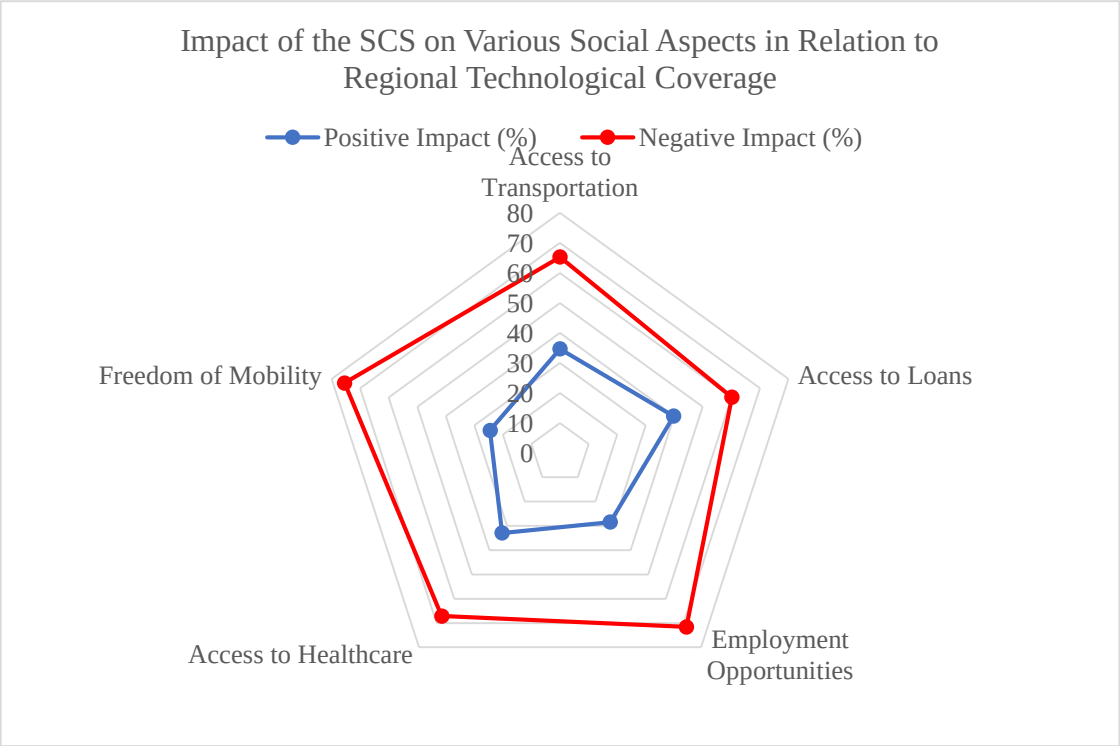
Evaluated Area	Positive Impact (%)	Negative Impact (%)
Freedom of movement	24.50	75.50
Employment opportunities	28.40	71.60
Access to healthcare	32.90	67.10
Access to transportation	34.70	65.30
Access to credit	39.80	60.20

Source: Own elaboration based on Nguyen et al. (2023).

The assessment reveals a punitive governance structure grounded in algorithmic classification. This mechanism generates negative externalities on upward social mobility, reconfiguring access to public goods according to behavior-based conditionality. The result is a model of stratified citizenship, in which social participation becomes contingent upon metrics of compliance.

Figure 1 visualizes the correlation between technological coverage and the adverse impacts of the system. It shows a direct relationship between technological deployment and the severity of negative effects, particularly in employment, transportation, and healthcare.

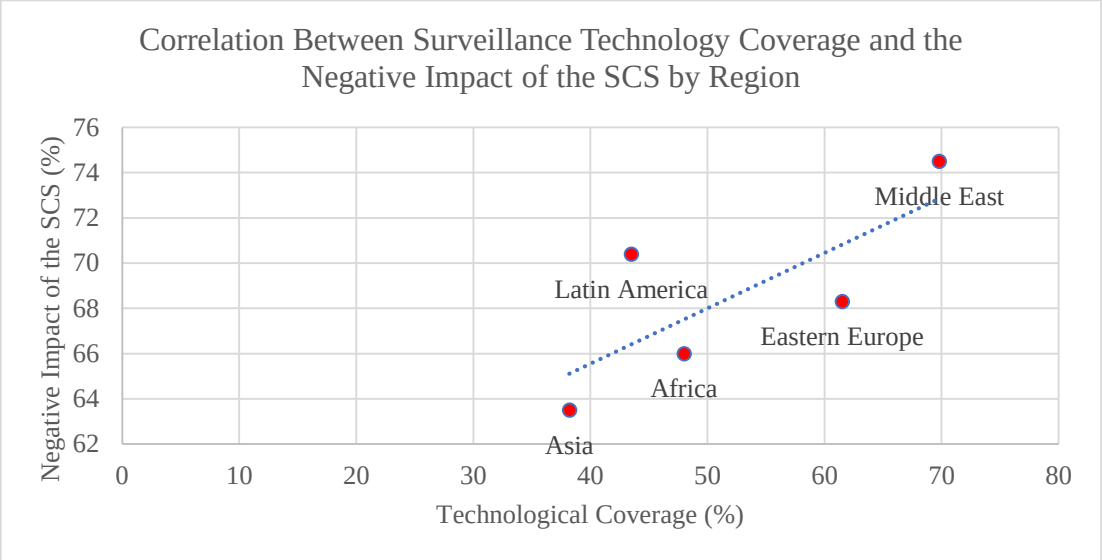
Figure 1. *Impact of the SCS on Different Social Dimensions in Relation to Regional Technological Coverage*



Source: Own elaboration based on Nguyen et al. (2023) and Segal (2025)

The correlation between technological infrastructure and rights restrictions becomes more evident in Figure 2, which illustrates the negative impact by geographic region as a function of system coverage. The Middle East and Asia, both with surveillance penetration rates exceeding 60%, show the highest levels of adverse effects. Latin America, despite its comparatively lower adoption rate, also proves significant consequences. This suggests that the effectiveness of the model is not solely a function of technological reach, but also of institutional fragility at the national level (Wright, 2018; Gomes Rêgo de Almeida & Dos Santos Júnior, 2025).

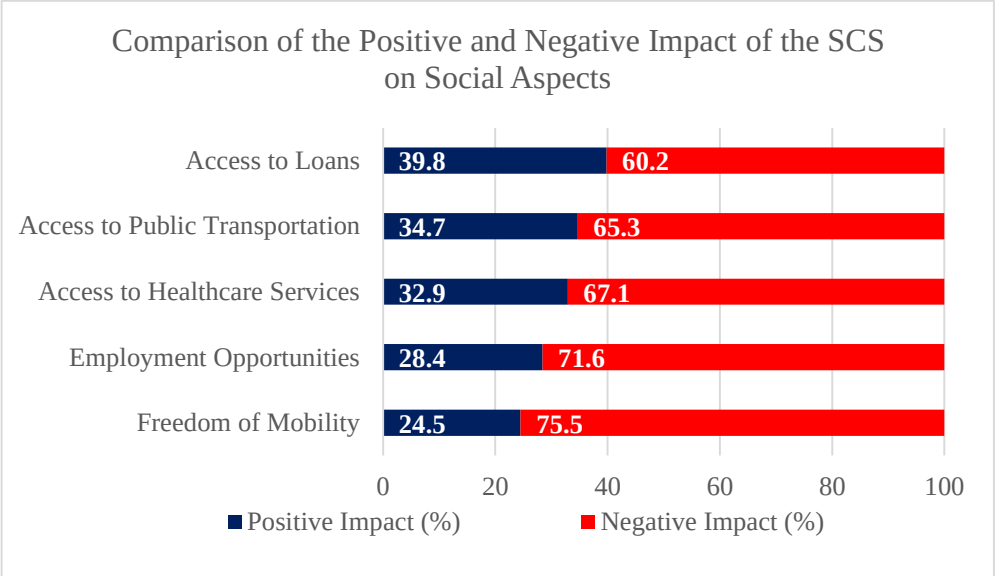
Figure 2. *Correlation Between Surveillance Technology Coverage and Negative Impact of the SCS by Region*



Source: Own elaboration based on Nguyen et al. (2023) and Segal (2025).

Figure 3 reinforces this trend by directly comparing the percentages of positive and negative impact. The percentage differentials reveal a concentration of adverse effects on domains that constitute essential rights. The system thus conditions social inclusion on recorded obedience, weakening the principle of equality before the law and eroding the normative core of fundamental rights (Amoore, 2020; Castellanos-Claramunt, 2023).

Figure 3. *Comparison of the Positive and Negative Impact of the SCS Across Different Social Domains*



Source: Own elaboration based on Nguyen et al. (2023).

Based on these findings, the **State Control Index (ICE)** was applied as a tool for comparative measurement. As previously defined, the **ICE** is expressed as:

$$\boldsymbol{I_c = (\alpha \times S) + (\beta \times V) - (\gamma \times L)}$$

Where:

- $\boldsymbol{S}$ = perception of public security
- $\boldsymbol{V}$ = intensity of digital surveillance
- $\boldsymbol{L}$ = degree of restriction of fundamental rights

The coefficients $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ were calibrated using multiple linear regression analysis applied to a custom-built comparative dataset, combining empirical metrics and specialized literature. The weighting was informed by three core criteria: the intensity of state action, the ideological alignment of the regime with digital authoritarian models, and the normative depth of the legal framework in cybersecurity and algorithmic control[6].

The cases selected for this quantitative evaluation include the PRC, Venezuela, and Nigeria. This methodological decision follows a nested design logic with maximal contextual variation[7]. All three countries maintain technological links with Beijing but differ in terms of institutional appropriation, operational efficacy, and regulatory consolidation in the realm of digital governance[8]. Table 3 presents the values used to estimate the index in each case.

Table 3. *Impact of SCS on Society*

Country	S (security)	V (surveillance)	L (restrictions)	α	β	γ
PRC	85.5	100	94.8	0.8	1.2	1.5
Venezuela	68.9	79	87	0.8	1.2	1.5
Nigeria	58.4	55	74.5	0.8	1.2	1.5

Source: Own elaboration based on Mozur et al. (2019), Nguyen et al. (2023), Feldstein (2019) and Adeyeye & Grobbelaar (2024).

The calculations yield an ICE of **46.12** for the PRC, reflecting a fully consolidated model in which the interdependence among security perception, technological coverage, and institutionalized restrictions acquires systemic consistency. In Venezuela, the index reaches **36.18**, indicating an intermediate structure sustained by technological cooperation with China but constrained by a fragmented legal architecture. Nigeria, with an ICE of **1.05**, stands for a still-emerging model, lacking robust legal articulation and sufficient public legitimacy to institutionalize its control mechanisms.

These results confirm that ICE is a valid metric to assess the institutionalization of algorithmic state control. Its design enables a rigorous empirical reading of authoritarian diffusion, integrating technological, legal, and sociopolitical dimensions that rarely converge in a single indicator. Beyond quantifying technological presence, the index allows inferences about a regime's structural capacity to embed such technology as a governance tool.

This interpretation is supported by recent studies that address the SCS as an expression of digital authoritarian rationality. SCS should not be understood as a mere tool for administrative efficiency. Its logic is structurally designed to maximize state control by progressively reducing the margins of individual autonomy. This form of algorithmic architecture is based on data correlations rather than deliberative processes or legal safeguards and tends to consolidate in contexts characterized by high coercive capacity and limited democratic oversight (Stanger et al., 2024; Ding, 2018; Goodman & Flaxman, 2016).

The evidence presented supports the argument that the SCS redefines the notion of citizenship under the logic of algorithmic legibility, wherein every individual is subject to constant evaluation with direct material consequences. The following sections will examine how this model has been adapted across other political and cultural contexts and will assess the variables that modulate its effectiveness beyond the normative framework of China.

[6] "*Normative depth*" refers to the level of institutional density, legal development, and enforcement effectiveness within regulatory frameworks oriented toward digital control and algorithmic surveillance (Vickers, 2022).

[7] The comparison through nested cases enables the analysis of units with shared structural relationships while maintaining key differences in institutional configuration, thereby allowing for more robust inferences in comparative politics research (Gerring, 2007).

[8] Several studies have documented the technological and regulatory exportation of China's digital control model to hybrid or authoritarian regimes, highlighting its role as a structuring vector of emerging forms of transnational surveillance (Greitens, Lee & Yazici, 2022).

Exportation of the Chinese Model and Geopolitical Correlations

The international strategy of the PRC in the realm of digital surveillance is structured around a comprehensive approach that integrates technological infrastructure, regulatory architecture, and institutional mechanisms to transfer a centralized model of control grounded in artificial intelligence and algorithmic analysis of large-scale data flows. This model has become a cornerstone of the country's foreign policy, which combines material elements—such as 5G networks, surveillance systems, and mass data processing platforms—with regulatory instruments designed to influence institutional configurations in recipient states (Zhu, Cerina, Chessa, Caldarelli, & Riccaboni, 2014; Pearson, Rithmire, & Tsai, 2022; Wu, Esposito, & Evans, 2024).

This global projection goes beyond the mere exportation of hardware or technical solutions. It entails a deep restructuring of digital regulatory ecosystems through the strategic expansion of state-owned enterprises, cybersecurity agreements, and the provision of legal frameworks that align with algorithmic governance logic (Ding, 2018; Aoyama, 2022). Table 4 illustrates the global distribution of Chinese digital surveillance technology across different world regions, highlighting a strategic concentration in areas marked by weak institutional consolidation or insufficient legal safeguards for personal data protection.

Table 4. *Global distribution of PRC digital surveillance technology*

Region	Number of countries with Chinese technology	Regional coverage (%)
Asia	15.00	61.50
Africa	12.00	48.00
Latin America	10.00	43.50
Eastern Europe	8.00	38.20
Middle East	14.00	69.80

Source: Own elaboration based on Segal (2025).

The geographical deployment of this technology is supported by institutionalized mechanisms of transfer and expansion. As shown in Table 5, these mechanisms do not operate in isolation but function as strategic channels to replicate the PRC's algorithmic governance model in external environments. This has enabled the projection of an alternative normative framework to prevail Western multilateral standards through bilateral agreements and specialized technical cooperation.

Table 5. *Export mechanisms of the Chinese digital governance model*

Export Mechanism	Description
Investment in digital infrastructure	Financing and construction of 5G networks, surveillance systems, and data platforms in developing countries.
Technology transfer	Provision of surveillance software, facial recognition systems, and social credit platforms to foreign governments.
Cybersecurity cooperation	Bilateral agreements with allied nations to share digital control technologies and data analytics.
Expansion of state-owned enterprises	Chinese firms such as Huawei and ZTE as key actors in the global deployment of technological networks.
Exportation of regulatory norms	Application of digital control and surveillance models within the legal systems of recipient state.

Source: Own elaboration based on Zhu et al. (2014) and Wu et al. (2024).

This internationalization strategy finds its most favorable reception conditions in contexts where institutional frameworks are fragile or susceptible to external influence. As shown in Table 6, there is a significant correlation between the presence of Chinese technology and the implementation of digital control schemes, particularly in regions maintaining close ties with

Beijing. Central Asia and the Middle East lead in both metrics, suggesting a structural alignment with the algorithmic governance model promoted by the CCP.

Table 6. *Penetration of Chinese technologies and implementation of digital control models by region*

Region	Presence of Chinese Technology (%)	Implementation of Control Models (%)
Asia	47.30	38.90
Africa	52.60	42.10
Latin America	68.50	59.30
Eastern Europe	73.20	65.70
Middle East	49,70	41,40

Own elaboration based on Sánchez & Asmat (2024) and Wu et al. (2024).

The consolidation of the digital governance model promoted by Beijing's leadership has not relied exclusively on legal frameworks or bilateral agreements. Its effectiveness has also been supported by the strategic deployment of digital platforms developed by technology conglomerates linked to the Chinese state, which function as instruments for institutionalizing a far-reaching algorithmic surveillance regime. These platforms have been introduced in recipient governments under the guise of technological modernization, although their operational logic is geared toward continuous behavioral evaluation, mass supervision, and anticipatory management of public order.

The analyzed systems share an architecture based on AI, continuous monitoring, and real-time processing of large volumes of data. In institutional environments with limited oversight capacity, these platforms do not serve merely technical functions. They configure a grammar of governability that redefines the relationship between state and citizen. They classify, score, archive, and feed back into public decision-making based on predictive logic. The most emblematic case is the Social Credit System, which transforms everyday behavior into a criterion of eligibility for basic services. Complementary systems include Skynet, a facial recognition-based surveillance infrastructure; Huawei Cloud, a platform for massive state data storage and processing; and Safe City, an urban control framework based on predictive policing algorithms. Table 7 summarizes the most relevant platforms exported by the PRC and their institutional use in recipient countries.

Table 7. *Digital governance platforms exported by the PRC*

Plataform	Function in Recipient Country
Social Credit System	Evaluation of citizen behavior to determine access to government benefits.
Skynet	Large-scale surveillance network with integrated facial recognition.
ZTE Smart City	Urban management based on real-time data analysis.
Huawei Cloud	Infrastructure for storage and processing of government data.
Safe City	AI integration in public security for crime prevention.

Source: Own elaboration based on Bonsón et al. (2012) and Wu et al. (2024).

The functional rationale behind this digital architecture has also manifested in the economic sphere, where automated systems have enabled substantial improvements in logistics, administration, and trade. Table 8 documents significant reductions in operational costs and processing times, reinforcing the perception of efficiency that, in some cases, has justified the adoption of the model despite the absence of democratic safeguards (Adeyeye & Grobbelaar, 2024; Oliveira, Murton, Rippa, Harlan & Yang, 2020).

Table 8. *Impact of Chinese digital automation on logistics and international trade*

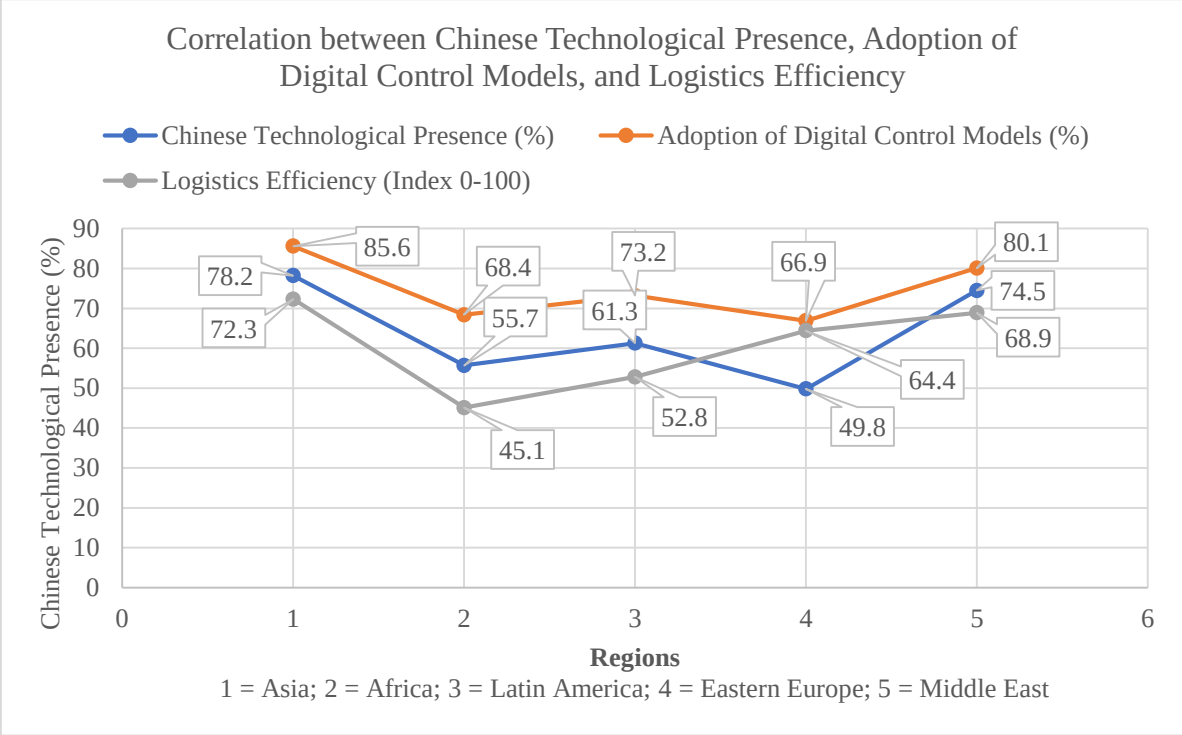
Sector	Cost Reduction (%)	Processing Time Reduction (%)
Maritime transport	24.50	36.80
Port logistics	30.20	42.10
E-commerce	28.70	40.50

Customs administration	22.30	33.60

Source: Own elaboration based on Sánchez & Asmat (2024).

This dual functionality—structural surveillance and operational efficiency—is visually represented in Figure 4, which illustrates the correlation between the presence of Chinese technology, the adoption of digital control models, and logistical performance across different regions.

Figure 4. *Correlation Between Chinese Technological Presence, Adoption of Digital Control Models, and Logistical Efficiency*



Source: Own elaboration based on Nguyen et al. (2023), Wu et al. (2024) and Bonsón et al. (2012).

The analysis indicates that the Chinese model of digital surveillance is not deployed as a collection of isolated solutions. Rather, it constitutes a systemic architecture that promotes a specific mode of state governance, where order, predictability, and centralization are prioritized over transparency, deliberation, and the safeguarding of fundamental rights (Chan, Papyshev & Yarime, 2024; Cancela-Outeda, 2024; Castellanos-Claramunt, 2023).

Comparative Assessment through the State Control Index (SCI)

The comparative analysis of digital surveillance models requires tools that integrate technological, regulatory, and sociopolitical variables. To this end, the State Control Index (SCI) is proposed as a composite metric that allows for the quantitative assessment of the intensity of algorithmic control exercised by states over their populations. This index considers, first, the degree of penetration of digital surveillance technologies; second, the level of perceived citizen security; and finally, the documented impact on fundamental rights, particularly regarding privacy and freedom of expression.

The initial application of the SCI includes five representative states that share three structural characteristics: elevated levels of technological adoption, permissive regulatory frameworks concerning privacy, and institutional architectures oriented toward informational control. The selected cases are the PRC, Venezuela, Iran, Saudi Arabia, and the Russian Federation. These serve to contrast varying degrees of consolidation of the digital surveillance model promoted by Beijing.

The first component of the SCI, associated with the perceived legitimacy of the control apparatus, is analyzed through the relationship between the use of Chinese surveillance technology and perceived state security. Table 9 summarizes this relationship, showing that the PRC reports the highest technological coverage alongside the highest perception of security. The remaining countries show acceptable levels of perceived safety, although technological gaps suggest differences in operational and narrative capacity across the regimes analyzed (Mozur, Kessel & Chan, 2019; Wright, 2018).

Table 9. *Use of Chinese Surveillance Technology and Perception of Security.*

Country	Use of Chinese Technology (%)	Perception of Security (%)
PRC	100.00	85.40
Venezuela	79.00	68.90
Iran	76.00	70.20
Saudi Arabia	73.00	74.80
Russia	71.00	72.30

Source: Compiled by the authors based on Mozur et al. (2019) and Wright (2018).

Although the perception of safety in these countries remains high, this phenomenon cannot be interpreted solely because of increased citizen protection. According to Amoore (2020), such figures may be explained by an internalized algorithmic ethic, in which citizens, facing omnipresent surveillance, reconfigure their expectations of security based on their conformity with the monitoring system.

The second component of SCI analyzes concrete restrictions on fundamental liberties. Table 10 details the rates of censorship, intrusive surveillance, and documented political repression over the past five years. In all cases, there is a direct relationship between the intensive use of AI for surveillance and systematic practices of silencing dissent (Greitens, Lee & Yazici, 2020; Feldstein, 2019).

Table 10. *Impact of Digital Surveillance on Freedom of Expression and Privacy*

Country	Restriction of Freedom of Expression (%)	Restriction of Privacy (%)	Documented Cases of Political Repression (Last 5 Years)
PRC	92.30	94.80	135,000+
Venezuela	89.70	87.20	10,400
Iran	87.10	89.50	9,800
Saudi Arabia	84.50	88.10	7,900
Russia	80.90	85.40	6,500

ource: Compiled by the authors based on Greitens et al. (2020) and Feldstein (2019).

The data indicates that digital surveillance models foster normalized coercive practices. Zuboff (2019) terms this "*computational authoritarianism*", where mass data and algorithmic classification reduce individual agency to measurable behavioral outputs.

Table 11 provides an analysis of the institutional framework adopted by each country, distinguishing between the system's stated objectives and its documented use. This contrast enables the identification of divergences between official security narratives and the concrete effects on the public sphere.

Table 11. *Digital Surveillance Models and Their Stated vs. Actual Objectives*

Country	Adopted Surveillance Model	Official Objective	Documented Use
PRC	Social Credit System, *Skynet*	National security and stability	Population control through mass digital surveillance.
Venezuela	Carnet de la Patria, digital censorship	Economic and social control	Monitoring and restricting service access based on political loyalty.
Iran	National intranet, content filtering	Protection of Islamic values	Censorship and restriction of access to dissenting information.

Saudi Arabia	Facial recognition algorithms, forensic biometrics	Counter-terrorism	Surveillance and repression of opposition and activists.
Russia	SORM (Communication Interception System)	Cybersecurity	Monitoring communication networks and political repression.

Source: Compiled by the authors based on Mozur et al. (2019) y Nguyen et al. (2023).

This pattern of politically motivated technological deployment does not occur in a vacuum. As shown in Table 12, its implementation is closely shaped by demographic factors, population density levels, and weak regulatory frameworks. Larger populations provide stronger incentives for adopting automated algorithmic control mechanisms. Simultaneously, restriction levels tend to rise as technological infrastructure becomes more interoperable with state architectures (Stanger et al., 2024; Ding, 2018).

Table 12. *Comparison of Population, Surveillance Technology Penetration, and Restriction of Freedoms in Digital Monitoring Regimes*

Country	Population (millions)	Surveillance Technology Use (%)	Restriction of Freedoms (%)
PRC	1,410	100.00	94.80
Venezuela	28	79.00	87.20
Irán	85	76.00	89.50
Russia	144	71.00	85.40
Nigeria	223	55.00	74.50
Saudi Arabia	36	73.00	88.10

Source: Compiled by the authors based on Stanger et al. (2024) and Ding (2018).

An essential component in the calculation of the State Control Index (SCI) is the legal dimension, which reflects the normative infrastructure that supports or limits the deployment of algorithmic surveillance systems. Table 13 presents a comparative overview of regulatory frameworks, emphasizing the contrast between regimes that prioritize the protection of individual rights and those that adopt centralized legal architectures facilitating state surveillance. While the European Union enforces a rights-based approach grounded in transparency and data protection, countries aligned with the PRC's governance logic tend to implement top-down regulatory schemes with limited mechanisms for independent oversight. This contrast underscores the role of legal systems in either safeguarding civil liberties or reinforcing digitally enabled state control (Goodman & Flaxman, 2016; Pearson, Rithmire & Tsai, 2022).

Table 13. *Comparison of Regulatory Frameworks on Privacy and State Control*

Country/Region	Key Regulation	Regulatory Approach	Use of AI in Surveillance
European Union	GDPR (EU Regulation 2016/679)	Protection of data and individual rights	Restricted to public security with oversight.
United States	Federal Privacy Act	Sector-based data protection	Cybersecurity and crime prevention applications.
PRC	Data Security Law, Cybersecurity Law	State control over information flows	Extensive: AI used in social credit and facial recognition.
Russia	Yarovaya Law, SORM System	State supervision of communications	Mass monitoring is supported by predictive algorithms.
Venezuela	Carnet de la Patria, digital censorship tools	Socioeconomic control and censorship	Early-stage implementation with Chinese infrastructure.

Source: Compiled by the authors based on Goodman & Flaxman (2016), Vickers (2022) and Pearson et al. (2022).

Finally, Table 14 contrasts the regulatory approaches adopted by democratic and authoritarian regimes in relation to both public and private uses of artificial intelligence. This comparative

analysis underscores the positioning of the PRC's model within a framework of centralized state dominance, where control is prioritized over accountability. Such an approach reveals a fundamental incompatibility with the principles of transparency, institutional oversight, and individual autonomy that underpin liberal democratic systems (Stanger et al., 2024).

Table 14. *Regulatory Strategies for AI in Public and Private Domains*

Aspect	Democratic Approach	Authoritarian Approach
AI Governance	Based on transparency and public auditing	State control with no independent oversight.
Data Access	Regulated to protect individual privacy	Centralized and unrestricted state access.
Use in Education	Applied for personalized learning	Ideological enforcement and homogenization.
Corporate Supervision	Regulated to prevent bias and monopolies	Corporate-state integration.

Source: Compiled by the authors based on Stanger et al. (2024) and Ding (2018).

The comprehensive analysis of the SCI confirms that the digital governance architecture promoted by the PRC is not confined to its domestic domain. Its international expansion reflects a structured logic grounded in operational efficiency, institutional consolidation, and the programmed reduction of individual autonomy. This model redefines digital security parameters, imposing a paradigm of algorithmic surveillance that challenges contemporary legal frameworks and poses critical risks to the global architecture of human rights.

DISCUSSION

The findings presented reveal a profound reconfiguration of the relationship between power, technology, and citizenship. In contexts marked by limited institutional oversight, digital surveillance has stopped being a subsidiary tool for enhancing state security. It has become the functional nucleus of an emerging mode of governance, where control is not an exceptional measure but a continuous operational principle. This transformation is not confined to technical dimensions. It signals a political shift from law as a normative boundary to algorithmic correlation as the dominant form of regulation. Decisions are no longer shaped through reflective processes; they are generated automatically. The democratic subject is replaced by a functional entity: a citizen who is monitored, predictable, and structurally legible.

The case of the People's Republic of China (PRC) is illustrative of this institutionalized paradigm of digital surveillance. Under the leadership of the current General Secretary of the Chinese Communist Party (CCP) and seventh President of the PRC, a model has emerged that transcends traditional supervision. What has been implemented is not simply a technical tracking system but a sociopolitical architecture of algorithmic control. Platforms such as Skynet and the Social Credit System have been deployed to convert every individual action into data subject to normative evaluation. In this ecosystem, citizen behavior is observed, processed, and transformed into a reliability score. That score is far from neutral: it conditions access to rights, shapes life trajectories, and imposes boundaries without judicial review.

This is not merely a public administration infrastructure. It is a system of engineered consent, whose logic exceeds bureaucratic efficiency and aligns with a totalizing project of government. Transparency is unidirectional—demanded from the bottom up—while those in power remain concealed behind layers of institutional opacity. This design does not simply punish deviations; it seeks to preempt them. It defines the acceptable in advance. Everything that deviates from statistical norms is flagged as a potential threat. Surveillance is no longer corrective. It becomes constitutive of social order.

The vertical configuration between observer and observed serves as the backbone of a renewed form of political domination. Visible violence is no longer necessary. The constant possibility

of being watched suffices for the political subject to internalize the gaze of power. What is external becomes internal. Norms are no longer enforced through coercion; they become embodied in habits, daily decisions, and the perception of one's environment as a monitored space. Behavior adjusts to thresholds defined by the system. Self-censorship is not imposed—it emerges as an adaptive strategy. Public life becomes a choreography of predictability. Legitimate conflict is neutralized before it can take shape.

The methodological tool proposed in this study, the State Control Index (SCI), quantifies these processes. China registers the highest values, not only due to its technological infrastructure but also because of its capacity to translate that infrastructure into effective mechanisms of social regulation. Venezuela represents a partial imitation, where technological cooperation with Beijing coexists with structural institutional weaknesses. Nigeria, by contrast, exhibits a fragmented implementation, lacking internal legitimacy and relying on external assistance. In all cases, a common pattern emerges: the gradual erosion of the citizen's autonomous space for action.

In Latin America, this debate takes on a pressing relevance. The region's democratic systems are increasingly strained by the demand for immediate solutions to deep-rooted issues such as insecurity, corruption, and representation crises. In this context, the Chinese model may appear to offer a functional response. However, adopting such a paradigm without solid institutional safeguards risks undermining constitutional frameworks. The historical inclination to privilege administrative efficiency over institutional legitimacy has produced enduring consequences across the region. Once mechanisms of control are introduced, they exhibit a marked tendency toward permanence. Measures initially framed as provisional gradually acquire the status of standard procedure. Regulatory frameworks, instead of evolving, solidify into rigid norms resistant to reform or democratic scrutiny.

The model exported from Beijing is not neutral. It does not consist solely of technological platforms, but rather of a conception of power rooted in the technical management of human behavior. It privileges predictability over dissent. It treats freedom as dysfunction. Its logic is imposed not through violence, but through the appearance of rationality. Control is framed as modernization. Order as efficiency. The consequence, however, is citizenry reduced to a parameter and politics reduced to calculation.

The current Chinese head of state has played a pivotal role in this transformation. Xi Jinping has advanced a model of governance that replaces pluralism with homogeneity and public deliberation with anticipatory silencing. Under his mandate, surveillance has ceased to be tactical and has become doctrinal. The aim is not to manage conflict but to eliminate it before it materializes. A society of assessable, obedient, and uniform citizens is designed. Technological advancement is not used to expand freedoms, but to restrict them. Difference –central to democratic life– is treated as a statistical anomaly.

This model resonates internationally because it offers the promise of stability. In democracies where institutions have lost responsiveness, imitation becomes tempting. It is presented as a solution to complexity, a tool to discipline perceived chaos. Yet the cost is high: agency is relinquished, public debate is curtailed, and the political sphere is reduced to a protocol of permitted behaviors. Citizenship becomes a data function. The political is absorbed by the technical.

Even in settings where formal checks and balances exist, surveillance logics are expanding quietly. The contemporary citizen interacts daily with devices that collect, process, and analyze movements, preferences, and routines. This monitoring is no longer perceived as exceptional: is part of the landscape. Democracies that normalize this condition without critical reflection risk adopting, inadvertently, the premises of authoritarian order. The boundary between

legitimate oversight and total control becomes blurred. What once required legal justification is now implemented in the name of preventive security.

The international community stands at a critical juncture. The core challenge lies not in the technological sophistication of surveillance systems but in the absence of robust normative frameworks capable of constraining their political implications. Without binding global regulations that establish clear boundaries for algorithmic control, a new mode of governance is likely to emerge. This model normalizes the silent suppression of dissent and transforms public life into a sequence of automated processes. Within this configuration, the state ceases to act as a guarantor of rights and instead becomes a manager of behavioral predictability. Citizenship is reduced to a data point in a regulatory system. Political conflict is reframed as system failure. Dissent is no longer a legitimate expression but is treated as a statistical aberration.

The current risk does not stem from technological advancement, but from political retreat. The deeper threat lies in the progressive erosion of human judgment, the silencing of open debate, and the loss of uncertainty that gives substance to freedom. When security is elevated as an unquestionable priority, democratic principles begin to dissolve. In such circumstances, the effectiveness of the system no longer represents strength; it signals the end of deliberation and the closure of political possibility.

It is therefore urgent to adopt a firm position. Institutions must be reinforced. Privacy must be defended as a non-negotiable right. Legal limits must be imposed. All technology must be compatible with the principle of human dignity. Security is a legitimate public good, but without freedom, transparency, and space for difference, that security becomes coercion. And when coercion is normalized, the capacity to imagine and construct the future is annulled. Democracy cannot survive if it surrenders its right to error, to dissent, to change. Against boundless surveillance, the truest act of resistance is to continue choosing the uncertainty of liberty over the comfort of absolute control.

Authors' Declaration: The authors approve the final version of the article.

Conflict of Interest Statement: The authors declare no conflict of interest.

Contribución de los autores:

- Conceptualization: Diego Sebastián Sánchez Chumpitaz.
- Data Curation: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Formal Analysis: Diego Sebastián Sánchez Chumpitaz.
- Investigation: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Methodology: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Writing – Original Draft: Diego Sebastián Sánchez Chumpitaz.
- Writing – Review & Editing: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.

Funding: This study has been self-funded as part of an academic project at San Ignacio de Loyola University (Lima, Peru), with the objective of contributing to the analysis of international security, digital governance, and human rights in the global context.

BIBLIOGRAPHIC REFERENCES

国务院关于重组社会信用体系建设部际联席会议的批复 (Approval of the State Council on the Restructuring of the Interministerial Conference for the Development of the Social Credit System), Pub.

L. No. 国函〔2012〕88号, State Council of the People's Republic of China (2012). https://www.pkulaw.com/chl/558cf12828e9f4d4bdfb.html?isFromV5=1

Adeyeye, A. D., & Grobbelaar, S. S. (2024). Analysis of the functional dynamics of innovation for inclusive development systems: An event history analysis of the Nigerian growth enhancement support scheme. *Technology in Society*, *79*, 102716. https://doi.org/10.1016/j.techsoc.2024.102716

Amoore, L. (2020). *Cloud Ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.

Aoyama, R. (2022). Continuity or change? China's sweeping reforms under Xi Jinping. *Journal of Contemporary East Asia Studies*, *11* (2), 191–194. https://doi.org/10.1080/24761028.2023.2197387

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Bergdahl, J., Latikka, R., Celuch, M., Savolainen, I., Soares Mantere, E., Savela, N., & Oksanen, A. (2023). Self-determination and attitudes toward artificial intelligence: Cross-national and longitudinal perspectives. *Telematics and Informatics*, *82*. https://doi.org/10.1016/j.tele.2023.102013

Bonsón, E., Torres, L., Royo, S., & Flores, F. (2012). Local e-government 2.0: Social media and corporate transparency in municipalities. *Government Information Quarterly*, *29* (2), 123–132. https://doi.org/10.1016/j.giq.2011.10.001

Cancela-Outeda, C. (2024). The EU's AI act: A framework for collaborative governance. *Internet of Things. 27, 101291*. https://doi.org/10.1016/j.iot.2024.101291

Castellanos-Claramunt, J. (2023). Sobre los desafíos constitucionales ante el avance de la Inteligencia Artificial. Una perspectiva nacional y comparada. *Revista de Derecho Político*, *118*, 261–287. https://doi.org/10.5944/rdp.118.2023.39105

Chan, K. J. D., Papyshev, G., & Yarime, M. (2024). Balancing the tradeoff between regulation and innovation for artificial intelligence: An analysis of top-down command and control and bottom-up self-regulatory approaches. *Technology in Society*, *79*, 102747. https://doi.org/10.1016/j.techsoc.2024.102747

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

Ding, J. (2018). *Deciphering China's AI dream: the context, components, capabilities, and consequences of China's strategy to lead the world in AI.* Future of Humanity Institute, University of Oxford.

Drexel, B., & Kelley, H. (2023). *China is flirting with AI catastrophe: why accidents pose the biggest risk*. Foreign Affairs. https://www.foreignaffairs.com/china/china-flirting-ai-catastrophe

European Commission. (2021). *Proposal for a regulation of the European Parliament and of The Council. Laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Forno, R. (2024). What is Salt Typhoon? A security expert explains the chinese hackers and their attack on US Telecommunications Networks. *UMBC*. https://umbc.edu/stories/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks/

Gomes Rêgo de Almeida, P., & Dos Santos Júnior, C. D. (2025). Artificial intelligence governance: Understanding how public organizations implement it. *Government Information Quarterly*, *42* (1), 102003. https://doi.org/10.1016/j.giq.2024.102003

Goodman, B., & Flaxman, S. (2016). European union regulations on algorithmic decision making and a "right to explanation". *AI Magazine*, *38*(3), 50–57. https://doi.org/10.1609/aimag.v38i3.2741

Greitens, S. C., Lee, M., & Yazici, E. (2020). Counterterrorism and Preventive Repression: China's Changing Strategy in Xinjiang. *International Security*, *44* (3), 9–47. https://doi.org/10.1162/isec_a_00368

He, Q. (2023). The Integration of Outstanding Traditional Chinese Culture into English Language Teaching (中华优秀传统文化在英语教育中的融入). *Modern Education Forum (现代教育论坛)*, *3* (8). http://dx.doi.org/10.32629/mef.v3i8.2778

Knieps, G. (2024). Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing. *Telecommunications Policy*, *48* (10), 102867. https://doi.org/10.1016/j.telpol.2024.102867

Li, Y., Dai, J., & Cui, L. (2020). The impact of digital technologies on economic and environmental performance in the context of industry 4.0: A moderated mediation model. *International Journal of Production Economics*, *229*, 107777. https://doi.org/10.1016/j.ijpe.2020.107777

Mac Síthigh, D., & Siems, M. (2019). The Chinese Social Credit System: A Model for Other Countries? *The Modern Law Review*, *82* (6), 1034–1071. https://doi.org/10.1111/1468-2230.12462

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

Mozur, P., Kessel, J. M., & Chan, M. (24 abril 2019). Made in China, Exported to the World: The Surveillance State. *The New York Times.* https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Neuberger, A. (2025, enero 15). *Spy vs. AI: How Artificial Intelligence Will Remake Espionage*. Foreign Affairs. https://www.foreignaffairs.com/united-states/spy-vs-ai

Nguyen, V. Q., Lafrance, S., & Vu, T. C. (2023). China's social credit system: a challenge to human rights. *Revista de Direito, Estado e Telecomunicacoes*, *15* (2), 99–116. https://doi.org/10.26512/lstr.v15i2.44770

Oliveira, G. de L. T., Murton, G., Rippa, A., Harlan, T., & Yang, Y. (2020). China's Belt and Road Initiative: Views from the ground. *Political Geography*, *82*, 102225. https://doi.org/10.1016/j.polgeo.2020.102225

Pearson, M. M., Rithmire, M., & Tsai, K. S. (2022). China's Party-State Capitalism and International Backlash From Interdependence to Insecurity. *International Security*, *47* (2), 135–176. https://doi.org/10.1162/isec_a_00447

Reynoso Vanderhorst, H., Heesom, D., & Yenneti, K. (2024). Technological advancements and the vision of a meta smart twin city. *Technology in Society*, *79*, 102731. https://doi.org/10.1016/j.techsoc.2024.102731

Rocha Pino, M. J. (2017). Los proyectos de integración megarregional de China: el caso de la iniciativa Cinturón y Ruta (CYR). *Anuario Mexicano de Derecho Internacional*, *1* (17), 547-589. https://doi.org/10.22201/iij.24487872e.2017.17.11045

Sánchez Chumpitaz, D. S., & Asmat Caro, G. L. (2024). Inversión extranjera en inteligencia artificial para la seguridad en Perú: un análisis desde APEC 2024. *Política Internacional*, (136), 114–136. https://doi.org/10.61249/pi.vi136.173

Sandbrink, J. B., Hobbs, H., Swett, J. L., Dafoe, A., & Sandberg, A. (2024). Risk-sensitive innovation: leveraging interactions between technologies to navigate technology risks. *Science and Public Policy*, *51* (6), 1028-1041. https://doi.org/10.1093/scipol/scae043

Segal, A. (2025). *China Has Raised the Cyber Stakes: The "Salt Typhoon" Hack Revealed America's Profound Vulnerability*. Foreign Affairs. https://www.foreignaffairs.com/united-states/china-has-raised-cyber-stakes

Shum, N.-Y. E., & Lau, H.-P. B. (2024). Perils, power and promises: Latent profile analysis on the attitudes towards artificial intelligence (AI) among middle-aged and older adults in Hong Kong. *Computers in Human Behavior: Artificial Humans*, *2* (2), 100091. https://doi.org/10.1016/j.chbah.2024.100091

Skare, M., Gavurova, B., & Blažević Burić, S. (2024). Artificial intelligence and wealth inequality: A comprehensive empirical exploration of socioeconomic implications. *Technology in Society*, *79*, 102719. https://doi.org/10.1016/j.techsoc.2024.102719

Stanger, A., Kraus, J., Lim, W., Millman-Perlah, G., & Schroeder, M. (2024). Terra Incognita: The Governance of Artificial Intelligence in Global Perspective. *Annual Review of Political Science*, *27*, 445–465. https://doi.org/10.1146/annurev-polisci-041322-042247

Tuzov, V., & Lin, F. (2024). Two paths of balancing technology and ethics: A comparative study on AI governance in China and Germany. *Telecommunications Policy*, *48* (10), 102850. https://doi.org/10.1016/j.telpol.2024.102850

Vickers, E. (2022). Smothering Diversity: Patriotism in China's School Curriculum under Xi Jinping. *Journal of Genocide Research*, *24* (2), 158–170. https://doi.org/10.1080/14623528.2021.1968142

Wang, M. (2021). *China's Techno-authoritarianism has gone global: Washington needs to offer an alternative*. Foreign Affairs. https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global

Wright, N. (2018). *How Artificial Intelligence Will Reshape the Global Order: the coming competition between digital authoritarianism and liberal democracy*. Foreign Affairs. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order

Wu, R., Esposito, C., & Evans, J. (2024). *China's Rising Leadership in Global Science*. https://doi.org/10.48550/arXiv.2406.05917

Xi, J. (2014). *Xi Jinping: The Governance of China*. http://www.flp.com.cn

Yang, J., & Liu, W. (2024). Knowledge source switching under state interventions of latecomer regions: A case study of Shenzhen. *Technology in Society*, *79*, 102730. https://doi.org/10.1016/j.techsoc.2024.102730

Zeng, J., & Glaister, K. W. (2018). Value creation from big data: Looking inside the black box. *Strategic Organization*, *16*(2), 105–140. https://doi.org/10.1177/1476127017697510

Zhang, X., & Shaw, G. (2023). 'Becoming' a global leader: China's evolving official media discourse in Xi's New Era. *Global Media and Communication*, *19* (3), 313–333. https://doi.org/10.1177/17427665231209617

Zhu, Z., Cerina, F., Chessa, A., Caldarelli, G., & Riccaboni, M. (2014). The Rise of China in the International Trade Network: A Community Core Detection Approach. *PLOS One*, *9* (8), e105496 https://doi.org/10.1371/journal.pone.0105496

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