

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 Chumpitaz¹, Jorge Enrique Abarca Del Carpio¹

¹Universidad San Ignacio de Loyola, School of Law. Lima, Peru.

ABSTRACT

The People's Republic of China's (PRC) digital surveillance model, based on artificial intelligence (AI) and the social credit system (SCS), reshapes the balance between security and fundamental freedoms with global implications. This study examines its exportation and its impact on governance, international security, and human rights. A mixed-methods approach is employed, combining documentary analysis with quantitative data on the implementation of these technologies. The findings reveal the normalization of state surveillance, the consolidation of technological dependencies, and challenges for democratic stability. It is concluded that urgent international regulatory frameworks are needed to balance security with fundamental rights in the digital era. The rise of these systems raises questions about the future of privacy and individual autonomy, particularly in societies with weak institutional safeguards.

Palabras clave: International security; human rights; artificial intelligence; surveillance; internet governance; data protection

RESUMEN


El modelo de vigilancia digital de la República Popular China (RPC), basado en inteligencia artificial (IA) y el sistema de crédito social (SCS), redefine la relación entre seguridad y libertades fundamentales con implicancias globales. Este estudio analiza su exportación y su impacto en la gobernanza, la seguridad internacional y los derechos humanos. Se emplea un enfoque mixto, combinando análisis documental con datos cuantitativos sobre la implementación de estas tecnologías. Los resultados evidencian la normalización de la vigilancia estatal, la consolidación de dependencias tecnológicas y desafíos para la estabilidad democrática. Se concluye que es urgente establecer marcos regulatorios internacionales para equilibrar la seguridad con los derechos fundamentales en la era digital. El auge de estos sistemas plantea interrogantes sobre el futuro de la privacidad y la autonomía individual, especialmente en sociedades con instituciones frágiles.

Keywords: 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](https://doi.org/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 Sutti 
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

The People's Republic of China (PRC) has established an unprecedented digital surveillance infrastructure in recent history, emerging as the most sophisticated model of state control based on Artificial Intelligence (AI), Big Data, and the Social Credit System (SCS). With a population exceeding 1.4 billion, the Chinese Communist Party (CCP) has developed an apparatus that extends beyond optimizing security and domestic stability; it redefines the concept of governmental oversight on a global scale (Nguyen et al., 2023). The integration of technologies such as facial recognition, predictive analytics, and automated decision-making has enabled the state to manage social risks with unparalleled precision. However, this has led to a systematic restriction of individual freedoms (Vickers, 2022).

The issue transcends China's borders: Beijing exports its model to various countries through the Belt and Road Initiative (BRI), providing digital infrastructure and surveillance tools that have been adopted in contexts where democratic institutions are weak, or regimes seek to consolidate their control (Oliveira et al., 2020). This phenomenon, which could be described as an *authoritarian contagion process*, has allowed nations such as Venezuela, Iran, and Russia to implement similar mechanisms under the justification of ensuring national security (Greitens et al., 2020). As a result, there has been a gradual shift toward digital governance models where state surveillance is normalized, and individual autonomy is increasingly constrained (Segal, 2025).

The West is not immune to this trend. In the United States, the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA) have developed mass surveillance programs under the premise of counterterrorism and cybersecurity, demonstrating that the dilemma between liberty and control is not exclusive to authoritarian regimes (Feldstein, 2019). However, the key difference lies in institutional checks and the existence of legal frameworks that limit the political instrumentalization of digital surveillance (Cancela-Outeda, 2024). While surveillance in the PRC is institutionalized within the state apparatus, the European Union's *AI Act*¹ and other regulatory frameworks seek to establish transparency mechanisms in AI deployment, preventing its use as an indiscriminate tool of repression (Barredo Arrieta et al., 2020).

China's influence on global digital governance extends beyond technological infrastructure. It has also reshaped narratives concerning state power, security, and social stability, promoting a vision of technological development in which efficiency and control take precedence over individual freedoms (Castellanos-Claramunt, 2023; Zhang & Shaw, 2023). The legitimization of this model through official discourse has mitigated international criticism, reinforcing a framework in which surveillance is not only accepted but actively promoted as an imperative necessity in the digital era (Xi, 2014).

This study examines the expansion of Beijing's surveillance model and its impact on international security and human rights. Through the analysis of specific case studies and the technological architecture underpinning the system, this research will evaluate how its exportation is transforming global governance. Additionally, it will explore the implications of AI for geopolitical stability and the regulatory challenges faced by the international community in preventing the consolidation of digital authoritarianism.

FINDINGS

The PRC's surveillance model: foundations and evolution

The surveillance model developed by the PRC government has evolved rapidly, consolidating itself as a central component of its national security strategy and digital governance. It is not

¹ The *Artificial Intelligence Act* (AI Act) is a legislative proposal by the European Union that establishes a regulatory framework for the development, commercialization, and use of artificial intelligence systems within the European market. Its approach is based on risk classification, restricting applications that could infringe upon fundamental rights, such as mass biometric surveillance in public spaces. This regulation aims to ensure transparency, independent oversight, and adherence to ethical principles in the deployment of AI (European Commission, 2021).

merely a passive monitoring network but rather a control structure where AI, big data² analysis and the SCS converge to create an ecosystem of observation, evaluation, and regulation of citizen behavior. Its implementation serves both internal stability and the consolidation of the CCP's technological leadership in the digital era (Creemers, 2019; Feldstein, 2019).

State control in the PRC was initially based on community supervision networks organized at the neighborhood level. However, the economic modernization and rapid urbanization of the 1980s exposed the obsolescence of these rudimentary methods. The transition to a more advanced system became inevitable, particularly in a context where Deng Xiaoping's "**Reform and Opening**"³ (改革开放, *Gǎigé Kāifàng*), policy prioritized the modernization of state structures to maintain social stability amid unprecedented economic growth. The transformation of the surveillance model was embedded within this strategy of consolidating state control, at a time when China was beginning to position itself as a power in the digital revolution. Within this framework, in the early 2000s, the government implemented the "**Golden Shield**" project (金盾工程, *Jīndùn Gōngchéng*) internationally known as the "**Great Firewall of China**"⁴ (防火长城, *Fánghuǒ Chángchéng*). This system marked a turning point by enabling the regulation of digital traffic, restricting access to external content deemed detrimental to the regime's stability (Feldstein, 2019).

The introduction of AI in monitoring systems during the 2010s represented a paradigm shift. The SCS, implemented progressively, operates under a scoring scheme that classifies citizens based on their behavior in various areas, from commercial transactions to administrative records. These evaluations determine access to essential services, creating a social regulation mechanism where surveillance becomes a structural pillar of the state governance model (Greitens et al., 2020). Beyond individual control, the interconnection of facial recognition systems, government databases, and predictive algorithms has generated an environment where the distinction between public and private spheres becomes increasingly blurred.

From an economic perspective, the mass collection of data has strengthened the state's security apparatus while also generating value through the real-time analysis of vast amounts of information. Zeng & Glaister (2018) argue that the strategic use of big data does not solely depend on the volume of data collected but on the system's ability to process, contextualize, and convert it into actionable insights. In the PRC, this dynamic has been applied both in governmental planning and the development of control infrastructures, consolidating an ecosystem where information serves as the backbone of state decision-making.

The evolution of the PRC's surveillance system has followed a process of progressive sophistication, aligning with technological advancements and the state's strategic imperatives. From its origins in community-based supervision structures to the consolidation of a monitoring ecosystem driven by AI and big data, the apparatus has transitioned from decentralized surveillance to an interconnected digital infrastructure with predictive and regulatory capabilities. Table 1 synthesizes the key phases of this transformation, highlighting

² *Big data* refers to large and complex datasets that exceed the processing capacity of traditional tools, characterized by their volume, velocity, and variety. Its analysis enables the identification of real-time patterns for strategic decision-making (Mayer-Schönberger & Cukier, 2013).

³ "*Reform and Opening*" was the policy implemented by Deng Xiaoping in 1978, aimed at China's economic modernization through the liberalization of strategic sectors, the gradual opening to foreign trade, and the attraction of foreign investment. This process marked the country's transition from a planned economy to a market-oriented socialism model, driving unprecedented growth and solidifying the PRC as a global power.

⁴ The term "*Great Firewall of China*" (GFW) is a play on words derived from "*Great Wall of China*", establishing a symbolic parallel between the historical function of the Great Wall as a physical defensive barrier and the role of the GFW as a digital control infrastructure. The GFW regulates and monitors the flow of information in cyberspace, safeguarding the interests of the Chinese state against both external and internal influences.



the integration of advanced technologies and their impact on state governance. The analysis of this trajectory underscores the transition toward a model where mass surveillance and algorithmic regulation converge as fundamental pillars of social control, establishing a state surveillance framework with global reach.

Table 1. *The Evolution of the PRC's Surveillance Model*

Decade	Key Characteristics	Core Technologies	Impact on Society
1980s	Traditional community surveillance	Neighborhood networks, human oversight	Localized control, limited to small environments
1990s	Initial data digitization	Basic databases	Improved information collection
2000s	Implementation of the Golden Shield	Internet censorship, web traffic control	Restricted access to global information
2010s	Expansion of the Social Credit System	AI, big data, facial recognition	Real-time evaluation of citizen behavior
2020s	Exportation of the model and control sophistication	Algoritmos predictivos, ciberseguridad avanzada	Normalization of mass surveillance and international control

Source: Own elaboration based on Creemers (2019), Feldstein (2019), Greitens, Lee & Yazici (2020), and Mac Síthigh & Siems (2019).

The PRC's surveillance model has transcended its borders through the Belt and Road Initiative (BRI), promoting the adoption of monitoring technologies in countries with weak regulatory frameworks. This expansion has enabled the consolidation of supervision schemes that reinforce state control and reconfigure geopolitical balance (Mac Síthigh & Siems, 2019). In contexts with lower institutional capacity, the integration of these infrastructures has facilitated the strengthening of regimes with authoritarian tendencies.

The evolution of this model reveals a process of increasing sophistication, in which AI and predictive algorithms have transformed the relationship between security and fundamental rights. As these tools are integrated into different political systems, surveillance structures emerge that intensify the tension between the exercise of state sovereignty and the protection of individual freedoms. Digital monitoring, far from operating solely as a security mechanism, redefines state governance and challenges the strength of legal frameworks designed to guarantee privacy and autonomy in the digital era.

Artificial Intelligence (AI) and the Social Credit System (SCS) as pillars of Social Control

The Social Credit System (SCS) has evolved into a central mechanism within the PRC's digital governance apparatus, integrating surveillance, data analysis, and social discipline into a unified system. The sophistication of this model lies not only in its massive data collection capabilities but also in the state's ability to classify, predict, and condition citizen behavior based on "trustworthiness" parameters defined by the ruling structure (Nguyen et al., 2023). Unlike traditional control strategies, the SCS does not rely on direct coercion but instead operates through a system of *incentives and restrictions that encourage self-regulation*. This model creates an environment where adherence to norms is monitored in real time, affecting everyday life in an all-encompassing manner and minimizing individual autonomy outside state supervision.

The functioning of this system is based on a highly interconnected technological infrastructure. Real-time surveillance networks, facial recognition, and databases that record digital interactions and economic transactions enable systematic monitoring of social and financial activity⁵. The assignment of scores based on regulatory compliance and individual behavior

⁵ The continuous collection and analysis of data allow the state to evaluate citizens' behavior in real time across different spheres, from financial transactions to digital interactions and mobility history. This information is processed through

conditions access to essential services, such as transportation, housing, education, and medical assistance (Greitens et al., 2020). Consequently, citizens adjust their behavior based on the anticipation of rewards or sanctions, generating a logic of anticipatory social control⁶ that shifts classical surveillance toward an omnipresent model of algorithmic regulation (Wright, 2018). The impact of the SCS manifests in various aspects of daily life, creating a stark division between its perceived benefits and the costs in terms of fundamental rights. While some sectors defend its implementation, arguing that it enhances the efficiency of public service delivery and contributes to reducing minor crimes, concerns surrounding its application focus on the erosion of privacy, restrictions on freedom of expression, and the reinforcement of structural inequalities within the socioeconomic system (Drexel & Kelley, 2023). State surveillance, rather than being a mechanism confined to public security, has evolved into a tool that shapes citizens’ lives by conditioning access to opportunities and essential services.

SCS’s impact on society manifests across multiple dimensions, altering how individuals access fundamental goods and services. The following table 2 presents quantitative data on the positive and negative effects of the SCS on mobility, employment, and access to critical resources.

Table 2. *Impact of SCS on Society*

Evaluated Aspect	Positive Impact (%)	Negative Impact (%)
Freedom of mobility	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 loans	39.80	60.20

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

The expansion of the SCS has gone beyond the domestic sphere, solidifying itself as a replicable model in scenarios where state control is reinforced through digital tools. Wang (2021) argues that this proliferation is not limited to the transfer of technology but also introduces regulatory frameworks that prioritize regime stability over the protection of individual rights. The growing adoption of these infrastructures in national security systems presents challenges in managing sensitive data, increasing the risks of external interference, and altering the balance of power in cyberspace.

The accelerated development of digital surveillance infrastructures has created critical vulnerabilities in cybersecurity and geopolitics. Knieps (2024) warns that the expansion of interconnected networks for data collection and management increases the risk of cyberattacks, state espionage, and information manipulation. In this context, the instrumentalization of these systems has transcended domestic population control to become a tool with interstate implications. Segal (2025) documents how incidents like Operation “*Salt Typhoon*”⁷ illustrate that digital surveillance affects both individuals under state oversight and the strategic disputes between states, escalating the risk of geopolitical tensions.

Data from table 3 shows that the Middle East (69.8%) and Asia (61.5%) have the highest adoption rates of PRC-origin digital surveillance technology, whereas Africa (48.0%) and Latin America (43.5%) register more moderate integration. Eastern Europe (38.2%) has the lowest coverage, suggesting disparities in the incorporation of these systems depending on the

algorithms that assign trustworthiness scores, affecting access to essential services and regulating individuals’ participation in the economy and society.

⁶ Behavior monitoring is not limited to detecting past violations but is based on predictive algorithms that identify risk patterns before specific events occur. Through this analysis, the system can restrict freedoms or modify access to prevent regulatory deviations, establishing a governance mechanism rooted in the anticipation of potentially problematic behaviors.

⁷ *Salt Typhoon* refers to an Advanced Persistent Threat (APT) group linked to the PRC’s Ministry of State Security. This collective specializes in cyber-espionage operations, particularly in infiltrating telecommunications networks in the United States, aiming to intercept sensitive communications and obtain strategic intelligence information (Forno, 2024).



geopolitical context and regulatory frameworks in each region. The expansion of these technological infrastructures is driven by cooperation agreements, while simultaneously evidencing the consolidation of digital supervision strategies used as state control tools. The comparative analysis between Table 2 and Table 3 confirms a correlation between the expansion of these technologies and the intensification of restrictions on fundamental rights. Regions with higher coverage, such as the Middle East and Asia, report the highest levels of limitations on mobility, access to economic opportunities, and citizen autonomy. This phenomenon goes beyond security justifications and is embedded within a *global control architecture*⁸, where access to information and services is subject to systematic monitoring systems (Segal, 2025).

Table 3. *Global Distribution of PRC Digital Surveillance Technology*

Region	Number of Countries using 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)

Technology, far from being neutral, has been strategically employed to reinforce power structures through **predictive regulation of social behavior**. Within SCS, adherence to norms does not emerge from a deliberative consensus but rather results from a conditioning process in which algorithmic systems anticipate behavioral patterns and limit individual action **before it occurs** (Neuberger, 2025; Wright, 2018). In this scenario, the Chinese supervision model does not merely respond to infractions but operates under a logic of *proactive prevention and restriction*⁹.

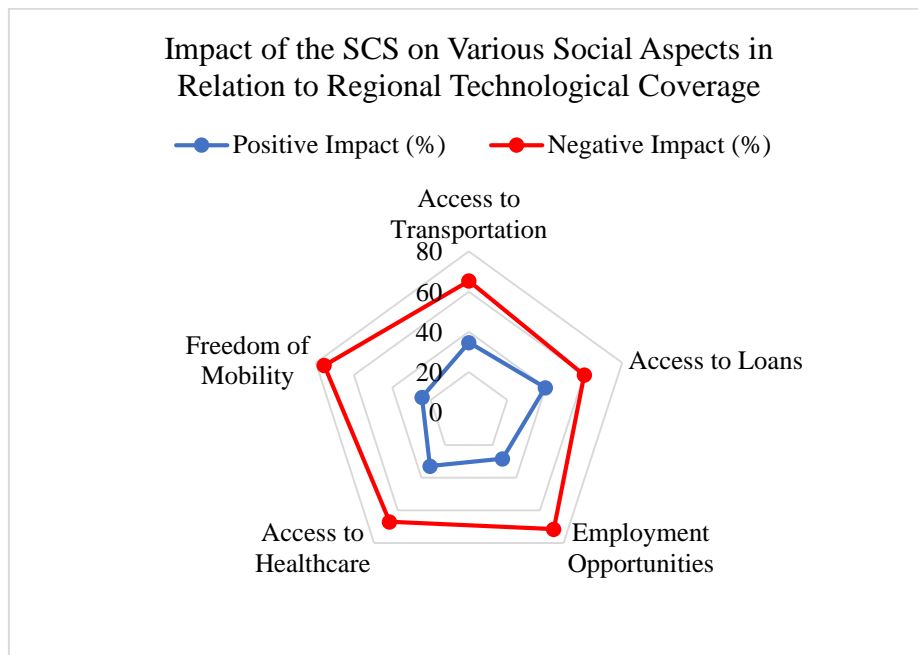
The dissemination of these technologies outside the PRC is not limited to the transfer of surveillance software and hardware but also entails the adoption of governance frameworks that reinforce large-scale *digital control structures*. Wang (2021) argues that this phenomenon has accelerated the institutionalization of authoritarian systems under the pretext of ensuring security and stability, thereby obstructing the consolidation of democratic regimes and creating structural barriers that hinder transparency and accountability. The expansion of the SCS has transcended the national sphere and has been adopted in various political contexts, establishing itself as a replicable model of digital state control.

The expansion of SCS has generated significant impacts across multiple social dimensions, solidifying itself as a structural pillar of digital control. Figure 1 illustrates how this system affects mobility, access to employment, and the availability of essential services. Data analysis reveals that negative impacts far exceed perceived benefits. In terms of loan accessibility, 60.2% of respondent's experience restrictions, while mobility limitations affect 75.5%. Algorithmic supervision not only regulates individual behavior but also establishes criteria that determine access to economic and social opportunities (Nguyen et al., 2023; Segal, 2025).

⁸ This term refers to the consolidation of a transnational digital surveillance framework, where data collection, processing, and usage are not confined within national borders but are integrated into interoperable systems that enable coordinated monitoring of individuals at an interstate level. This phenomenon has been facilitated by the convergence of AI, big data, and advanced telecommunications networks, raising concerns over digital sovereignty and individual autonomy in the era of hyperconnectivity (Zuboff, 2019).

⁹ In the SCS context, this implies the implementation of predictive systems that, beyond identifying potentially problematic behaviors, apply preemptive restrictions to prevent their occurrence. This approach is based on machine learning techniques and algorithmic risk modeling, aligning with pre-crime governance strategies—a paradigm that shifts the state's traditional role from punishing committed offenses to regulating probabilistic behavioral outcomes (Amoore, 2020).

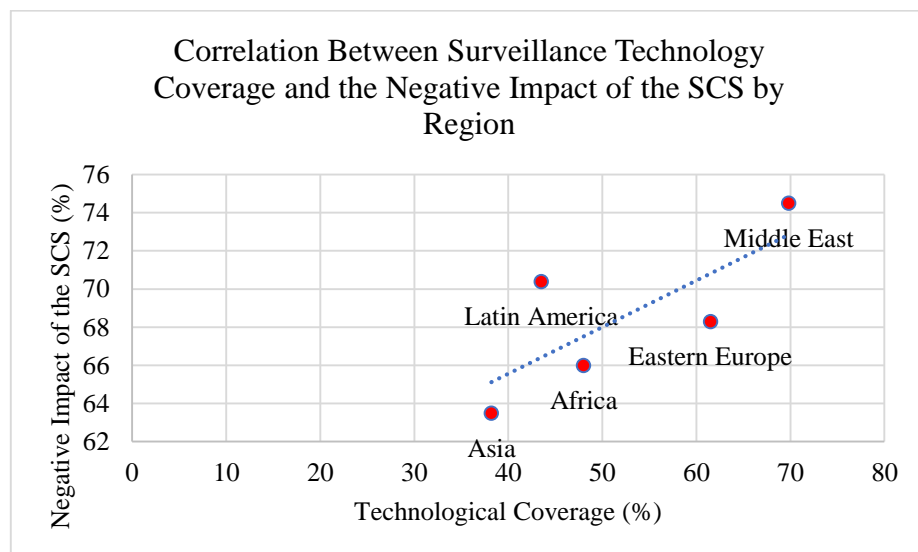
Figure 1. *Impact of the SCS on Different Social Aspects in Relation to Regional Technological Coverage*



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

The correlation between SCS technological coverage and the increase in restrictions on fundamental rights is reflected in figure 2. The Middle East and Asia, with penetration levels of 69.8% and 61.5%, respectively, exhibit the highest levels of restrictions. Latin America, with lower technological penetration (43.5%), still registers significant negative impacts, indicating that the effect of the SCS depends not only on the presence of technology but also on the preexisting regulatory frameworks. The global control architecture configured by this model is structured based on the state’s ability to integrate surveillance mechanisms into its governance structures.

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

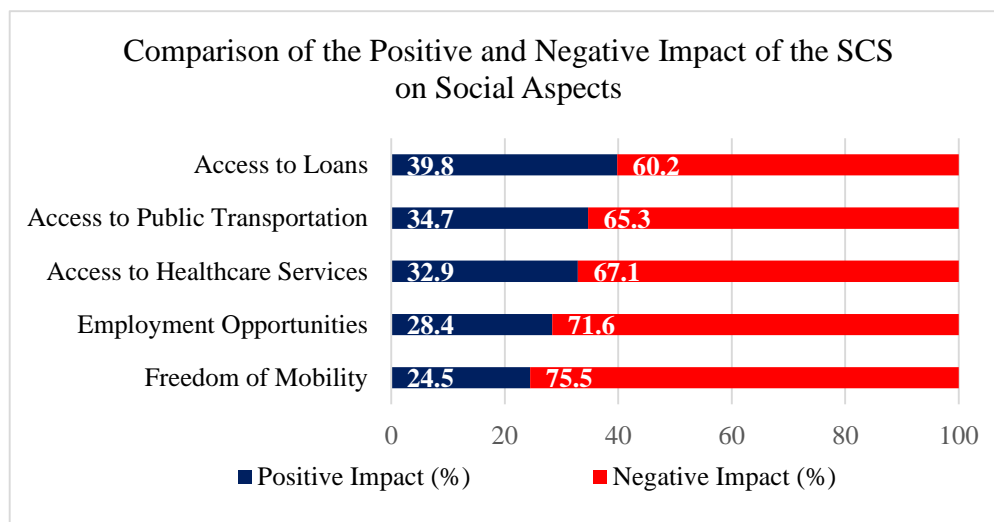


Source: Own elaboration based on Nguyen et al. (2023) and Segal (2025)

Figure 3 reinforces this trend by comparing the positive and negative impact of SCS across different domains. The data show that mobility and access to employment are the areas most affected, with restrictions reaching 75.5% and 71.6%, respectively. Skare et al. (2024) warn that the adoption of these mechanisms in economies with structural inequalities tends to

reinforce models of social exclusion, limiting economic mobility and strengthening digital stratification systems. As SCS expands beyond the PRC, its impact intensifies in emerging markets, where the lack of regulation facilitates the normalization of these control schemes.

Figure 3. Comparison of the Positive and Negative Impact of the SCS on Different Social Aspects



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

The growth of this technological infrastructure is not limited to national surveillance but is linked to a normative diffusion process that strengthens governance models based on digital surveillance. Wang (2021) argues that the exportation of these technologies promotes the institutionalization of authoritarian systems under the pretext of ensuring security and stability, making it more difficult to consolidate democratic regimes and hindering transparency and accountability. This dynamic has reinforced the technological dependence of recipient states, encouraging the adoption of restrictive regulatory frameworks that establish surveillance as an essential component of the state apparatus.

The phenomenon known as *authoritarian contagion* is evident in the gradual incorporation of these systems into government oversight structures. The expansion of monitoring technologies in emerging markets is not limited to the transfer of surveillance hardware and software but also promotes a governance model where the automation of social control is framed as a mechanism to optimize state efficiency. Drexel & Kelley (2023) y Neuberger (2025) warn that the lack of supranational regulations to curb the proliferation of these systems could accelerate the structural erosion of fundamental rights, weakening democratic principles and fostering the consolidation of automated surveillance systems.

The exportation of the Chinese model: implications for Global Governance

The Chinese model of digital governance has become an instrument of power projection beyond its borders, consolidating itself as an expansion scheme that integrates advanced technological infrastructure, investment strategies, and capacity transfers in markets with more flexible regulatory frameworks. The convergence of AI, big data, and surveillance systems is not confined to the domestic sphere but is deployed through strategic agreements that reinforce technological dependence and strengthen China's normative influence in global cyberspace (Zhu et al., 2014).

The analysis of the penetration of these infrastructures reveals a clear trend: countries with lower technological regulatory capacity have been the most receptive to the implementation of these systems. According to Wu et al. (2024), the exportation of advanced technological solutions by the PRC has grown by more than 60% over the past decade, consolidating its leadership in the digital transformation of various emerging economies. The following table (table 4) synthesizes the main mechanisms through which the PRC expands its digital control model:

Table 4. *Mechanisms for Exporting the Chinese Digital Governance Model*

Export Mechanism	Description
Investment in digital infrastructure	Financing and construction of 5G networks, video surveillance systems, and data platforms in developing countries.
Technology transfer	Provision of surveillance software, facial recognition systems, and social credit platforms to other governments.
Cybersecurity cooperation	Bilateral agreements with allied nations to share digital control technologies and data analysis capabilities.
Expansion of state-owned enterprises	Huawei, ZTE, and other Chinese companies as key players in the deployment of global technological networks.
Exportation of regulatory standards	Digital control and surveillance models are integrated into the legal systems of recipient countries.

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

The impact of this expansion is most pronounced in regions where economic and technological dependence on the PRC is significant. Latin America has become a strategic focal point within this dynamic, with megaprojects such as the Chancay port, which, in addition to strengthening bilateral trade, drive the penetration of digital solutions into public infrastructure (Sánchez Chumpitaz & Asmat Caro, 2024). Table 5 presents quantitative data on Xi Jinping’s China’s technological presence in various regions and its relationship with the adoption of digital control models.

Table 5. *Penetration of Chinese Technologies and Adoption of Digital Control Models by Region*

Region	Presence of Chinese Technology (%)	Implementation of Control Models (%)
Latin America	47.30	38.90
Africa	52.60	42.10
Central Asia	68.50	59.30
Middle East	73.20	65.70
Eastern Europe	49.70	41.40

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

The correlation between Chinese technological presence and the adoption of digital surveillance systems reveals a consistent pattern: the incorporation of these infrastructures is not limited to the provision of hardware and software but also involves the assimilation of regulatory principles that consolidate governance models with higher levels of state oversight (Li et al., 2020). Chan et al. (2024) argue that technological dependence facilitates the transfer of capabilities and introduces regulatory frameworks that, in practice, reduce recipient states' autonomy in establishing independent policies on digital governance.

The expansion of the Chinese digital governance model has integrated technological platforms designed to optimize government management, with applications in public security, urban planning, and state administration (Bonsón et al., 2012). These infrastructures have been adopted across various countries, enhancing real-time data processing and surveillance capabilities. Table 6 presents a set of digital governance platforms exported by China and their functions in recipient states, illustrating the integration of AI-based solutions and mass surveillance into administrative and state control frameworks.

Table 6. *Digital Governance Platforms Exported by China*

Platform	Function in Recipient Country
SCS	Evaluation of citizen behavior to determine access to government benefits.
Skynet	Mass video surveillance network with integrated facial recognition.
ZTE Smart City	Urban management system based on real-time data analysis.
Huawei Cloud	Infrastructure for storing and processing government data.
Safe City	AI-based security system for crime prevention.

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

The impact of China’s influence on global governance can be analyzed from an economic perspective, particularly in logistics optimization and administration through artificial intelligence. Digital automation has reconfigured supply chains across various sectors, enhancing operational efficiency in ports and international trade networks (Sánchez Chumpitaz & Asmat Caro, 2024). Table 7 details these impacts in terms of cost reductions and processing time improvements across different sectors.

Table 7. *Impact of Chinese Digital Automation on Logistics and International Trade*

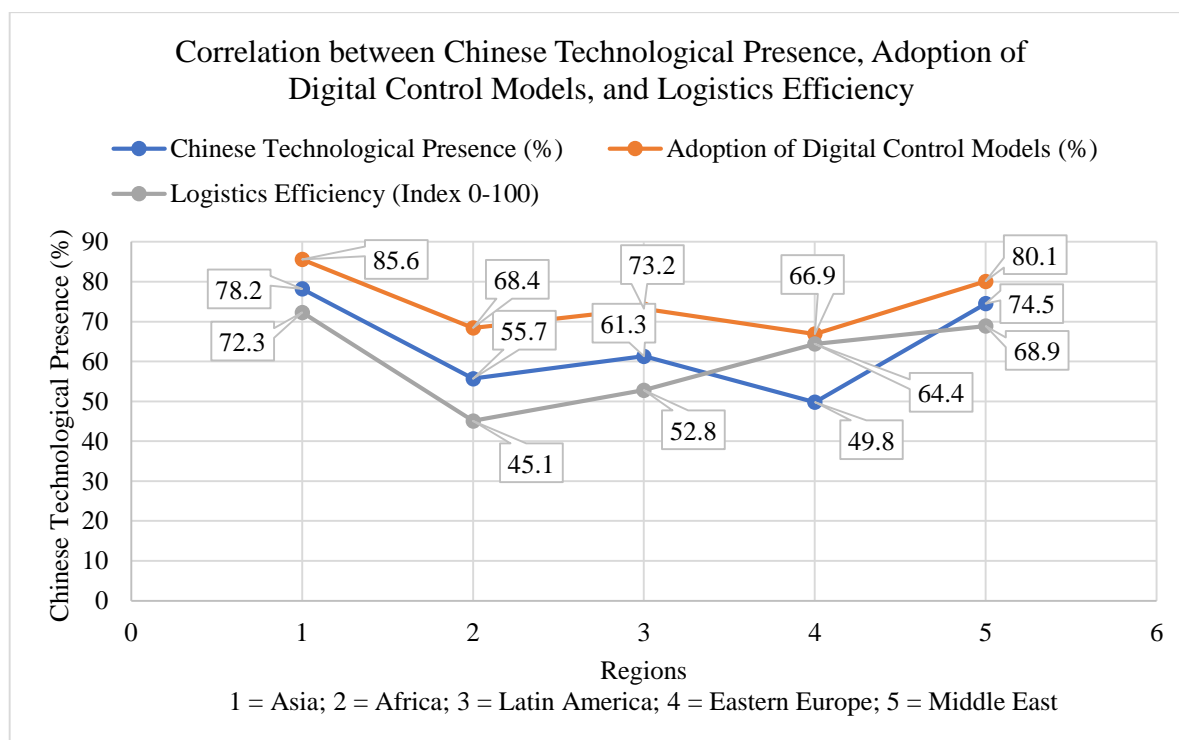
Sector	Cost Reduction (%)	Processing Time Reduction (%)
Maritime Transport	24.50	36.80
Port Logistics	30.20	42.10
E-commerce	28.70	40.50
Customs Administration	22.30	33.60

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

The exportation of the Chinese digital governance model is not merely a technological transfer process but involves a reconfiguration of the regulatory and structural principles of recipient countries. Through infrastructure investment, process standardization, and regulatory model adaptation, China has consolidated its position as a central actor in global digital transformation.

Figure 4 illustrates the relationship between Chinese technological presence, the adoption of digital control models, and their effect on logistical and commercial efficiency in recipient countries, highlighting patterns of integration and optimization across various geopolitical contexts.

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)

Digital Surveillance and the reconfiguration of the International Order: Security, Human Rights, and Strategic Challenges in the Age of Technological Authoritarianism

The evolution of digital surveillance has transformed the balance of power in the international system, reshaping the relationship between the state and its citizens, redefining security

perceptions, and consolidating new paradigms of authoritarian governance. The interconnection of AI, big data, and mass monitoring has enabled governments to manage social behavior on an unprecedented scale, blurring the boundaries between protection and the restriction of rights.

In the PRC, the state surveillance model has expanded under Xi Jinping's political stability doctrine, reinforcing the concept of security as a pillar of national development (Xi, 2014). The SCS and the Skynet video surveillance network consolidate a permanent monitoring infrastructure that conditions mobility and access to goods and services based on the level of trustworthiness assigned to each citizen (Nguyen et al., 2023). Surveillance is no longer solely reactive but operates as a predictive mechanism based on algorithmic regulation.

Sandbrink et al. (2024) warn that the convergence of emerging technologies with state control systems has strengthened anticipatory supervision frameworks, which limit individual autonomy and expand governmental intervention capabilities. The implementation of these models in political systems with low accountability reinforces the trend toward digital authoritarianism. Adeyeye & Grobbelaar (2024) emphasize that the consolidation of monitoring infrastructures in countries with institutional weaknesses not only optimizes state control but also transforms the very structure of governance, shifting decision-making to automated mechanisms that reshape power dynamics.

The Chinese model has expanded through the Belt and Road Initiative (BRI), facilitating the adoption of surveillance technology in states with institutional weaknesses or authoritarian tendencies (Rocha Pino, 2017). Governments such as those of Venezuela, Iran, Russia, and Saudi Arabia have integrated these digital infrastructures to strengthen social control, restrict access to information, and suppress dissent through reinforced state supervision mechanisms (Mozur et al., 2019).

Empirical analysis of these dynamics shows that states with greater implementation of digital surveillance technology tend to report higher perceptions of security. In table 8, the PRC, with 100% use of Chinese technology, reports a security perception of 85.4%, while countries such as Venezuela and Iran, with lower levels of technological adoption (79% and 76%, respectively), present lower values in this perception. These data suggest that digital surveillance is perceived as a stability factor, although its actual impact on security and citizens' rights remains a subject of debate.

Table 8. *Use of Chinese Surveillance Technology and Security Perception*

Country	Use of Chinese Technology (%)	Security Perception (%)
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: Own elaboration based on Mozur et al. (2019) and Wright (2018).

Although the adoption of Chinese surveillance technology is linked to a high perception of security due to continuous population monitoring, its implementation also entails adverse effects on human rights and individual freedoms. Table 9 shows that countries with high levels of digital surveillance experience significant restrictions on freedom of expression and privacy. In the PRC, where 92.3% of the population faces limitations on freedom of expression and 94.8% on privacy, over 135,000 cases of political repression have been documented in the last five years. Similar trends are observed in Venezuela, Iran, and Saudi Arabia, where censorship and social control rates are high. These data indicate that digital surveillance, although perceived as a security mechanism, functions as a state supervision tool that affects the exercise of fundamental rights.

Table 9. *Impact of Digital Surveillance on Freedom of Expression and Privacy*

Country	Restriction on Freedom of Expression (%)	Restriction on 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

Source: Own elaboration based on Greitens et al. (2020) and Feldstein (2019)

The digital surveillance models analyzed in table 10 show that, while they are presented as security and stability mechanisms, their implementation has been marked by social control, censorship, and political repression. In the PRC, the SCS and Skynet operate as mass supervision tools, while in Venezuela, Iran, Saudi Arabia, and Russia, systems such as the Carnet de la Patria, content filtering, and communications interception have been used to monitor citizens and restrict access to information.

The combined analysis with table 8 and table 9 reveals that the presence of surveillance technology is associated with a high perception of security, although it also entails significant restrictions on fundamental rights. In the PRC, where digital monitoring reaches 100%, perceived security stands at 85.4%, yet freedom of expression and privacy are affected by 92.3% and 94.8%, respectively, with over 135,000 documented cases of political repression. Similar patterns are observed in Venezuela, Iran, and Saudi Arabia, confirming that state surveillance is not solely limited to security but also establishes a supervision ecosystem that conditions the exercise of citizens' rights.

Table 10. *Digital Surveillance Models and Their Objectives*

Country	Adopted Surveillance Model	Declared Objective	Documented Use
PRC	Social Credit System, Skynet	National security and stability	Population control through mass digital surveillance
Venezuela	<i>Carnet de la Patria</i> , digital censorship	Economic and social control	Monitoring and limiting access to services based on political loyalty
Iran	National intranet, content filtering	Protection of Islamic values	Censorship and restriction of access to dissident information
Saudi Arabia	Facial recognition algorithms, forensic biometrics	Terrorism prevention	Tracking and control of opposition groups and activists
Russia	SORM (Communications Interception System)	Cybersecurity	Network monitoring and political repression

Source: Own elaboration based on Mozur et al. (2019) and Nguyen et al. (2023).

Table 11 highlights the relationship between the use of surveillance technologies and the restriction of freedoms, demonstrating how these systems reinforce state control. The PRC, with 100% adoption, has the highest level of restrictions (94.8%), consolidating its digital supervision model. Venezuela and Iran, with rates of 79% and 76%, show restrictions above 87%, indicating that these mechanisms extend beyond security and impact the political and social sphere. Stanger et al. (2024) note that the expansion of these infrastructures tends to strengthen more restrictive regulatory frameworks, limiting individual autonomy. Nigeria, with lower adoption (55%), maintains significant restrictions (74.5%), suggesting that the impact of surveillance depends not only on its scope but also on the regulatory context. Ding et al. (2018) emphasize that these systems reshape state power, where access to surveillance tools reinforces control dynamics with effects that transcend security.



Table 11. Comparison of Population, Surveillance Technology Use, and Restriction of Freedoms in Countries with Digital Monitoring Models.

Country	Population (Millions)	Use of Surveillance Technology (%)	Restriction of Freedoms (%)
PRC	1,410	100.00	94.80
Venezuela	28	79.00	87.20
Iran	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: Own elaboration based on Stanger et al. (2024) and Ding (2018)

The development and expansion of these monitoring systems have created the need to measure their impact on governance and the relationship between security, surveillance, and restrictions on rights. To this end, the *State Control Index* (SCI or I_c), has been designed as a tool to model this interaction in regimes with intensive supervision. Its mathematical formulation allows for the analysis of how perceived security contributes to state legitimacy, while the increase in digital surveillance and restrictions on freedoms implies political costs that may influence regime stability.

SCI quantifies the relationship between perceived security (S), digital surveillance (V) and restrictions on freedoms (F) in regimes with intensive supervision systems. The PRC has developed a model based on AI and big data, which has become a reference for states with authoritarian tendencies and has expanded through the Belt and Road Initiative (Nguyen et al., 2023; Rocha Pino, 2017).

The mathematical formulation of SCI seeks to quantify the interaction between perceived security, digital surveillance, and restrictions on freedoms in regimes with intensive supervision. A higher perception of security tends to legitimize state control, while the extent of digital surveillance determines the state’s capacity to regulate citizen behavior. In contrast, increasing restrictions on freedoms generates political costs that may affect regime stability. To model this dynamic and provide an analytical framework for its study, the following equation is proposed:

$$I_c = (\alpha \times S) + (\beta \times V) - (\gamma \times F)$$

The coefficients α , β and γ have been calibrated based on comparative studies across multiple countries. In this model, α (*alpha*) weighs perceived security, as trust in the state facilitates its capacity for control. Then, β (*beta*) measures the impact of digital surveillance on the consolidation of state power. Meanwhile, γ (*gamma*) quantifies the political wear caused by repression, as high levels of restrictions can erode legitimacy and generate social opposition (Mozur et al., 2019).

To evaluate the application of SCI, the cases of the **PRC** and **Nigeria** were analyzed, two states with different degrees of digital control consolidation. In the case of the **PRC**, empirical values reflect a high perception of security ($S = 85.4$), a fully integrated digital surveillance system ($V = 100$) and severe restrictions on freedoms ($F = 94.8$). With adjusted coefficients of $\alpha = 0.8$, $\beta = 1.2$ y $\gamma = 1.5$, the following is obtained:

$$I_c = (0.8 \times 85.4) + (1.2 \times 100) - (1.5 \times 94.8)$$

$$I_c = 68.32 + 120 - 142.2$$

$$I_c = 46.12$$

The findings confirm that the **PRC** maintains a high SCI, demonstrating the efficiency of its surveillance infrastructure in ensuring political stability and consolidating the CCP’s dominance. The integration of the SCS and the Skynet video surveillance network has strengthened the government’s ability to monitor citizen behavior and shape it through algorithmic incentive and sanction systems (Nguyen et al., 2023; Xi, 2014). The institutionalization of this framework has been supported by regulatory measures promoted by the *State Council of the PRC* (2012), establishing a legal framework that legitimizes the use of



surveillance technologies to restrict access to services and consolidate a highly centralized digital governance model.

On the other hand, **Nigeria's** adoption of surveillance infrastructure funded by the **PRC** has been partial, with lower technological consolidation. The data reflect a low perception of security ($S = 58.4$), a moderate level of surveillance ($V = 55$) and significant restrictions on freedoms ($F = 74.5$). Applying the equation with the same coefficients:

$$I_c = (0.8 \times 58.5) + (1.2 \times 55) - (1.5 \times 74.5)$$

$$I_c = 46.8 + 66 - 111.75$$

$$I_c = 1.05$$

The *SCI* for Nigeria is 1.05, reflecting weak state control despite the partial implementation of digital surveillance funded by Beijing. The low perception of security and lack of social legitimacy have hindered the consolidation of an effective model (Feldstein, 2019). In contrast, the PRC presents an *SCI* of 46.12, demonstrating the effectiveness of its surveillance infrastructure, based on SCS and Skynet, in strengthening political stability and reinforcing government control (Nguyen et al., 2023; Xi, 2014).

The comparison between both countries reveals a substantial difference in digital surveillance management. While in the PRC, the combination of AI, predictive analysis, and supervision mechanisms has enabled a highly consolidated state control model, Nigeria, with a security perception of 58.4, a surveillance level of 55, and freedom restrictions of 74.5, has failed to establish a similar control structure. The absence of a robust technological infrastructure and the lack of cohesion in its supervision policies have hindered the projection of state authority through these systems (Feldstein, 2019).

Beyond Nigeria's specific case, the expansion of digital monitoring models presents a geopolitical challenge, where technological supremacy emerges as a new factor in state dominance competition. As more countries adopt control frameworks based on AI and predictive algorithms, the dispute over information will intensify, shaping a scenario where the line between security and oppression becomes increasingly blurred.

Considerations for the design of International Regulatory Frameworks

The rapid expansion of AI and digital surveillance infrastructures has underscored the urgency of developing international regulatory frameworks that establish clear limits on their implementation and prevent their use for authoritarian purposes. The absence of a coherent global regulatory framework has allowed some states to structure supervision models based on advanced technologies, prioritizing state control over citizen security and data protection. This has facilitated the consolidation of mass surveillance regimes with direct implications for human rights and the stability of the international system (Ding, 2018; Stanger et al., 2024).

The concentration of digital power in the PRC has turned its governance model into a reference for governments seeking to strengthen their supervision mechanisms and information management systems. This trend has fueled a debate on the need for regulations that reconcile technological advancement with the protection of fundamental freedoms, preventing the expansion of AI from resulting in tools of political repression and large-scale social control (Pearson et al., 2022).

The GDPR in the European Union and the Federal Privacy Law in the United States have sought to establish regulatory frameworks to restrict the abusive use of digital surveillance and mass data exploitation. However, these efforts present limitations, as they do not comprehensively address the implications of AI in both the public and private spheres (Goodman & Flaxman, 2016).

In contrast, the PRC has developed regulations that reinforce state control over information flows and online activity, consolidating a model replicated in states with authoritarian tendencies such as Iran, Venezuela, and the Russian Federation (Aoyama, 2022; Vickers, 2022). Table 12 presents a comparison between different jurisdictions, highlighting the gap

between privacy-oriented regulations and those designed to strengthen government supervision.

Table 12. *Comparison of Regulatory Frameworks on Privacy and State Control*

Country/Region	Key Regulation	Approach	Use of AI in Surveillance
European Union	GDPR (Regulation EU 2016/679)	Data protection and individual rights	Limited to public security with restrictions
United States of America	Federal Privacy Law	Sectoral data protection	Applications in cybersecurity and crime prevention
PRC	Data Security Law, Cybersecurity Law	Control of information flows and state surveillance	Extensive: AI applied in social credit systems and facial recognition
Russian Federation	Yarovaya Law, SORM System	State supervision and communication control	Mass monitoring with support from predictive algorithms
Venezuela	<i>Carnet de la Patria</i> and digital censorship	Socioeconomic control and censorship	Emerging implementation with support from Chinese infrastructure

Source: Own elaboration based on Goodman & Flaxman (2016), Vickers (2022) and Pearson et al. (2022)

The regulatory frameworks adopted by states determine the degree of governmental supervision and redefine the level of digital autonomy and citizen participation in the public sphere (He, 2023). In the PRC, technological control has converged with educational policy, facilitating the homogenization of discourse and the elimination of narratives contrary to the CCP (Vickers, 2022). This dynamic has extended to governments that have received technological assistance from Beijing through the BRI, integrating surveillance mechanisms into their governance models (Oliveira et al., 2020). The strategic use of education as a vehicle for ideological control has strengthened the regime's internal cohesion and consolidated its influence over the national socio-political structure (Aoyama, 2022). In environments with weaker regulatory capacity, this combination of digital supervision and discourse standardization creates an ecosystem conducive to the replication of systemic surveillance models with minimal institutional resistance.

From a global governance perspective, AI regulation must consider the risks associated with its instrumentalization for authoritarian purposes. International organizations have emphasized the urgency of establishing regulatory frameworks that balance innovation with the protection of fundamental rights (Gomes Rêgo de Almeida & Dos Santos Júnior, 2025). Table 13 presents a comparison of regulatory approaches in the public and private sectors, highlighting the projection of the Chinese model in environments with weaker democratic foundations.

Table 13. *Regulatory Strategies for AI in the Public and Private Sectors*

Aspect	Democratic Approach	Authoritarian Approach
AI Governance	Based on transparency and public auditing	State control without independent oversight.
Data Access	Regulation to protect individual privacy	Centralization and unrestricted state access.
Use in Education	Applications for personalized learning	Ideological instrumentalization and homogenization.
Corporate Supervision	Regulation to prevent bias and monopolies	Integration of corporations with the state apparatus.

Source: Own elaboration based on Stanger et al. (2024) and Ding (2018)

The design of global regulatory frameworks must consider the need for supranational supervision to prevent AI from becoming an unrestricted surveillance tool. Technological governance cannot be subjected to fragmented national regulations; rather, it requires multilateral mechanisms that ensure transparency, accountability, and the protection of fundamental rights (Stanger et al., 2024). The recent UN proposal to establish an international AI oversight body represents a step in this direction, although its implementation faces obstacles due to resistance from states with centralized governance models (Ding, 2018).



The geopolitical dimension of technological regulation is unavoidable. The concentration of digital infrastructures in the hands of state actors with expansionist agendas has created power asymmetries in the international system. The dependence on platforms of Chinese or American origin has turned access to information into a tool of strategic influence, with direct implications for global security and stability (Pearson et al., 2022).

The development of international regulatory standards must prevent the consolidation of technological monopolies and curb the expansion of models that use AI as a tool for repression and mass surveillance. An effective regulatory framework must guarantee the protection of privacy and digital autonomy while establishing mechanisms to counteract algorithmic censorship and implement independent audits that mitigate the risks associated with the concentration of technological power. The ability of the international community to address these challenges will determine the future balance between technological advancement and respect for fundamental rights in an increasingly automated world.

The consolidation of AI-based digital surveillance models has intensified the state's ability to shape social behavior, generating new control dynamics that extend beyond public security. In the PRC, tools such as Skynet and SCS have been used to condition mobility, restrict access to services, and establish social scoring systems that reinforce citizen compliance (Bergdahl et al., 2023; Shum & Lau, 2024). This strategy has expanded through the Belt and Road Initiative, facilitating the adoption of monitoring infrastructures in environments with weak regulations, where Chinese technology has been instrumentalized to consolidate authoritarian regimes (Mozur et al., 2019; Tuzov & Lin, 2024).

In contrast, democratic states have implemented regulatory frameworks with divergent approaches. While the EU has developed regulations such as the AI Act to mitigate risks associated with automation, other jurisdictions have allowed the expansion of digital surveillance under the pretext of cybersecurity and counterterrorism efforts (Cancela-Outeda, 2024; Goodman & Flaxman, 2016). However, the absence of international standards prevents effective regulation, paving the way for the proliferation of unrestricted supervision systems and the consolidation of technological monopolies with defined political agendas. In light of this scenario, AI governance must prioritize transparency, independent oversight, and the protection of digital autonomy, preventing technological advancements from becoming a global instrument of repression (Reynoso Vanderhorst et al., 2024). Additionally, the evolution of supervision models in China demonstrates how state intervention has been a determining factor in transforming its digital ecosystem, turning mass data collection into a pillar of its development strategy and consolidating its technological influence on a global scale (Yang & Liu, 2024).

CONCLUSIONS

Digital surveillance in the PRC has transcended traditional state supervision. It has consolidated into an omnipresent structure where AI, big data, and the SCS have shaped an unprecedented ecosystem of control. Every interaction, transaction, and movement is recorded in a system that not only observes but also predicts, classifies, and sanctions. Security and political stability have been the rhetorical pillars justifying the expansion of this model. However, the question remains: is a society of this scale viable without advanced supervision mechanisms, or is the price of such order the complete erosion of individual autonomy?

The impact of this paradigm has extended beyond China's borders. States with authoritarian regimes have integrated these infrastructures under the pretext of strengthening national security. Venezuela, Iran, Russia, Saudi Arabia. The implementation of these systems has revealed their true purpose. They do not enhance public security. They do not guarantee stability. Instead, they establish a permanent surveillance architecture designed to control dissent, restrict access to information, and perpetuate regimes with questionable legitimacy. The perception of security in these countries has increased, but at the cost of systematic censorship, mobility restrictions, and the progressive elimination of public space as an environment free from state monitoring.



The dilemma is not exclusive to authoritarian regimes. Liberal democracies face their own contradiction. In the name of counterterrorism and cybersecurity, mass surveillance has been adopted without resistance by agencies such as the NSA, the FBI, or the CIA. Programs like PRISM have exposed the extent of this intrusion into citizens' privacy. The European Union has responded with regulatory frameworks such as the *AI Act*, establishing risk mitigation mechanisms and algorithmic transparency. The fundamental difference with the PRC lies in the existence of institutional checks and balances. However, how effective are these limits? How long before does security takes precedence over civil liberties in societies that today perceive themselves as democratic?

Stability has been used as a justification for sacrificing the right to privacy. In mainland China, the expansion of digital surveillance has eliminated any notion of anonymity. Systems like Skynet and the SCS do not merely monitor; they constitute a model of social engineering where individual behavior is regulated through algorithms that determine who can access services, who is deemed trustworthy, and who becomes a digital outcast. AI has enhanced the capacity of the Chinese state and the power of Xi Jinping to shape behaviors. It has introduced a system of incentives and sanctions that reinforce obedience, discourages political participation, and structures daily life according to state-assigned scores. What began as a tool of supervision has evolved into a mechanism for citizen domestication.

On the global stage, AI governance has become a geopolitical priority. The PRC and the EU represent opposing poles in this debate. While one prioritizes total control over information and data flows, the other opts for regulations oriented towards transparency and accountability. This clash of models will define the future of digital governance. Meanwhile, the BRI has served as a channel for exporting surveillance infrastructures to countries with weak regulatory capacity, facilitating the adoption of supervisory tools in contexts where democracy is fragile or nonexistent.

The problem is no longer digital surveillance itself. It is the absence of effective limits. The lack of international standards has allowed these systems to expand unchecked, without independent oversight mechanisms, and without rights guarantees. The international community faces an imminent challenge. Without global regulations that establish clear red lines, technology will consolidate as a tool of repression rather than a means for human development.

As China's influence grows, the possibility of replicating its model in other regions becomes increasingly tangible. Without resistance, without restrictions, without real opposition. The question is no longer whether the world can afford surveillance models like China's. The question is whether, in the absence of clear limits, these models will become the norm rather than the exception.

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 Construction 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., Papyshv, 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 in English 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/ijj.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.