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

Artículo Original/ Original Article

La exportación del modelo de vigilancia chino: inteligencia artificial, crédito social y el impacto en la seguridad global y los derechos humanos

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

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

[1]*Universidad San Ignacio de Loyola, Facultad de Derecho, Carrera de Relaciones Internacionales. Lima, Perú.*

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

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

Cómo citar/How to cite:
Sánchez Chumpitaz, D. S., y Abarca Del Carpio, J. E. (2025). La exportación del modelo de vigilancia chino: inteligencia artificial, crédito social y el impacto en la seguridad global y los derechos humanos. *Revista científica en ciencias sociales, 7*, e701202. 10.53732/rccsociales/e701202

Editor Responsable:
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

Fecha de recepción: 13/02/2025

Fecha de revisión: 18/02/2025

Fecha de aceptación: 10/03/2025

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

INTRODUCCIÓN

El presente estudio examina la arquitectura de vigilancia digital promovida por la República Popular China (RPC), centrada en el Sistema de Crédito Social (SCS), y su proyección internacional como modelo replicable de gobernanza algorítmica. Esta infraestructura estatal de control, desarrollada mediante inteligencia artificial (IA), macrodatos[1], reconocimiento facial y automatización administrativa, configura un régimen de supervisión ciudadana sin precedentes en la historia reciente (Creemers, 2018; Castellanos-Claramunt, 2023; Stanger et al., 2024). La sistematización tecnológica de este ecosistema no se limita a la optimización de la seguridad pública, sino que ha redefinido los parámetros del orden institucional en clave autoritaria.

La evolución del aparato de control estatal debe situarse en el marco de las reformas estructurales impulsadas desde la política de Reforma y Apertura (**改革开放**, *Gǎigé Kāifàng*)[2]. La transición desde redes comunitarias de vigilancia hacia infraestructuras digitales masivas se consolidó con la implementación del proyecto Escudo Dorado (**金盾工程**, *Jīndùn Gōngchéng*)[3] y el establecimiento del *Great Firewall of China* (**防火长城**, *Fánghuǒ Chángchéng*)[4], permitiendo al Partido Comunista Chino (PCCh) ejercer un control integral sobre la circulación de información y la conducta social.

La exportación del SCS y sus tecnologías asociadas ha trascendido las fronteras de la RPC. A través de mecanismos como la Iniciativa de la Franja y la Ruta (BRI), acuerdos bilaterales en ciberseguridad y cooperación en infraestructura digital, Beijing ha promovido un diseño tecnopolítico[5] orientado a institucionalizar formas de vigilancia automatizada en países con niveles diversos de consolidación democrática (Oliveira et al., 2020; Rocha Pino, 2017; Ding, 2024). Esta estrategia ha tenido una acogida significativa en contextos como Irán, Venezuela, Rusia y Nigeria, donde las élites gobernantes utilizan dichos sistemas para reforzar el control interno y limitar la rendición de cuentas (Nguyen et al., 2023; Segal, 2025; Adeyeye & Grobbelaar, 2024).

El análisis se sostiene en una estrategia metodológica mixta, combinando análisis documental de marcos normativos y plataformas tecnológicas, con una evaluación empírica a través del Índice de Control Estatal (ICE), herramienta diseñada para medir cuantitativamente la relación entre percepción de seguridad, vigilancia digital y restricciones a derechos fundamentales (Mozur et al., 2019; Wright, 2018). A partir de este enfoque, se busca contribuir al debate

[1] El término *macrodatos* (big data) hace referencia al procesamiento masivo de información para establecer patrones de comportamiento, utilizado por el Estado chino para implementar sistemas de clasificación ciudadana automatizados (Mayer-Schönberger & Cukier, 2013).

[2] La política de Reforma y Apertura (**改革开放**, *Gǎigé Kāifàng*) fue impulsada por Deng Xiaoping a partir de 1978 como una estrategia de modernización económica, institucional y tecnológica, facilitando el desarrollo de sistemas de control digital.

[3] El *Escudo Dorado* (**金盾工程**, *Jīndùn Gōngchéng*) es un programa de seguridad pública desarrollado a partir del año 2000 por el Ministerio de Seguridad Pública de la RPC. Su propósito es integrar bases de datos, sistemas de videovigilancia y herramientas de identificación digital para reforzar el control estatal mediante tecnologías inteligentes (Creemers, 2018; Xi, 2014).

[4] La expresión *Great Firewall of China* (**防火长城**, *Fánghuǒ Chángchéng*) alude al sistema de censura y filtrado de internet implementado por el Estado chino como barrera digital para controlar el flujo de información, enmarcado dentro de la arquitectura de control cibernético del régimen (Feldstein, 2019; Goodman & Flaxman, 2016).

[5] El *diseño tecnopolítico* alude a la construcción de infraestructuras digitales que codifican decisiones normativas y estructuras de poder, articulando vigilancia, administración y coerción bajo una lógica algorítmica (Zuboff, 2019; Srivastava & Bullock, 2024).

académico sobre los límites de la legitimidad en regímenes autoritarios digitales, así como problematizar el riesgo de difusión de estos modelos hacia democracias frágiles o en transición.

METODOLOGÍA

El presente estudio adoptó una estrategia metodológica de enfoque mixto, sustentada en un diseño explicativo-comparado orientado a analizar la proyección transnacional del modelo de vigilancia digital promovido por la RPC. Esta aproximación se estructuró en dos niveles analíticos: (*i*) la sistematización cualitativa de marcos normativos, plataformas tecnológicas y discursos institucionales de legitimación, y (*ii*) la utilización de herramientas cuantitativas que permitieron modelar el impacto del sistema sobre variables clave en contextos autoritarios y semi-autoritarios.

Desde el plano cualitativo, se recurrió al análisis documental de fuentes primarias, como la *Aprobación del Consejo de Estado sobre la reestructuración de la conferencia interministerial para la construcción del SCS* (Consejo de Estado de la RPC, 2012), así como literatura especializada en inteligencia artificial, gobernanza algorítmica, seguridad digital y derechos humanos (Creemers, 2018; Feldstein, 2019; Castellanos-Claramunt, 2023). Este examen permitió identificar las dinámicas tecnopolíticas vinculadas a la conformación del ecosistema de vigilancia chino y sus mecanismos de proyección internacional.

En este marco, se asumió una concepción del diseño tecnopolítico como estructurador del orden digital contemporáneo. Bajo esta óptica, los dispositivos de inteligencia artificial no se consideraron herramientas neutrales, sino arquitecturas de poder contenidas en estructuras normativas, capacidades estatales y racionalidades políticas (Zuboff, 2019; Stanger et al., 2024; Srivastava & Bullock, 2024). Por ello, el SCS fue comprendido no como un sistema exclusivamente nacional, sino como un mecanismo de regulación sociopolítica con vocación transnacional (Ding, 2024; Huawen, 2021; Zhang & Shaw, 2023).

En la dimensión cuantitativa, se construyó una base de datos comparativa a partir de reportes consolidados (Nguyen et al., 2023; Mozur et al., 2019; Segal, 2025), que permitió estructurar cinco ejes de observación: percepción de seguridad, grado de penetración tecnológica, restricciones a la libertad de expresión, vulneración de la privacidad informacional y casos de represión política documentada. Los datos se sistematizaron en matrices regionales con el fin de identificar patrones de control estatal digital, diferenciando su implementación en regímenes institucionalmente robustos frente a Estados frágiles o cooptados (Pearson et al., 2022; Oliveira et al., 2020).

El componente innovador de esta investigación residió en la formulación del **Índice de Control Estatal (ICE)**, una herramienta de modelación que permitió cuantificar la relación entre vigilancia digital, percepción de seguridad y grado de restricción de libertades fundamentales. El ICE se expresó mediante la siguiente ecuación:

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

donde $\boldsymbol{S}$ representó la percepción ciudadana de seguridad, $\boldsymbol{V}$ el alcance efectivo de los sistemas de vigilancia digital implementados y $\boldsymbol{L}$ el nivel de restricción a derechos y libertades fundamentales. Los coeficientes de ponderación $\boldsymbol{\alpha}$ (*alfa*), $\boldsymbol{\beta}$ (*beta*) y $\boldsymbol{\gamma}$ (*gama*) fueron definidos a partir de análisis de regresión lineal múltiple, aplicando métodos de estimación ponderada sobre la base empírica recabada. La calibración de pesos se realizó tomando en cuenta tanto el número de países que adoptaron tecnologías chinas de control (Skare et al., 2024), como la magnitud de los impactos negativos registrados en variables sociopolíticas sensibles (Feldstein, 2019; Nguyen et al., 2023). El índice fue concebido como una herramienta replicable para el análisis comparado del autoritarismo digital, al proporcionar un marco cuantificable aplicable desde el campo de las Relaciones Internacionales.

Para validar empíricamente el ICE, se adoptó una lógica de casos anidados. Se analizaron tres escenarios contrastantes: (*i*) la RPC, como modelo de vigilancia digital plenamente institucionalizado; (*ii*) Nigeria, como caso de implementación parcial dependiente de transferencia tecnológica externa (Adeyeye & Grobbelaar, 2024); y (*iii*) Venezuela, país receptor de tecnología de control chino, cuya arquitectura autoritaria instrumentalizó tales sistemas en contextos de erosión democrática (Greitens et al., 2020; Wright, 2018). Esta estrategia respondió al principio de variación estructural mínima[6] permitió evaluar diferencias en eficacia, legitimidad y resistencia social ante la expansión de mecanismos digitales de control.

El enfoque teórico del estudio articuló una perspectiva transdisciplinaria que entrelazó elementos de teoría de regímenes, gobernanza algorítmica, estudios críticos de tecnología y geopolítica digital (Chan et al., 2024; Tuzov & Lin, 2024; Sandbrink et al., 2024). Asimismo, se inscribió en los debates contemporáneos sobre la difusión autoritaria[7], donde la exportación de modelos de control encontró legitimidad a través de marcos legales, cooperación estratégica e infraestructuras digitales (Rocha Pino, 2017; Cancela-Outeda, 2024; Stanger et al., 2024).

Por último, la aproximación epistemológica responde a una lógica abductiva, en la que las inferencias se construyen inductivamente a partir de datos empíricos, además buscan teorizar nuevas configuraciones del poder en el entorno internacional. De este modo, la metodología aquí propuesta se erige como un aporte original para el análisis del autoritarismo digital, sus condiciones de reproducción y su impacto sobre los equilibrios globales de seguridad, gobernanza y derechos fundamentales.

RESULTADOS

Evolución del modelo de vigilancia en la República Popular China

La consolidación del sistema de vigilancia digital en la RPC se ha configurado como un proceso estratégico sostenido, que responde a una visión tecnopolítica del poder estatal. Este modelo se estructura sobre una lógica normativa centralizada, una infraestructura tecnológica distribuida y una arquitectura de procesamiento algorítmico orientada al control poblacional. Lejos de constituir una reacción coyuntural a factores de inseguridad interna, la institucionalización de este régimen de supervisión se enmarca en un proyecto político de largo aliento, promovido por el PCCh, en el que convergen elementos de reforma institucional, cohesión ideológica y modernización autoritaria (Creemers, 2018; Xi, 2014; Feldstein, 2019; Ding, 2018).

El punto de partida normativo se ubica en la "*Aprobación del Consejo de Estado sobre la reestructuración de la conferencia interministerial para la construcción del sistema de crédito social*" (Consejo de Estado de la RPC, 2012), documento que estableció las bases administrativas, técnicas y jurídicas del SCS. Este instrumento delineó una red interinstitucional de interoperabilidad, destinada a consolidar un entorno digital en el que la ciudadanía pudiera ser evaluada en función de sus comportamientos, registros económicos, prácticas cívicas y patrones de interacción digital. La lógica subyacente parte de una

[6] El principio de *variación estructural mínima* se emplea en estudios comparativos para seleccionar casos que, aunque contrastantes en ciertas variables clave, comparten suficientes similitudes estructurales que permiten aislar el efecto de la variable independiente bajo análisis (George & Bennett, 2005). Esta estrategia metodológica incrementa la validez interna al reducir sesgos derivados de diferencias contextuales extremas.

[7] El concepto de *difusión autoritaria* refiere al proceso mediante el cual los regímenes autocráticos exportan prácticas institucionales, tecnologías de control o marcos regulatorios a otros Estados, promoviendo modelos de gobernanza que limitan deliberadamente la participación política y las libertades fundamentales (Way, 2015; Greitens, 2020). Este fenómeno puede darse mediante acuerdos bilaterales, cooperación tecnológica o narrativas que legitiman el autoritarismo digital en nombre de la estabilidad.

racionalidad meritocrática algorítmica, en la que el desempeño individual se transforma en un insumo para la toma de decisiones administrativas automatizadas.

El desarrollo progresivo del sistema se dio en fases sucesivas: desde proyectos piloto localizados, como el caso de Rongcheng (Mozur, Kessel y Chan, 2019), hasta una expansión nacional mediante tecnologías de reconocimiento facial, vigilancia biométrica y centralización de bases de datos regionales. La Tabla 1 sintetiza esta evolución en términos cronológicos, destacando los hitos normativos, tecnológicos e institucionales.

Tabla 1. *Línea de tiempo de evolución del modelo de vigilancia en la RPC*

Década	Hito	Descripción
2003	Iniciativa “Skynet”	Implementación de una red de videovigilancia urbana interconectada, con más de 20 millones de cámaras distribuidas en zonas metropolitanas.
2012	Reestructuración del Sistema de Crédito Social	Aprobación del instrumento nacional para establecer una plataforma de evaluación cívica integral mediante el documento oficial N.° 88 del Consejo de Estado (Consejo de Estado, 2012).
2015	Aplicación d sistemas de puntuación social	Implementación de sistemas de evaluación ciudadana en ciudades piloto, como Rongcheng, con integración de datos judiciales, financieros y comunitarios.
2018	Ampliación mediante reconocimiento facial	Expansión del sistema a espacios públicos mediante tecnologías de vigilancia biométrica e inteligencia artificial en tiempo real.
2020	Consolidación algorítmica a escala nacional	Centralización de plataformas de datos regionales en un sistema unificado de monitoreo ciudadano
2022	Internacionalización del modelo	Exportación de soluciones tecnológicas a Estados de África, Asia Central y América Latina mediante convenios interestatales y empresariales.

Fuente: Elaboración propia basada en Consejo de Estado (2012), Creemers (2018), Ding (2018), Mozur et al. (2019), Castellanos-Claramunt (2023) y Wright (2018).

Esta progresión evidencia una capacidad singular del Estado chino para articular medios tecnológicos con mecanismos normativos, permitiendo así la consolidación de un sistema de vigilancia predictiva basado en el cruce automatizado de información personal. A ello se suma una capacidad narrativa que legitima este modelo en nombre de la estabilidad social y el orden público, reforzando una concepción del ciudadano como objeto de observación constante y sujeto a evaluación permanente (Amoore, 2020; Zhang y Shaw, 2023; Vickers, 2022). La integración de algoritmos a marcos normativos ha dotado al sistema de una flexibilidad operativa que excede el ámbito de la supervisión individual, permitiéndole intervenir en las condiciones de acceso a servicios fundamentales como salud, transporte y empleo (Nguyen, Lafrance y Vu, 2023).

Impactos del SCS en derechos fundamentales

La implementación del SCS por parte de la RPC ha modificado sustantivamente las condiciones de ciudadanía, al consolidar un modelo de supervisión algorítmica que convierte el comportamiento individual en parámetro decisivo para el acceso a derechos fundamentales. Este esquema de gobernanza articulado por datos no se limita a modernizar la administración pública, sino que instituye una racionalidad política centrada en la evaluación permanente del sujeto gobernado, legitimando su inclusión o exclusión del sistema a partir de criterios de mérito cívico (Creemers, 2018; Amoore, 2020; Castellanos-Claramunt, 2023).

A partir de la promulgación del documento normativo N.º 88 del Consejo de Estado (2012), la infraestructura legal y tecnológica del SCS habilitó mecanismos de calificación individual y organizacional mediante plataformas digitales unificadas, sin requerimientos de intervención judicial ni garantías procesales tradicionales (Consejo de Estado, 2012; Mac Síthigh & Siems, 2019). Este ecosistema funciona como una arquitectura de visibilidad forzada, integrada por redes gubernamentales, empresas privadas, medios digitales y sistemas biométricos, que procesan información proveniente de registros financieros, decisiones judiciales, comportamiento en redes sociales y relaciones comerciales.

Uno de los ejemplos más citados es el caso de la ciudad de Rongcheng, utilizada como laboratorio piloto para el despliegue del SCS, donde se combinan datos judiciales, bancarios y comunitarios para elaborar una puntuación cívica que determina el acceso a servicios públicos y la posibilidad de desplazamiento o endeudamiento.

La evidencia empírica recogida muestra un impacto desproporcionadamente adverso en diversas dimensiones críticas de la vida ciudadana. La Tabla 2 sistematiza el efecto positivo y negativo percibido en relación con cinco áreas clave:

Tabla 2. *Impacto del SCS en la sociedad*

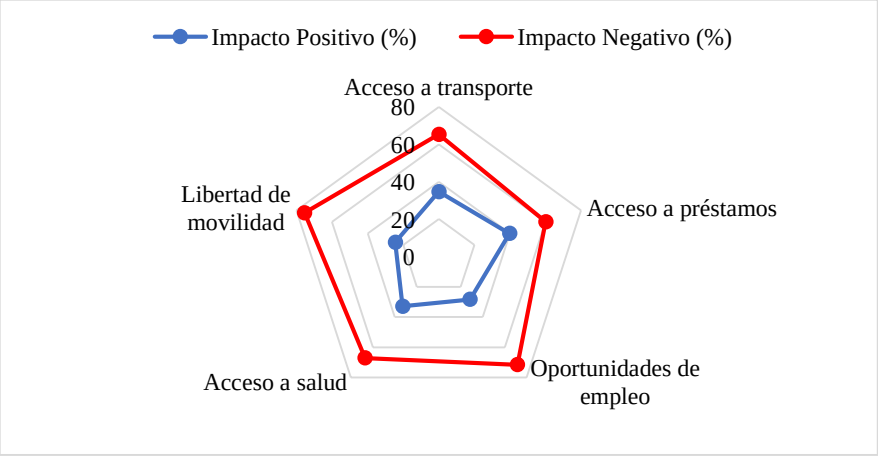
Aspecto Evaluado	Impacto Positivo (%)	Impacto Negativo (%)
Libertad de movilidad	24,50	75,50
Oportunidades de empleo	28,40	71,60
Acceso a salud	32,90	67,10
Acceso a transporte	34,70	65,30
Acceso a préstamos	39,80	60,20

Fuente: Elaboración propia en base a Nguyen et al. (2023).

La evaluación revela una estructura de gobernanza punitiva basada en el principio de clasificación algorítmica. Este mecanismo genera externalidades negativas sobre la movilidad social ascendente, reconfigurando el acceso a bienes públicos bajo un principio de condicionalidad conductual. El resultado es un modelo de ciudadanía gradualmente estratificada, donde la participación social se vuelve contingente a métricas de obediencia.

La Figura 1 permite visualizar cómo la cobertura tecnológica incide en los efectos adversos del sistema. Se observa una correlación directa entre el despliegue tecnológico y la gravedad del impacto, especialmente en empleo, transporte y salud.

Figura 1. *Impacto del SCS en diferentes aspectos sociales en relación con la cobertura tecnológica regional*

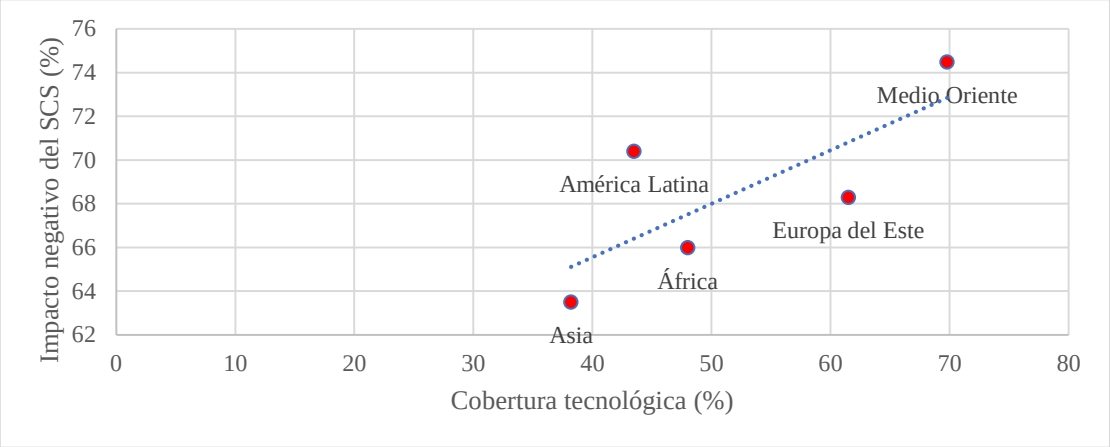


Fuente: Elaboración propia en base a Nguyen et al. (2023) y Segal (2025)

La correlación entre infraestructura tecnológica y restricción de derechos se visualiza con mayor claridad en la Figura 2, que representa el impacto negativo por región geográfica en

función de la cobertura del sistema. Medio Oriente y Asia, con niveles de penetración superiores al 60%, presentan los índices más altos de afectación. América Latina, pese a su menor nivel de adopción, evidencia consecuencias significativas, lo que sugiere que la eficacia del modelo también se vincula a las debilidades institucionales locales (Wright, 2018; Gomes Rêgo de Almeida y Dos Santos Júnior, 2025).

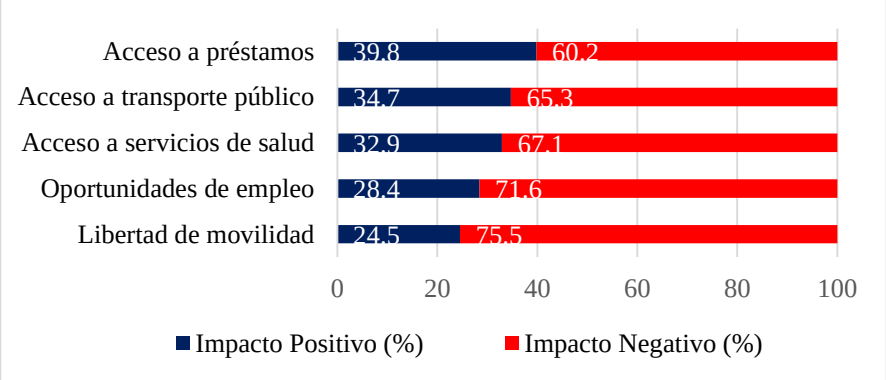
Figura 2. *Correlación entre la cobertura de tecnología de vigilancia y el impacto negativo del SCS por región*



Fuente: Elaboración propia en base a Nguyen et al. (2023) y Segal (2025).

La Figura 3 refuerza esta tendencia comparando directamente los porcentajes de impacto positivo y negativo. Las diferencias porcentuales reflejan una concentración de efectos adversos en aquellas áreas que constituyen derechos básicos. El sistema condiciona así la inclusión social a la obediencia registrada, debilitando el principio de igualdad ante la ley y erosionando el núcleo normativo de los derechos fundamentales (Amoore, 2020; Castellanos-Claramunt, 2023).

Figura 3. *Comparación del impacto positivo y negativo del SCS en distintos aspectos sociales*



Fuente: Elaboración propia en base a Nguyen et al. (2023).

A partir de estos hallazgos, se aplicó el **Índice de Control Estatal (ICE)** como herramienta de medición comparada. Recordemos que el **ICE** se expresa como:

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

Donde:

- S = percepción social de seguridad
- V = intensidad de la vigilancia digital
- L = nivel de restricción a derechos fundamentales

Los coeficientes α, β y γ fueron calibrados mediante análisis de regresión lineal múltiple aplicado a una base de datos comparativa construida exprofeso, combinando métricas

empíricas con literatura especializada. La ponderación diferencial se sustentó en tres criterios principales: intensidad de la acción estatal, afinidad ideológica del régimen con modelos autoritarios digitales, y profundidad normativa del marco jurídico en materia de ciberseguridad y control algorítmico[8].

La selección de los casos considerados para esta evaluación cuantitativa incluye a la RPC, Venezuela y Nigeria. Esta decisión metodológica se fundamenta en un diseño comparado por máxima variación contextual en condiciones anidadas[9]. Cada uno de estos países mantiene vínculos tecnológicos con Beijing, aunque presenta distintos niveles de apropiación institucional, eficacia operativa y consolidación normativa en materia de gobernanza digital[10]. La Tabla 3 muestra los valores utilizados para la estimación del índice en cada caso.

Tabla 3. *Impacto del SCS en la sociedad*

País	S (seguridad)	V (vigilancia)	L (restricciones)	α	β	γ
RPC	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

Fuente: Elaboración propia con base en Mozur et al. (2019), Nguyen et al. (2023), Feldstein (2019) y Adeyeye y Grobbelaar (2024).

Los cálculos arrojan un ICE de **46,12** para la RPC, lo cual refleja un modelo plenamente consolidado, donde la interdependencia entre percepción de seguridad, cobertura tecnológica y restricciones institucionalizadas alcanza un carácter sistémico. En Venezuela, el índice alcanza **36,18**, lo que pone en evidencia una estructura intermedia, condicionada por su cooperación tecnológica con China, pero limitada por una arquitectura normativa fragmentada. Nigeria, con un ICE de **1,05**, muestra un modelo aún incipiente, sin articulación legal robusta ni aceptación social suficiente para legitimar sus dispositivos de control.

Estos resultados permiten afirmar que el ICE es una métrica válida para evaluar la institucionalización del control algorítmico estatal. Su diseño posibilita una lectura empírica rigurosa del fenómeno de la difusión autoritaria, integrando dimensiones tecnológicas, normativas y sociopolíticas que rara vez convergen en un solo indicador. Además de cuantificar la presencia tecnológica, el índice permite inferir la capacidad estructural de los regímenes para incorporar dicha tecnología como herramienta de gobernanza efectiva.

Esta lectura se encuentra respaldada por estudios recientes que han abordado el SCS como parte de una racionalidad autoritaria digital. El SCS no debe ser entendido como un simple instrumento de eficiencia administrativa, ya que su lógica está estructurada para maximizar el control estatal mediante la reducción progresiva de los márgenes de autonomía ciudadana. Este tipo de arquitectura algorítmica se sustenta en correlaciones de datos más que en procesos deliberativos o garantías jurídicas, y tiende a consolidarse en contextos donde el aparato estatal posee alta capacidad de coerción institucional y escasa fiscalización democrática (Stanger et al., 2024; Ding, 2018; Goodman y Flaxman, 2016).

La evidencia presentada permite sostener que el SCS redefine la noción de ciudadanía bajo una lógica de legibilidad algorítmica, donde cada individuo es sujeto a evaluación constante con consecuencias materiales directas. Las siguientes secciones abordarán la manera en que este

[8] La "*profundidad normativa*" se entiende como el nivel de densidad institucional, desarrollo jurídico y eficacia de aplicación en marcos regulatorios orientados al control digital y la vigilancia algorítmica (Vickers, 2022).

[9] La comparación mediante casos anidados permite examinar unidades con relaciones estructurales compartidas, manteniendo a la vez diferencias clave en la configuración institucional, lo que facilita inferencias más robustas en estudios de política comparada (Gerring, 2007).

[10] Diversos estudios han documentado la exportación tecnológica y normativa del modelo de control digital chino hacia regímenes híbridos o autoritarios, evidenciando su papel como vector estructurante de nuevas formas de vigilancia transnacional (Greitens, Lee & Yazici, 2022).

modelo ha sido adaptado en otros contextos políticos y culturales, y evaluarán los factores que modulan su eficacia más allá del entorno normativo chino.

Exportación del modelo chino y correlaciones geopolíticas

La estrategia internacional de la RPC en materia de vigilancia digital se estructura a partir de un enfoque integral que articula infraestructura tecnológica, arquitectura regulatoria y mecanismos institucionales para transferir un modelo de control centralizado, sustentado en IA y análisis algorítmico de grandes volúmenes de datos. Este modelo se ha consolidado como parte de una política exterior que combina elementos materiales, como redes 5G, sistemas de videovigilancia y plataformas de procesamiento masivo de información, con instrumentos normativos orientados a influir en la configuración institucional de los países receptores (Zhu, Cerina, Chessa, Caldarelli y Riccaboni, 2014; Pearson, Rithmire y Tsai, 2022; Wu, Esposito y Evans, 2024).

Esta proyección internacional no se limita a la exportación de hardware o soluciones tecnológicas. Supone una reorganización profunda del ecosistema normativo digital mediante la expansión estructurada de empresas estatales, acuerdos en ciberseguridad y provisión de marcos jurídicos funcionales a una lógica de control algorítmico (Ding, 2018; Aoyama, 2022). La Tabla 4 muestra la distribución de la tecnología china de vigilancia digital en distintas regiones del sistema internacional, evidenciando una inserción estratégica especialmente en zonas con baja consolidación institucional o escaso blindaje normativo en materia de protección de datos personales.

Tabla 4. *Distribución global de tecnología de vigilancia digital de la RPC*

Región	Número de países con tecnología China	Porcentaje de cobertura regional (%)
Asia	15,00	61,50
África	12,00	48,00
América Latina	10,00	43,50
Europa del Este	8,00	38,20
Medio Oriente	14,00	69,80

Fuente: Elaboración propia en base a Segal (2025).

El despliegue geográfico de esta tecnología se apoya en mecanismos institucionalizados de transferencia y expansión. Tal como se muestra en la Tabla 5, estos mecanismos no operan de manera aislada. Se configuran como canales estratégicos para reproducir la gobernanza algorítmica de la RPC en contextos externos. Esto ha permitido proyectar una normatividad alternativa a los estándares multilaterales occidentales, a través de acuerdos bilaterales y cooperación técnica especializada.

Tabla 5. *Mecanismos de exportación del modelo chino de gobernanza digital*

Mecanismo de exportación	Descripción
Inversión en infraestructura digital	Financiación y construcción de redes 5G, sistemas de videovigilancia y plataformas de datos en países en desarrollo.
Transferencia de tecnología	Provisión de software de vigilancia, sistemas de reconocimiento facial y plataformas de crédito social a otros gobiernos.
Cooperación en ciberseguridad	Acuerdos bilaterales con naciones aliadas para compartir tecnologías de control digital y análisis de datos.
Expansión de empresas estatales	Huawei, ZTE y otras compañías chinas como actores clave en el despliegue de redes tecnológicas globales.
Exportación de normas regulatorias	Modelos de control digital y vigilancia aplicados en sistemas legales de países receptores.

Fuente: Elaboración propia en base a Zhu et al. (2014) y Wu et al. (2024).

Esta estrategia de internacionalización encuentra sus mejores condiciones de recepción en contextos donde la institucionalidad es frágil o permeable a la injerencia externa. Tal como se

aprecia en la Tabla 6, existe una correlación significativa entre la presencia de tecnología china y la implementación de esquemas de control digital, particularmente en regiones con vínculos estrechos con Beijing. Asia Central y Medio Oriente lideran en ambas métricas, lo que sugiere un patrón de alineamiento estructural con la gobernanza algorítmica promovida por el PCCh.

Tabla 6. *Penetración de tecnologías chinas y adopción de modelos de control digital por región*

Región	Presencia de Tecnología China (%)	Implementación de Modelos de Control (%)
América Latina	47,30	38,90
África	52,60	42,10
Asia Central	68,50	59,30
Medio Oriente	73,20	65,70
Europa del Este	49,70	41,40

Fuente: Elaboración propia en base a Sánchez & Asmat (2024) y Wu et al. (2024).

La consolidación del modelo de gobernanza digital promovido por el gobierno de Beijing no ha descansado únicamente en marcos normativos o acuerdos bilaterales. Su eficacia ha sido reforzada por la incorporación estratégica de plataformas digitales desarrolladas por conglomerados tecnológicos estrechamente vinculados al Estado chino, los cuales operan como instrumentos funcionales para institucionalizar un régimen de vigilancia algorítmica de alcance extensivo. Estas tecnologías no han sido adoptadas en abstracto. Se han introducido en gobiernos receptores bajo el argumento de modernización administrativa y eficiencia pública. Sin embargo, su lógica operativa responde a esquemas de evaluación constante del comportamiento ciudadano, supervisión intensiva y administración anticipatoria del orden colectivo. El propósito declarado de innovación digital oculta un objetivo estructural: reorganizar la interacción entre gobernantes y gobernados mediante sistemas de control automatizado.

Los sistemas estudiados comparten una arquitectura basada en inteligencia artificial, monitoreo permanente y procesamiento en tiempo real de grandes volúmenes de información. En entornos institucionales con escasa capacidad de fiscalización, estas plataformas dejan de ser herramientas técnicas y se convierten en matrices normativas que codifican criterios de gobernabilidad. Clasifican, puntúan, almacenan y retroalimentan decisiones públicas desde una lógica predictiva que desplaza a la deliberación ciudadana. El caso paradigmático es el Sistema de Crédito Social, que convierte la conducta cotidiana en variable determinante para el acceso a servicios esenciales. A este se suman *Skynet*, como infraestructura de videovigilancia facial; Huawei Cloud, que provee almacenamiento masivo para el aparato estatal; y *Safe City*, un dispositivo urbano diseñado para la gestión algorítmica de la seguridad pública. La Tabla 7 sintetiza las plataformas más relevantes exportadas por la RPC y su utilización institucional en los países receptores.

Tabla 7. *Plataformas digitales de gobernanza exportadas por la RPC*

Plataforma	Función en el país receptor
Sistema de Crédito Social	Evaluación del comportamiento ciudadano para acceso a beneficios gubernamentales.
Skynet	Red de videovigilancia masiva con reconocimiento facial integrado.
ZTE Smart City	Gestión urbana basada en análisis de datos en tiempo real.
Huawei Cloud	Infraestructura para almacenamiento y procesamiento de datos gubernamentales.
Safe City	Integración de IA en seguridad pública para prevención del crimen.

Fuente: Elaboración propia en base Bonsón et al. (2012) y Wu et al. (2024).

La racionalidad funcional detrás de esta arquitectura digital se ha manifestado también en ámbitos económicos, donde los sistemas automatizados han permitido mejoras sustantivas en logística, administración y comercio. La Tabla 8 documenta reducciones importantes en costos operativos y tiempos de procesamiento, reforzando la percepción de eficiencia que justifica, en algunos casos, la adopción del modelo en ausencia de garantías democráticas (Adeyeye y Grobbelaar, 2024; Oliveira, Murton, Rippa, Harlan y Yang, 2020).

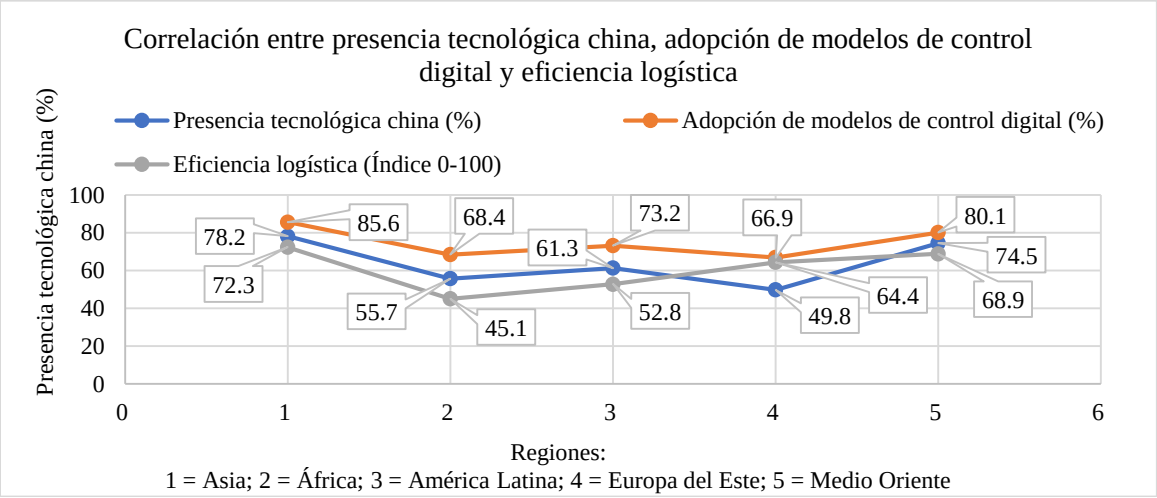
Tabla 8. *Impacto de la automatización digital china en logística y comercio internacional*

Sector	Reducción de Costos (%)	Disminución de Tiempos de Procesamiento (%)
Transporte marítimo	24,50	36,80
Logística de puertos	30,20	42,10
Comercio electrónico	28,70	40,50
Administración aduanera	22,30	33,60

Fuente: Elaboración propia en base a Sánchez & Asmat (2024).

Esta doble funcionalidad (vigilancia estructural y eficiencia operativa) se evidencia gráficamente en la Figura 4, que muestra la correlación entre presencia tecnológica china, adopción de modelos de control digital y desempeño logístico en diferentes regiones.

Figura 4. *Correlación entre presencia tecnológica china, adopción de modelos de control digital y eficiencia logística*



Fuente: Elaboración propia en base a Nguyen et al. (2023), Wu et al. (2024) y Bonsón et al. (2012).

El análisis revela que el modelo chino de vigilancia digital no se proyecta como un conjunto de soluciones aisladas. Se trata de una arquitectura sistémica que promueve una forma específica de gobernanza estatal, en la que el orden, la predictibilidad y la centralización se privilegian frente a la transparencia, la deliberación y la garantía de derechos fundamentales (Chan, Papyshev y Yarime, 2024; Cancela-Outeda, 2024; Castellanos-Claramunt, 2023).

Evaluación comparada mediante el Índice de Control Estatal (ICE)

El análisis comparativo de modelos de vigilancia digital requiere de herramientas que integren variables tecnológicas, normativas y sociopolíticas. A tal efecto, se propone el ICE como una métrica compuesta que permite evaluar cuantitativamente la intensidad del control algorítmico ejercido por los Estados sobre su población. Este índice considera, por un lado, el nivel de penetración de tecnologías de vigilancia digital; por otro, el grado de percepción ciudadana de

seguridad; y, finalmente, el impacto documentado sobre derechos fundamentales, especialmente en materia de privacidad y libertad de expresión.

La aplicación inicial del ICE contempla cinco Estados representativos que comparten tres características estructurales: elevados niveles de adopción tecnológica, marcos regulatorios permisivos en términos de privacidad, y una arquitectura institucional orientada al control informacional. Los casos incluidos en esta evaluación son la RPC, Venezuela, Irán, Arabia Saudita y la Federación Rusa. A través de ellos, se pretende contrastar distintos grados de consolidación del modelo de vigilancia digital promovido por Beijing.

El primer componente del ICE, asociado a la legitimidad percibida del aparato de control, se analiza mediante la relación entre el uso de tecnología china y la percepción de seguridad estatal. La Tabla 9 sintetiza esta relación, evidenciando que la RPC presenta la cobertura tecnológica más alta, acompañada de la mayor percepción de seguridad. El resto de los países mantiene niveles de percepción aceptables, aunque las brechas tecnológicas sugieren diferencias en la capacidad operativa y narrativa de los regímenes analizados (Mozur, Kessel y Chan, 2019; Wright, 2018).

Tabla 9. *Uso de tecnología de vigilancia china y percepción de seguridad*

País	Uso de tecnología china (%)	Percepción de seguridad (%)
RPC	100,00	85,40
Venezuela	79,00	68,90
Irán	76,00	70,20
Arabia Saudita	73,00	74,80
Rusia	71,00	72,30

Fuente: Elaboración propia basada en Mozur et al. (2019) y Wright (2018).

Aunque la percepción de seguridad en estos países es alta, este fenómeno no puede interpretarse como producto exclusivo de mayor protección ciudadana. Según Amoore (2020), estas cifras pueden explicarse como resultado de una ética algorítmica internalizada, en la que la ciudadanía, frente a una vigilancia omnipresente, reconfigura sus expectativas de seguridad en función de su conformidad con el sistema de monitoreo.

El segundo componente del ICE analiza las restricciones concretas a libertades fundamentales. La Tabla 10 detalla las tasas de censura, vigilancia intrusiva y represión política documentada en el quinquenio reciente. En todos los casos analizados, se verifica una relación directa entre uso intensivo de IA para vigilancia y prácticas sistemáticas de silenciamiento del disenso (Greitens, Lee y Yazici, 2020; Feldstein, 2019).

Tabla 10. *Impacto de la vigilancia digital en la libertad de expresión y la privacidad*

País	Restricción de libertad de expresión (%)	Restricción de privacidad (%)	Casos de represión política documentados (últimos 5 años)
RPC	92,30	94,80	135 000+
Venezuela	89,70	87,20	10 400
Irán	87,10	89,50	9 800
Arabia Saudita	84,50	88,10	7 900
Rusia	80,90	85,40	6 500

Fuente: Elaboración propia basada en Greitens et al. (2020) y Feldstein (2019).

Los datos sugieren que los modelos de vigilancia digital están asociados a un repertorio de prácticas coercitivas normalizadas. Zuboff (2019) ha descrito este fenómeno como autoritarismo computacional, aludiendo a la consolidación de una infraestructura de control basada en datos masivos y clasificaciones algorítmicas, que reduce la agencia individual a indicadores de comportamiento observables y puntuables.

La Tabla 11 ofrece un análisis del marco institucional adoptado por cada uno de los países, distinguiendo entre la finalidad declarada del sistema y su uso documentado. Este contraste

permite identificar las divergencias entre la narrativa oficial de seguridad y los efectos concretos sobre la esfera pública.

Tabla 11. *Modelos de vigilancia digital y sus objetivos*

País	Modelo de Vigilancia adoptado	Objetivo Declarado	Uso real documentado
RPC	Sistema de Crédito Social, *Skynet*	Seguridad nacional y estabilidad	Control de la población mediante vigilancia digital masiva
Venezuela	Carnet de la Patria, censura digital	Control económico y social	Monitoreo y limitación del acceso a servicios según lealtad política
Irán	Intranet nacional, filtrado de contenido	Protección de valores islámicos	Censura y restricción del acceso a información disidente
Arabia Saudita	Algoritmos de reconocimiento facial, biometría forense	Prevención del terrorismo	Seguimiento y control de opositores y activistas
Rusia	SORM (Sistema de interceptación de comunicaciones)	Seguridad cibernética	Supervisión de redes de comunicación y represión política

Fuente: Elaboración propia basada en Mozur et al. (2019) y Nguyen et al. (2023).

Este patrón de uso político de la tecnología no se desarrolla en el vacío. Como muestra la Tabla 12, su implementación está directamente influida por factores demográficos, niveles de densidad poblacional y marcos regulatorios laxos. A mayor población, mayor incentivo para el uso de mecanismos de control algorítmico automatizado. En paralelo, el nivel de restricciones se incrementa conforme se consolida una infraestructura tecnológica interoperable con la arquitectura estatal (Stanger et al., 2024; Ding, 2018).

Tabla 12. *Comparación de población, uso de tecnología de vigilancia y restricción de libertades en países con modelos de monitoreo digital*

País	Población (millones)	Uso de tecnología de vigilancia (%)	Restricción de libertades (%)
RPC	1 410	100,00	94,80
Venezuela	28	79,00	87,20
Irán	85	76,00	89,50
Federación Rusa	144	71,00	85,40
Nigeria	223	55,00	74,50
Arabia Saudita	36	73,00	88,10

Fuente: Elaboración propia basada en Stanger et al. (2024) y Ding (2018).

Un componente clave en el cálculo del ICE es la dimensión legal. La Tabla 13 contrasta los marcos normativos que habilitan o restringen el uso de IA en contextos de vigilancia estatal. Mientras la Unión Europea mantiene un enfoque garantista, los países alineados con el modelo de gobernanza chino adoptan esquemas de control normativo centralizado, con escasa supervisión independiente (Goodman y Flaxman, 2016; Pearson, Rithmire y Tsai, 2022).

Tabla 13. *Comparación de marcos regulatorios sobre privacidad y control estatal*

País/Región	Regulación clave	Enfoque	Uso de la IA en vigilancia
Unión Europea	GDPR (Reglamento UE 2016/679)	Protección de datos y derechos individuales	Limitado a seguridad pública con restricciones
EE. UU.	Ley Federal de Privacidad	Protección sectorial de datos	Aplicaciones en ciberseguridad y prevención de delitos
RPC	Ley de Seguridad de Datos, Ley de Ciberseguridad	Control del flujo de información y vigilancia estatal	Extensivo: IA aplicada en crédito social y reconocimiento facial
Federación Rusa	Ley Yarovaya, Sistema SORM	Supervisión estatal y control de comunicaciones	Monitoreo masivo con apoyo de algoritmos predictivos

Venezuela	Carnet de la Patria y bloqueos digitales	Control socioeconómico y censura	Implementación incipiente con apoyo de infraestructura china

Fuente: Elaboración propia basada en Goodman & Flaxman (2016), Vickers (2022) y Pearson et al. (2022).

Finalmente, la Tabla 14 confronta los enfoques regulatorios de los regímenes democráticos y autoritarios en cuanto al uso público y privado de la IA. Esta comparación permite ubicar el modelo de la RPC dentro de una lógica de control estatal absoluto, incompatible con los principios de transparencia y auditoría externa característicos de las democracias liberales (Stanger et al., 2024).

Tabla 14. *Estrategias regulatorias de la I. A. en el ámbito público y privado*

Aspecto	Enfoque democrático	Enfoque autocrático
Gobernanza de la I. A.	Basada en transparencia y auditoría pública	Control estatal sin supervisión independiente.
Acceso a datos	Regulación para proteger privacidad individual	Centralización y acceso irrestricto del Estado.
Uso en educación	Aplicaciones para personalización del aprendizaje	Instrumentalización ideológica y homogenización.
Supervisión de empresas	Regulación para evitar sesgos y monopolios	Integración de corporaciones con el aparato estatal.

Fuente: Elaboración propia basada en Stanger et al. (2024) y Ding (2018).

El análisis integral del ICE confirma que la arquitectura de gobernanza digital promovida por la RPC no se circunscribe a su territorio nacional. Su expansión internacional responde a una racionalidad estructurada en torno a la eficacia operativa, la consolidación institucional y la reducción programada de espacios de autonomía individual. Este modelo redefine los parámetros de la seguridad digital, imponiendo un paradigma de supervisión algorítmica que tensiona los marcos normativos contemporáneos y plantea desafíos significativos para la arquitectura global de derechos humanos.

DISCUSIÓN

Los hallazgos presentados revelan una reconfiguración profunda en las relaciones entre poder, tecnología y ciudadanía. La vigilancia digital, en contextos de escasa fiscalización institucional, ha dejado de desempeñar un rol subsidiario frente a las necesidades de seguridad estatal. Se ha convertido en el núcleo funcional de una forma emergente de gobernanza, donde el control no es un recurso excepcional, sino un principio operativo permanente. Esta transformación no obedece exclusivamente a razones técnicas. Representa una mutación de orden político, donde se transita del derecho como límite hacia la correlación algorítmica como forma de regulación. Las decisiones dejan de ser deliberadas para volverse automatizadas. El sujeto democrático se ve desplazado por una figura funcional: el ciudadano monitoreado, previsible, legible.

El caso de la República Popular China resulta ilustrativo del nuevo paradigma de vigilancia digital institucionalizada. Bajo el liderazgo del actual Secretario General del PPCh y séptimo Presidente de la RPC, se ha consolidado un modelo que trasciende la supervisión tradicional. Lo que se implementa no es simplemente un sistema técnico de seguimiento ciudadano, sino una arquitectura sociopolítica de control algorítmico. Plataformas como Skynet y el Sistema de Crédito Social han sido integradas para convertir cada acción individual en un dato susceptible de evaluación normativa. En este ecosistema, las decisiones del ciudadano son observadas, procesadas y transformadas en un índice de confiabilidad. Esa métrica no es neutra: condiciona el acceso a derechos, moldea trayectorias de vida, impone límites sin necesidad de intervención judicial.

No se trata de una simple infraestructura de gestión pública. Es una ingeniería del consentimiento, cuya lógica excede la eficiencia y se inscribe en un proyecto de gobierno totalizante. La transparencia exigida es unidireccional. Se exige de abajo hacia arriba. En cambio, quienes gobiernan permanecen ocultos tras capas de opacidad institucional. Este diseño no busca solamente castigar desviaciones, sino anticiparlas. Define previamente el rango de lo permitido. Todo aquello que se aleje de la norma estadística es identificado como amenaza potencial. La vigilancia deja de ser correctiva para volverse constitutiva del orden social.

La configuración vertical entre quien observa y quien es observado opera como columna vertebral de una forma renovada de dominación. Ya no se necesita violencia visible. La supervisión constante y su posibilidad permanente bastan para que el sujeto político internalice la mirada del poder. Así, lo que era exterior se vuelve interior. Las normas dejan de imponerse por coerción directa. Se encarnan en los hábitos, en las decisiones cotidianas, en la percepción del entorno como espacio monitoreado. El comportamiento se ajusta a los umbrales definidos por el sistema. La autocensura emerge no como imposición, sino como mecanismo de adaptación. La vida pública se convierte en una coreografía previsible. El conflicto legítimo se invisibiliza antes de adquirir forma discursiva.

La herramienta metodológica propuesta en esta investigación, el Índice de Control Estatal, permite cuantificar estos procesos. China alcanza los valores más altos, no sólo por su infraestructura tecnológica, sino por su capacidad de traducir esa infraestructura en mecanismos de regulación social. Venezuela representa una imitación parcial, donde la cooperación tecnológica con Beijing convive con debilidades institucionales estructurales. Nigeria, en contraste, muestra una implementación fragmentaria, carente de legitimidad interna y dependiente de asistencia externa. En todos los casos, se observa un mismo desplazamiento: la erosión paulatina del espacio de acción libre del ciudadano.

En América Latina, esta discusión adquiere un carácter urgente. Los sistemas democráticos de la región enfrentan una presión creciente para ofrecer soluciones inmediatas frente a problemas estructurales como la inseguridad, la corrupción o la crisis de representación. En este contexto, el modelo chino se presenta como una alternativa funcional. Pero importar este paradigma sin adecuadas salvaguardas institucionales puede significar el debilitamiento definitivo del orden constitucional. La tentación de optar por la eficacia en lugar de la legitimidad ha sido históricamente costosa en nuestra región. Las herramientas de control, una vez instauradas, rara vez retroceden. Lo excepcional se transforma en norma. Y lo normativo se vuelve inmutable.

El modelo exportado desde Beijing no es neutral. No se trata únicamente de plataformas tecnológicas, sino de una concepción del poder basada en la administración técnica de la conducta humana. Una visión donde la previsibilidad es superior al disenso. Donde la libertad es considerada disfuncional. Esta lógica se impone no por la violencia, sino por su apariencia de racionalidad. El control aparece como modernización. El orden como eficiencia. Pero la consecuencia es una ciudadanía reducida a parámetro, una política reducida a cálculo.

El actual mandatario chino ha desempeñado un rol central en esta transformación. Xi Jinping ha promovido un modelo de gobierno que sustituye el pluralismo por la homogeneidad, el debate por el silenciamiento anticipado. Bajo su mandato, la vigilancia ha dejado de ser táctica y se ha convertido en doctrina. Lo que se pretende no es gestionar el conflicto, sino eliminarlo antes de que emerja. Se diseña una ciudadanía evaluable, obediente, uniforme. Los avances tecnológicos no se utilizan para ampliar libertades, sino para estrecharlas. La diferencia, que debería constituir el núcleo de la democracia, es tratada como una anomalía estadística.

Este modelo encuentra resonancia en otras latitudes por su promesa de estabilidad. En democracias donde las instituciones han perdido capacidad de respuesta, la imitación resulta tentadora. Se presenta como solución a la complejidad. Como herramienta para disciplinar lo

que se percibe como caos. Pero el costo es alto: se resigna la agencia, se clausura el debate, se reduce la esfera pública a un protocolo de comportamientos permitidos. La ciudadanía deviene una función de datos. Lo político es absorbido por lo técnico.

Incluso en contextos donde existen contrapesos formales, las lógicas de vigilancia se expanden silenciosamente. El ciudadano actual interactúa con dispositivos que recolectan, procesan y analizan sus movimientos, opiniones y hábitos. Esta supervisión ya no se percibe como excepción. Es parte del paisaje cotidiano. Las democracias, al aceptar esta normalización sin reflexión crítica, corren el riesgo de adoptar sin advertirlo las premisas de un orden autoritario. La frontera entre supervisión legítima y control total se vuelve difusa. Lo que antes requería justificación legal, hoy se implementa bajo el amparo de la seguridad preventiva.

La comunidad internacional enfrenta una disyuntiva insoslayable. El problema central no radica en la sofisticación técnica de las herramientas de vigilancia, sino en la ausencia de un marco normativo capaz de contener sus efectos políticos. Si no se articulan regulaciones globales vinculantes que delimiten el uso del control algorítmico, lo que se consolidará será una forma de gobierno centrada en la supresión silenciosa del disenso y en la gestión automatizada de la vida colectiva. En ese escenario, el Estado ya no será garante de derechos, sino gestor de previsibilidad. La ciudadanía dejará de ser sujeto de derechos para convertirse en variable de cálculo. El conflicto legítimo será leído como disfunción. La discrepancia como amenaza.

El riesgo, en este momento, no es que la tecnología avance. Es que la política se retraiga. El verdadero peligro reside en la progresiva renuncia al juicio humano, al debate abierto, a la incertidumbre que permite la libertad. Allí donde la seguridad se impone como principio absoluto, lo democrático se desvanece. Y cuando esto ocurre, la eficacia del sistema ya no es un logro, sino una forma de clausura.

Resulta urgente, por tanto, sostener una posición firme. Es imprescindible reforzar las instituciones, defender la privacidad como derecho irrenunciable, establecer límites jurídicos efectivos, garantizar que toda tecnología sea compatible con el principio de dignidad humana. La seguridad es un bien público legítimo, pero sin libertad, sin transparencia, sin espacios de diferencia, esa seguridad se transforma en coacción. Y la coacción, cuando se normaliza, anula la posibilidad de construir futuro. La democracia no puede sobrevivir si abdica de su derecho a equivocarse, a disentir, a cambiar. Frente a la vigilancia sin límites, el verdadero acto de resistencia es seguir eligiendo la incertidumbre de la libertad antes que la tranquilidad del control absoluto.

Declaración de los autores: Los autores aprueban la versión final del artículo.

Declaración de conflicto de interés: Los autores declaran no tener conflicto de interés.

Contribución de los autores:
- Conceptualización: Diego Sebastián Sánchez Chumpitaz.
- Curación de datos: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Análisis formal: Diego Sebastián Sánchez Chumpitaz.
- Investigación: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Metodología: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.
- Redacción – borrador original: Diego Sebastián Sánchez Chumpitaz.
- Redacción – revisión y edición: Diego Sebastián Sánchez Chumpitaz; Jorge Enrique Abarca Del Carpio.

Financiamiento: Este estudio ha sido autofinanciado como parte de un proyecto académico en la Universidad San Ignacio de Loyola (Lima, Perú), con el objetivo de contribuir al análisis de la seguridad internacional, la gobernanza digital y los derechos humanos en el contexto global.

REFERENCIAS BIBLIOGRÁFICAS

国务院关于重组社会信用体系建设部际联席会议的批复 (Aprobación del Consejo de Estado sobre la reestructuración de la conferencia interministerial para la construcción del sistema de crédito social), Pub. L. No. 国函〔2012〕88号, Consejo de Estado de la República Popular 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). La integración de la excelente cultura tradicional china en la enseñanza del inglés (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.