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

Artículo de reflexión/ Reflection 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. Lima, Perú.*

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.

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

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.

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

La República Popular China (RPC) ha establecido una infraestructura de vigilancia digital sin precedentes en la historia reciente, convirtiéndose en el modelo más sofisticado de control estatal basado en Inteligencia Artificial (IA), Big Data y el Sistema de Crédito Social (SCS). Con más de 1,400 millones de habitantes, el Partido Comunista Chino (PCCh) ha desarrollado un aparato que no se limita a la optimización de la seguridad y la estabilidad interna, sino que redefine el concepto de supervisión gubernamental a nivel global (Nguyen et al., 2023). La integración de tecnologías como el reconocimiento facial, la analítica predictiva y la automatización de decisiones ha permitido al Estado gestionar riesgos sociales con una precisión inigualable, pero esto ha llevado a una restricción sistemática de libertades individuales (Vickers, 2022).

El problema trasciende las fronteras chinas: Beijing exporta su modelo a diversos países mediante la Iniciativa de la Franja y la Ruta (BRI), proporcionando infraestructura digital y herramientas de monitoreo que han sido adoptadas en contextos donde las instituciones democráticas son débiles o los regímenes buscan consolidar su control (Oliveira et al., 2020). Este fenómeno, que podría denominarse *proceso de contagio autoritario*, ha permitido que naciones como Venezuela, Irán o Rusia implementen mecanismos similares bajo la justificación de garantizar la seguridad nacional (Greitens et al., 2020). Como resultado, un desplazamiento progresivo hacia modelos de gobernanza digital en los que la vigilancia se normaliza y la autonomía del ciudadano se ve peligrosamente limitada (Segal, 2025).

Occidente no es ajeno a esta tendencia. En Estados Unidos, la Agencia de Seguridad Nacional (NSA), Federal Bureau of Investigation (FBI) y Central Intelligence Agency (CIA) han desarrollado programas de vigilancia masiva bajo el argumento de la lucha contra el terrorismo y la ciberseguridad, lo que demuestra que el dilema entre libertad y control no es exclusivo de regímenes autoritarios (Feldstein, 2019). Sin embargo, la diferencia radica en los contrapesos institucionales y la existencia de regulaciones que limitan la instrumentalización política de la supervisión digital (Cancela-Outeda, 2024). Mientras en la RPC la vigilancia está institucionalizada dentro del aparato estatal, en la Unión Europea el *AI Act*[1] y otras normativas buscan establecer mecanismos de transparencia en el uso de la IA, evitando que se convierta en una herramienta de represión indiscriminada (Barredo Arrieta et al., 2020).

La influencia china en la gobernanza digital global no se limita a la infraestructura tecnológica. También ha redefinido la manera en que se conciben las narrativas sobre el poder estatal, la seguridad y la estabilidad social, promoviendo una versión del desarrollo tecnológico en la que la eficiencia y el control prevalecen sobre las libertades individuales (Castellanos-Claramunt, 2023; Zhang & Shaw, 2023). La legitimación de este modelo a través de discursos oficiales ha permitido suavizar las críticas internacionales, consolidando un marco de referencia en el que la vigilancia que, además de ser aceptada, es promovida como una necesidad imperativa en la era digital (Xi, 2014).

Este estudio examina la expansión del modelo de vigilancia de Beijing y su impacto en la seguridad internacional y los derechos humanos. A través del análisis de casos concretos y la arquitectura tecnológica que lo sustenta, se evaluará cómo su exportación transforma la gobernanza global. Asimismo, se abordarán las implicaciones de la IA en la estabilidad geopolítica y los desafíos normativos que enfrenta la comunidad internacional para evitar la consolidación del autoritarismo digital.

[1]El *Artificial Intelligence Act* (AI Act) es una propuesta legislativa de la Unión Europea que establece un marco normativo para el desarrollo, comercialización y uso de sistemas de inteligencia artificial dentro del mercado europeo. Su enfoque se basa en la clasificación de riesgos, restringiendo aplicaciones que puedan vulnerar derechos fundamentales, tales como la vigilancia biométrica masiva en espacios públicos. Esta regulación busca garantizar la transparencia, la supervisión independiente y el respeto a principios éticos en el uso de la I. A. (European Commission, 2021).

DESARROLLO

El modelo de vigilancia de la RPC: Fundamentos y Evolución

El modelo de vigilancia desarrollado por el gobierno de la RPC ha evolucionado de manera acelerada, consolidándose como un componente central en su estrategia de seguridad nacional y gobernanza digital. No es una simple red de monitoreo pasivo, sino una estructura de control en la que la IA, el análisis de *big data*[2] y el SCS convergen para generar un ecosistema de observación, evaluación y regulación del comportamiento ciudadano. Su implementación responde tanto a la estabilidad interna como a la consolidación del liderazgo tecnológico del PCCh en la era digital (Creemers, 2018; Feldstein, 2019).

El control estatal en la RPC inicialmente se sustentaba en redes de supervisión comunitaria organizadas a nivel vecinal. Sin embargo, la modernización económica y la urbanización acelerada de los años 80 evidenciaron la obsolescencia de estos métodos rudimentarios. La transición hacia un sistema más avanzado resultó inevitable, especialmente en un contexto en el que la China de Deng Xiaoping, bajo la política de **Reforma y Apertura**[3] (改革开放,*Gǎigé Kāifàng*), priorizaba la modernización de sus estructuras estatales para mantener la estabilidad social en medio de un crecimiento económico sin precedentes. La transformación del modelo de vigilancia se enmarcó en esta estrategia de consolidación del control estatal, en un momento en que el país comenzaba a posicionarse como una potencia en la revolución digital. Fue en este marco que, a inicios del año 2000, el gobierno implementó el proyecto **Escudo Dorado** (金盾工程, *Jīndùn Gōngchéng*) conocido a nivel internacional como el **Gran Cortafuegos de China** (*Great Firewall of China*[4], 防火长城, *Fánghuǒ Chángchéng*). Este sistema marcó un hito al permitir la regulación del tráfico digital, restringiendo el acceso a contenidos externos considerados perjudiciales para la estabilidad del régimen (Feldstein, 2019).

La introducción de la IA en los sistemas de monitoreo a partir de la década de 2010 representó un cambio de paradigma. El SCS, implementado de manera progresiva, opera bajo un esquema de puntuación que clasifica a los ciudadanos según su comportamiento en distintos ámbitos, desde sus interacciones comerciales hasta sus registros administrativos. Estas evaluaciones determinan el acceso a servicios esenciales, configurando un mecanismo de regulación social donde la supervisión se convierte en un eje estructural del modelo de gobernanza estatal (Greitens et al., 2020). Más allá del control individual, la interconexión de sistemas de reconocimiento facial, bases de datos gubernamentales y algoritmos predictivos ha generado un entorno donde la distinción entre lo público y lo privado se vuelve difusa.

Desde una perspectiva económica, la recopilación masiva de datos ha fortalecido el aparato de seguridad del Estado e impulsado la generación de valor a través del análisis avanzado de información en tiempo real. Zeng & Glaister (2018) sostienen que el aprovechamiento del *big data* no depende exclusivamente de la cantidad de datos recolectados, sino de la capacidad del sistema para gestionarlos, contextualizarlos y convertirlos en insumos estratégicos. En la RPC,

[2] *Big data* (macrodatos en español) se refiere al conjunto de datos masivos y complejos que superan la capacidad de procesamiento de las herramientas tradicionales, caracterizándose por su volumen, velocidad y variedad. Su análisis permite identificar patrones en tiempo real para la toma de decisiones estratégicas (Mayer-Schönberger & Cukier, 2013).

[3] La Reforma y Apertura fue la política implementada por Deng Xiaoping en 1978, orientada a la modernización económica de China a través de la liberalización de sectores estratégicos, la apertura gradual al comercio exterior y la atracción de inversión extranjera. Este proceso marcó la transición del país desde una economía planificada hacia un modelo de socialismo de mercado, impulsando un crecimiento sin precedentes y consolidando a la RPC como una potencia global.

[4] La denominación *Great Firewall of China* (idioma inglés, en adelante *GFW*), constituye un juego de palabras con la expresión *Great Wall of China* (Gran Muralla China), estableciendo un paralelismo simbólico entre la función histórica de la muralla como barrera física defensiva y el rol del *GFW* como una infraestructura de control digital que delimita y supervisa el flujo de información en el ciberespacio, protegiendo los intereses del Estado chino frente a influencias externas e internas.

esta dinámica ha sido aplicada tanto en la planificación gubernamental como en el desarrollo de infraestructuras de control, consolidando un ecosistema en el que la información se convierte en el pilar de la toma de decisiones estatales.

La evolución del sistema de vigilancia en la RPC ha seguido un proceso de sofisticación progresiva, alineándose con el desarrollo tecnológico y los imperativos estratégicos del Estado. Desde sus inicios con estructuras de supervisión comunitaria hasta la consolidación de un ecosistema de monitoreo basado en IA y *big data*, el aparato de control ha transitado de una vigilancia descentralizada a una infraestructura digital interconectada con capacidades predictivas y reguladoras. La tabla 1 sintetiza las principales fases de esta transformación, resaltando la integración de tecnologías avanzadas y su impacto en la gobernanza estatal. El análisis de esta trayectoria evidencia la transición hacia un modelo en el que la vigilancia masiva y la regulación algorítmica convergen como pilares fundamentales del control social, configurando un marco de supervisión estatal de alcance global.

Tabla 1. *Evolución del modelo de vigilancia de la RPC*

Década	Características Principales	Tecnologías Clave	Impacto en la Sociedad
1980s	Vigilancia comunitaria tradicional	Redes vecinales, control humano	Control localizado, limitado a entornos pequeños
1990s	Digitalización inicial de datos	Bases de datos rudimentarias	Mejora en la recolección de información
2000s	Implementación del Golden Shield	Censura en internet, control de tráfico web	Restricción del acceso a información global
2010s	Expansión del sistema de crédito social	I. A., *big data*, reconocimiento facial	Evaluación del comportamiento ciudadano en tiempo real
2020s	Exportación del modelo y sofisticación del control	Algoritmos predictivos, ciberseguridad avanzada	Normalización de la vigilancia masiva y control internacional

Fuente: Elaboración propia basada en Creemers (2018), Feldstein (2019), Greitens, Lee y Yazici (2020), y Mac Síthigh & Siems (2019).

El modelo de vigilancia de la RPC ha trascendido sus fronteras mediante la Iniciativa de la Franja y la Ruta (BRI), promoviendo la adopción de tecnologías de monitoreo en países con marcos regulatorios débiles. Esta expansión ha permitido la consolidación de esquemas de supervisión que refuerzan el control estatal y reconfiguran el equilibrio geopolítico (Mac Síthigh & Siems, 2019). En contextos con menor capacidad institucional, la integración de estas infraestructuras ha facilitado el fortalecimiento de regímenes con tendencias autoritarias. La evolución del modelo revela un proceso de sofisticación en el que la IA y los algoritmos predictivos han transformado la relación entre seguridad y derechos fundamentales. A medida que estas herramientas se integran en diferentes sistemas políticos, emergen estructuras de vigilancia que intensifican la tensión entre el ejercicio de la soberanía estatal y la protección de las libertades individuales. El monitoreo digital, lejos de operar únicamente como un mecanismo de seguridad, redefine la gobernanza estatal y desafía la solidez de los marcos jurídicos diseñados para garantizar privacidad y autonomía en la era digital.

Inteligencia Artificial (IA) y el Sistema de Crédito Social (SCS) como pilares del control social

El SCS ha evolucionado como un mecanismo central dentro del aparato de gobernanza digital de la RPC, articulando vigilancia, análisis de datos y disciplina social en un solo sistema. La sofisticación de este modelo reside tanto en la recolección masiva de información como en la capacidad del Estado para clasificar, predecir y condicionar comportamientos ciudadanos con base en parámetros de "confiabilidad" definidos desde la estructura de poder (Nguyen et al., 2023). A diferencia de estrategias tradicionales de control, el SCS no se basa en coerción directa, sino en un sistema de *incentivos y restricciones que fomentan la autorregulación*. La dinámica de este modelo genera un entorno donde la adhesión a las normas es monitoreada en tiempo real, afectando la vida cotidiana de manera integral y minimizando los márgenes de acción individual sin supervisión estatal.

El funcionamiento de este sistema se basa en una infraestructura tecnológica altamente interconectada. Redes de vigilancia en tiempo real, reconocimiento facial y bases de datos que registran interacciones digitales y transacciones económicas permiten un monitoreo sistemático de la actividad social y financiera[5]. La asignación de puntuaciones en función del cumplimiento normativo y la conducta individual condiciona el acceso a servicios esenciales, como transporte, vivienda, educación y asistencia médica (Greitens et al., 2020). En consecuencia, los ciudadanos ajustan sus comportamientos en función de la previsión de recompensas o sanciones, generando una lógica de control social anticipatorio[6] que desplaza la noción de supervisión clásica hacia un modelo de regulación algorítmica omnipresente (Wright, 2018).

El impacto del SCS varía en distintos aspectos de la vida cotidiana, generando una división marcada entre sus efectos percibidos como positivos y los costos en términos de derechos fundamentales. Mientras que algunos sectores defienden su implementación al considerar que mejora la eficiencia en la provisión de servicios públicos y contribuye a la reducción de delitos menores, las preocupaciones sobre su aplicación se centran en la erosión de la privacidad, la restricción de la libertad de expresión y el reforzamiento de desigualdades estructurales dentro del sistema socioeconómico (Drexel & Kelley, 2023). La supervisión estatal, en lugar de ser un mecanismo limitado a la seguridad pública, ha evolucionado hasta convertirse en una herramienta que moldea la vida de los ciudadanos mediante el acceso condicionado a oportunidades y servicios esenciales.

El impacto del SCS en la sociedad se manifiesta en múltiples dimensiones, modificando la manera en que los ciudadanos acceden a bienes y servicios esenciales. La siguiente tabla 2 presenta datos cuantitativos sobre los efectos positivos y negativos del SCS en la movilidad, el empleo y el acceso a recursos fundamentales.

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 expansión del SCS ha trascendido el ámbito doméstico, consolidándose como un modelo replicable en escenarios donde el control estatal se refuerza a través de herramientas digitales. Wang (2021) señala que esta proliferación no se limita a la transferencia de tecnología, sino que introduce esquemas regulatorios que favorecen la estabilidad del régimen sobre la protección de derechos individuales. La creciente adopción de estas infraestructuras en sistemas de seguridad nacional plantea desafíos en la administración de datos sensibles, incrementando los riesgos de injerencias externas y alterando el equilibrio de poder en el ciberespacio.

El desarrollo acelerado de infraestructuras de vigilancia digital ha generado vulnerabilidades críticas en términos de ciberseguridad y geopolítica. Knieps (2024) advierte que la expansión de redes interconectadas para la recopilación y gestión de datos incrementa el riesgo de ataques cibernéticos, espionaje estatal y manipulación de información. En este contexto, la instrumentalización de estos sistemas ha trascendido el control ciudadano para convertirse en una herramienta con implicancias interestatales. Segal (2025) documenta cómo incidentes

[5] La recopilación y análisis constante de datos permite al Estado evaluar en tiempo real el comportamiento de los ciudadanos en distintas esferas, desde sus transacciones financieras hasta sus interacciones en entornos digitales y su historial de movilidad. Esta información es procesada a través de algoritmos que asignan puntuaciones de confiabilidad, afectando el acceso a servicios esenciales y regulando la participación de los individuos en la economía y la sociedad.

[6] La supervisión del comportamiento no se limita a la detección de infracciones pasadas, sino que se fundamenta en algoritmos predictivos que identifican patrones de riesgo antes de que ocurran eventos específicos. A partir de este análisis, el sistema puede restringir libertades o modificar accesos con el objetivo de prevenir desviaciones normativas, estableciendo un mecanismo de regulación basado en la anticipación de conductas potencialmente problemáticas.

como la operación "*Salt Typhoon*[7]" muestran que la vigilancia digital impacta tanto a individuos bajo supervisión estatal como a la dinámica de las disputas estratégicas entre Estados, aumentando el riesgo de tensiones geopolíticas.

Los datos de la tabla 3 evidencian que Medio Oriente (69,8%) y Asia (61,5%) presentan la mayor adopción de tecnología de vigilancia digital proveniente de la RPC, mientras que África (48,0%) y América Latina (43,5%) registran una integración más moderada. Europa del Este (38,2%) muestra la menor cobertura, lo que sugiere diferencias en la incorporación de estos sistemas según el contexto geopolítico y los marcos regulatorios de cada región. La expansión de estas infraestructuras tecnológicas responde a acuerdos de cooperación, al mismo tiempo que evidencia la consolidación de estrategias de supervisión digital utilizadas como herramienta de control estatal.

El análisis comparativo entre la tabla 2 y la tabla 3 confirma una correlación entre la extensión de estas tecnologías y la intensificación de restricciones a derechos fundamentales. Regiones con mayor cobertura, como Medio Oriente y Asia, registran niveles más altos de limitaciones en movilidad, acceso a oportunidades económicas y autonomía ciudadana. Este fenómeno trasciende las justificaciones de seguridad y se inscribe en una arquitectura de control global[8], donde el acceso a información y servicios queda supeditado a sistemas de monitoreo sistemático (Segal, 2025).

Tabla 3. *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)

La tecnología, lejos de ser neutral, ha sido utilizada estratégicamente para reforzar estructuras de poder a través de la regulación predictiva del comportamiento social. Dentro del SCS, la adhesión a normativas no surge de un consenso deliberativo, sino que resulta de un proceso de condicionamiento en el que sistemas algorítmicos anticipan patrones de conducta y limitan la capacidad de acción individual antes de que esta ocurra (Neuberger, 2025; Wright, 2018). En este escenario, el modelo chino de supervisión no se limita a responder ante infracciones, sino que opera bajo una lógica de prevención y restricción proactiva[9].

La diseminación de estas tecnologías fuera de la RPC no se limita a la transferencia de *software* y *hardware* de vigilancia, sino que también conlleva la adopción de marcos de gobernanza que refuerzan estructuras de control digital a gran escala. Wang (2021) sostiene que este fenómeno ha impulsado la institucionalización de sistemas autoritarios bajo el pretexto de garantizar seguridad y estabilidad, lo que obstaculiza la consolidación de regímenes democráticos y genera barreras estructurales que restringen la transparencia y la rendición de cuentas. La expansión del SCS ha trascendido el ámbito nacional y ha sido adoptada en diversos contextos políticos, configurando un modelo replicable de control estatal digitalizado.

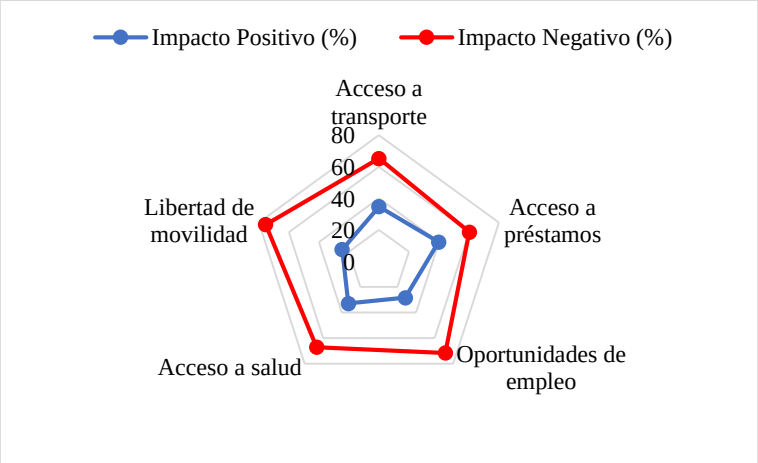
[7] *Salt Typhoon*, conocido en español como *Tifón de Sal*, designa a un grupo de Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés) vinculado al Ministerio de Seguridad del Estado de la RPC. Este colectivo se especializa en operaciones de ciber espionaje, destacándose por la infiltración en redes de telecomunicaciones en los Estados Unidos de América con el propósito de interceptar comunicaciones sensibles y obtener información estratégica de inteligencia (Forno, 2024).

[8] Se refiere a la consolidación de un marco de vigilancia digital transnacional, donde la recopilación, procesamiento y uso de datos no están restringidos a las fronteras nacionales: se integran en sistemas interoperables que permiten el monitoreo coordinado de individuos a nivel interestatal. Este fenómeno ha sido facilitado por la convergencia de I. A., *big data* y redes de telecomunicaciones avanzadas, generando preocupaciones sobre la soberanía digital y la autonomía individual en la era de la hiperconectividad (Zuboff, 2019).

[9] En el contexto del SCS implica la implementación de sistemas predictivos que además de identificar conductas potencialmente problemáticas, aplican restricciones anticipadas para evitar su ocurrencia. Este enfoque se basa en técnicas de aprendizaje automático y modelado algorítmico de riesgos, alineándose con estrategias de *pre-crime governance*, un paradigma que desplaza la función tradicional del Estado de sancionar delitos consumados hacia la regulación de probabilidades conductuales (Amoore, 2020).

La expansión del SCS ha generado impactos significativos en múltiples dimensiones sociales, consolidándose como un pilar estructural de control digital. La figura 1 muestra cómo este sistema afecta la movilidad, el acceso al empleo y la disponibilidad de servicios esenciales. El análisis de los datos evidencia que los impactos negativos superan ampliamente los beneficios percibidos. En términos de acceso a préstamos, el 60,2% de los encuestados experimenta restricciones, mientras que, en movilidad, la afectación alcanza el 75,5%. La supervisión algorítmica no regula únicamente la conducta individual, sino que, además, establece criterios que determinan el acceso a oportunidades económicas y sociales (Nguyen et al., 2023; Segal, 2025).

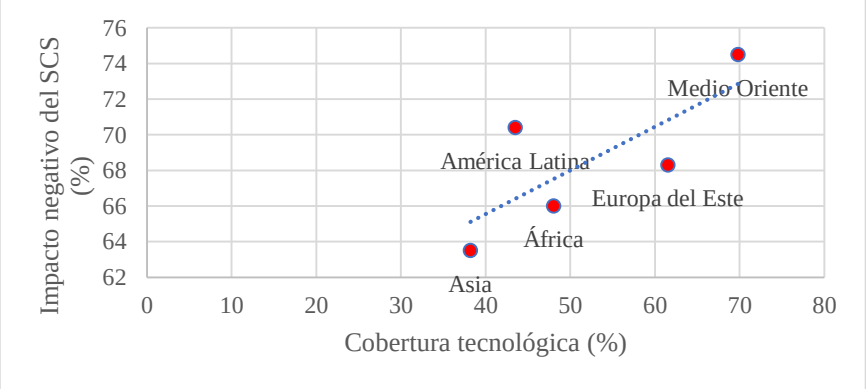
Figura 1. *Impacto del SCS en diferentes aspectos sociales en relación con la cobertura tecnológica regional*



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

La correlación entre la cobertura tecnológica del SCS y el incremento de restricciones a derechos fundamentales se refleja en la Figura 2. Medio Oriente y Asia, con niveles de penetración del 69,8% y 61,5%, respectivamente, presentan los mayores niveles de restricciones. América Latina, con una menor penetración tecnológica (43,5%), registra impactos negativos considerables, lo que indica que el efecto del SCS depende de la presencia de la tecnología, así como de los marcos regulatorios preexistentes. La arquitectura de control global que configura este modelo se articula en función de la capacidad estatal para integrar mecanismos de supervisión en sus estructuras de gobernanza.

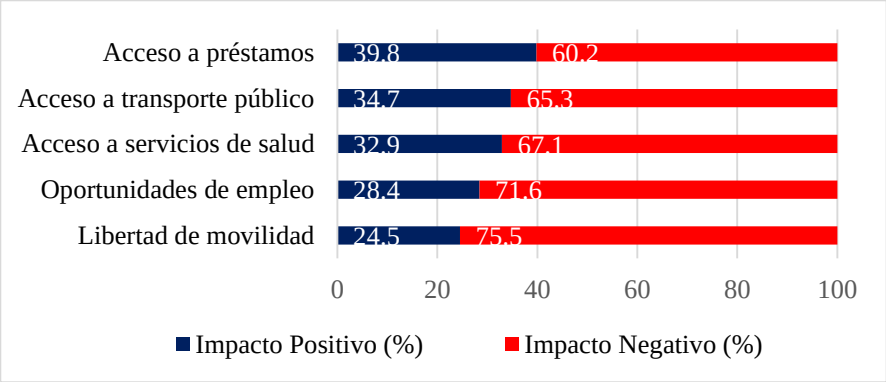
Figura 2. *Correlación entre la cobertura de tecnología de vigilancia y el impacto negativo del SCS por región*



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

La Figura 3 refuerza esta tendencia al comparar el impacto positivo y negativo del SCS en distintos ámbitos. Los datos muestran que la movilidad y el acceso al empleo son los más afectados, con restricciones que alcanzan el 75,5% y el 71,6%, respectivamente. Skare et al. (2024) advierten que la adopción de estos mecanismos en economías con desigualdades estructurales tiende a consolidar modelos de exclusión social, limitando la movilidad económica y reforzando sistemas de estratificación digital. A medida que el SCS se expande fuera de la RPC, su impacto se amplifica en mercados emergentes, donde la falta de regulación favorece la normalización de estos esquemas de control.

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



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

El crecimiento de esta infraestructura tecnológica no se limita a la supervisión nacional, sino que se vincula con un proceso de difusión normativa que fortalece modelos de gobernanza basados en la vigilancia digital. Wang (2021) argumenta que la exportación de estas tecnologías impulsa la institucionalización de sistemas autoritarios bajo el argumento de garantizar seguridad y estabilidad, lo que dificulta la consolidación de regímenes democráticos y obstaculiza la transparencia y la rendición de cuentas. Esta dinámica ha reforzado la dependencia tecnológica de los Estados receptores, promoviendo la adopción de marcos regulatorios restrictivos que consolidan la vigilancia como un componente esencial del aparato estatal.

El fenómeno conocido como *contagio autoritario* se manifiesta en la incorporación progresiva de estos sistemas en las estructuras de supervisión gubernamental. La expansión de tecnologías de monitoreo en mercados emergentes no se limita a la transferencia de *hardware* y *software*, sino que también fomenta un modelo de gobernanza donde la automatización del control social se presenta como un mecanismo para optimizar la eficiencia estatal. Drexel & Kelley (2023) y Neuberger (2025) advierten que la ausencia de regulaciones supranacionales que frenen la proliferación de estos esquemas podría acelerar la erosión estructural de los derechos fundamentales, debilitando los principios democráticos y favoreciendo la consolidación de sistemas de supervisión automatizados.

La exportación del modelo chino: implicancias en la gobernanza global

El modelo chino de gobernanza digital se ha convertido en un instrumento de proyección de poder más allá de sus fronteras, consolidándose como un esquema de expansión que fusiona infraestructura tecnológica avanzada, estrategias de inversión y transferencia de capacidades en mercados con marcos regulatorios más flexibles. La convergencia entre IA, *big data* y sistemas de vigilancia no permanece confinada al ámbito doméstico, sino que se despliega a través de acuerdos estratégicos que refuerzan la dependencia tecnológica y fortalecen la influencia normativa de China en el ciberespacio global (Zhu et al., 2014).

El análisis de la penetración de estas infraestructuras muestra una tendencia clara: los países con menor capacidad de regulación tecnológica han sido los más receptivos a la implementación de estos sistemas. De acuerdo con Wu et al. (2024), la exportación de soluciones tecnológicas avanzadas por parte de la RPC ha crecido más del 60% en la última

década, consolidando su liderazgo en la transformación digital de diversas economías emergentes. La siguiente tabla sintetiza los principales mecanismos mediante los cuales la RPC expande su modelo de control digital:

Tabla 4. *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).

El impacto de esta expansión se observa con mayor intensidad en regiones donde la dependencia económica y tecnológica de la RPC es significativa. América Latina se ha convertido en un punto estratégico dentro de esta dinámica, con megaproyectos como el puerto de Chancay, que además de fortalecer el comercio bilateral, impulsan la penetración de soluciones digitales en la infraestructura pública (Sánchez Chumpitaz & Asmat Caro, 2024). La tabla 5 presenta datos cuantitativos sobre la presencia tecnológica de la China de Xi Jinping en distintas regiones y su relación con la adopción de modelos de control digital.

Tabla 5. *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 correlación entre presencia tecnológica china y adopción de sistemas de vigilancia digital revela un patrón consistente: la incorporación de estas infraestructuras no se limita a la provisión de hardware y software, sino que conlleva la asimilación de principios regulatorios que consolidan modelos de gobernanza con mayores niveles de supervisión estatal (Li et al., 2020). Chan et al. (2024) explican que la dependencia tecnológica facilita la transferencia de capacidades e introduce marcos regulatorios que, en la práctica, debilitan el margen de maniobra de los Estados receptores para establecer normativas independientes sobre la gobernanza digital.

La expansión del modelo chino de gobernanza digital ha incorporado plataformas tecnológicas diseñadas para optimizar la gestión gubernamental, con aplicaciones en seguridad pública, planificación urbana y administración estatal (Bonsón et al., 2012). Estas infraestructuras han sido adoptadas en distintos países, fortaleciendo la capacidad de supervisión y procesamiento de datos en tiempo real. La tabla 6 presenta un conjunto de plataformas digitales exportadas por China y sus funciones en los Estados receptores, evidenciando la integración de soluciones basadas en IA y vigilancia masiva dentro de esquemas administrativos y de control estatal.

Tabla 6. *Plataformas digitales de gobernanza exportadas por China*

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).

El impacto de la influencia china en la gobernanza global puede analizarse desde una perspectiva económica, particularmente en la optimización de la logística y la administración mediante inteligencia artificial. La automatización digital ha reconfigurado las cadenas de suministro en diversos sectores, mejorando la eficiencia operativa en puertos y redes de comercio internacional (Sánchez Chumpitaz & Asmat Caro, 2024). La tabla 7 detalla estos impactos en términos de reducción de tiempos y costos en distintos sectores.

Tabla 7. *Impacto de la automatización digital china en logística y comercio internacional*

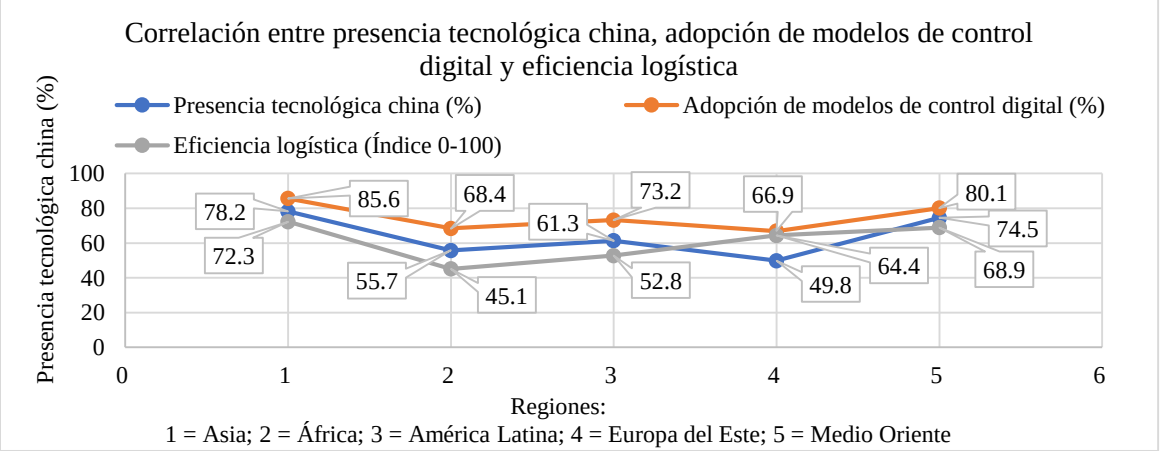
Sector	Reducción de Costos (%)	Disminución de Tiempos de Procesamiento (%)
Transporte marítimo	24,50	36,80
Logística de puertos	30,20	42,10
Comercio electrónico	28,70	40,50
Administración aduanera	22,30	33,60

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

La exportación del modelo chino de gobernanza digital no se reduce a un proceso de transferencia tecnológica, sino que implica una reconfiguración de los principios normativos y estructurales de los países receptores. A través de la inversión en infraestructura, la estandarización de procesos y la adaptación de modelos regulatorios, China ha consolidado su posición como actor central en la transformación digital a escala global.

La Figura 4 muestra la relación entre la presencia tecnológica china, la adopción de modelos de control digital y su efecto en la eficiencia logística y comercial en los países receptores, evidenciando patrones de integración y optimización en distintos contextos geopolíticos.

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).

Vigilancia digital y reconfiguración del orden internacional: seguridad, derechos humanos y desafíos estratégicos en la era del autoritarismo tecnológico.

La evolución de la vigilancia digital ha transformado el equilibrio de poder en el sistema internacional, modificando las relaciones entre el Estado y la ciudadanía, redefiniendo la percepción de seguridad y consolidando nuevos paradigmas de gobernanza autoritaria. La interconexión entre IA, *big data* y monitoreo masivo ha permitido a los gobiernos gestionar el comportamiento social con un alcance sin precedentes, alterando las fronteras entre protección y restricción de derechos.

En la RPC, el modelo de supervisión estatal se ha expandido bajo la doctrina de estabilidad política de Xi Jinping, que refuerza la idea de la seguridad como un eje del desarrollo nacional (Xi, 2014). El SCS y la red de videovigilancia *Skynet* consolidan una infraestructura de monitoreo permanente que condiciona la movilidad y el acceso a bienes y servicios en función de la confiabilidad asignada a cada ciudadano (Nguyen et al., 2023). La vigilancia ya no responde únicamente a un esquema reactivo, sino a un mecanismo predictivo basado en la regulación algorítmica.

Sandbrink et al. (2024) advierten que la convergencia de tecnologías emergentes con sistemas de control estatal ha fortalecido esquemas de supervisión anticipada que limitan la autonomía individual y amplían la capacidad de intervención gubernamental. La implementación de estos modelos en sistemas políticos con baja rendición de cuentas refuerza la tendencia hacia el autoritarismo digital. Adeyeye & Grobbelaar (2024) destacan que la consolidación de infraestructuras de monitoreo en países con debilidades institucionales no solo optimiza el control estatal, sino que también transforma la estructura misma de la gobernanza, desplazando la toma de decisiones hacia mecanismos automatizados que configuran nuevas dinámicas de poder.

El modelo chino se ha expandido a través de la Iniciativa de la Franja y la Ruta (BRI), facilitando la adopción de tecnología de vigilancia en Estados con debilidades institucionales o tendencias autoritarias (Rocha Pino, 2017). Gobiernos como los de Venezuela, Irán, Rusia y Arabia Saudita han integrado estas infraestructuras digitales para fortalecer el control social, restringir el acceso a información y suprimir la disidencia mediante mecanismos de supervisión estatal reforzada (Mozur et al., 2019).

El análisis empírico de estas dinámicas muestra que los Estados con mayor implementación de tecnología de vigilancia digital tienden a registrar una percepción elevada de seguridad. En la tabla 8, la RPC, con un uso del 100 % de tecnología china, reporta una percepción de seguridad del 85,4 %, mientras que países como Venezuela e Irán, con menores niveles de adopción tecnológica (79 % y 76 %, respectivamente), presentan valores más bajos en esta percepción. Estos datos sugieren que la vigilancia digital es vista como un factor de estabilidad, aunque su impacto en la seguridad real y en los derechos ciudadanos sigue siendo un punto de debate.

Tabla 8. *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).

Si bien la adopción de tecnología de vigilancia china está vinculada a una percepción elevada de seguridad debido al monitoreo continuo de la población, su implementación también conlleva efectos adversos en términos de derechos humanos y libertades individuales. La tabla 9 muestra que los países con altos niveles de vigilancia digital presentan restricciones significativas en la libertad de expresión y la privacidad. En la RPC, donde el 92,3 % de la población enfrenta limitaciones en la libertad de expresión y el 94,8 % en la privacidad, se han documentado más de 135 000 casos de represión política en los últimos cinco años. Tendencias similares se observan en Venezuela, Irán y Arabia Saudita, donde las tasas de censura y control

social son elevadas. Estos datos evidencian que la vigilancia digital, aunque percibida como un mecanismo de seguridad, opera como un instrumento de supervisión estatal que afecta el ejercicio de derechos fundamentales.

Tabla 9. *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).

El análisis conjunto con la tabla 8 y la tabla 9 revela que la presencia de tecnología de vigilancia se asocia con una percepción de seguridad elevada, aunque también con restricciones significativas en derechos fundamentales. En la RPC, donde el monitoreo digital alcanza el 100%, la seguridad percibida es del 85,4%, pero la libertad de expresión y la privacidad se ven afectadas en un 92,3% y 94,8%, respectivamente, con más de 135 000 casos documentados de represión política. Patrones similares se replican en Venezuela, Irán y Arabia Saudita, lo que confirma que la vigilancia estatal no se limita a la seguridad, sino que además configura un ecosistema de supervisión que condiciona el ejercicio de derechos ciudadanos.

Los modelos de vigilancia digital analizados en la tabla 10 muestran que, aunque se presentan como mecanismos de seguridad y estabilidad, su implementación ha estado marcada por el control social, la censura y la represión política. En la RPC, el SCS y *Skynet* operan como herramientas de supervisión masiva, mientras que, en Venezuela, Irán, Arabia Saudita y Rusia, sistemas como el Carnet de la Patria, el filtrado de contenido y la interceptación de comunicaciones han sido utilizados para monitorear a la ciudadanía y restringir el acceso a información.

Tabla 10. *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).

La tabla 11 evidencia la relación entre el uso de tecnologías de vigilancia y la restricción de libertades, reflejando cómo estos sistemas refuerzan el control estatal. La RPC, con una adopción del 100%, presenta el mayor nivel de restricciones (94,8%), consolidando su modelo de supervisión digital. Venezuela e Irán, con tasas del 79% y 76%, muestran restricciones superiores al 87%, lo que indica que estos mecanismos van más allá de la seguridad e impactan el ámbito político y social. Stanger et al. (2024) señalan que la expansión de estas infraestructuras tiende a fortalecer marcos regulatorios más restrictivos, limitando la autonomía individual. Nigeria, con una menor adopción (55%), mantiene restricciones significativas (74,5%), lo que sugiere que el impacto de la vigilancia no depende únicamente de su alcance, sino del contexto normativo. Ding (2018) enfatiza que estos sistemas reconfiguran el poder estatal, donde el acceso a herramientas de supervisión refuerza dinámicas de control con efectos que trascienden la seguridad.

Tabla 11. *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).

El desarrollo y expansión de estos sistemas de monitoreo han generado la necesidad de medir su impacto en la gobernanza y en la relación entre seguridad, vigilancia y restricciones de derechos. Para ello, se ha diseñado el *Índice de Control Estatal* (ICE o I_c), una herramienta que modela esta interacción en regímenes con supervisión intensiva. Su formulación matemática permite analizar cómo la seguridad percibida contribuye a la legitimidad del Estado, mientras que el aumento en la vigilancia digital y las limitaciones a las libertades implican costos políticos que pueden influir en la estabilidad del régimen.

El *ICE* cuantifica la relación entre percepción de seguridad (S), vigilancia digital (V) y restricción de libertades (L) en regímenes con sistemas de supervisión intensiva. La RPC ha desarrollado un modelo basado en IA y macrodatos, que se ha convertido en referencia para Estados con tendencias autoritarias y se ha expandido a través de la Iniciativa de la Franja y la Ruta (Nguyen et al., 2023; Rocha Pino, 2017).

La formulación matemática del *ICE* busca cuantificar la interacción entre seguridad percibida, vigilancia digital y restricción de libertades en regímenes con supervisión intensiva. Una mayor percepción de seguridad tiende a legitimar el control estatal, mientras que el alcance de la vigilancia digital determina la capacidad del Estado para regular el comportamiento ciudadano. En contraste, el aumento en las restricciones a las libertades genera costos políticos que pueden afectar la estabilidad del régimen. Para modelar esta dinámica y aportar un marco analítico a su estudio, se propone la siguiente ecuación:

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

Los coeficientes $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ y $\boldsymbol{\gamma}$ han sido calibrados con base en estudios comparativos de múltiples países. En este modelo, $\boldsymbol{\alpha}$ (alfa) pondera la percepción de seguridad, ya que la confianza en el Estado facilita su capacidad de control. Luego, $\boldsymbol{\beta}$ (beta) mide el impacto de la vigilancia digital en la consolidación del poder estatal. En cambio, $\boldsymbol{\gamma}$ (gama) cuantifica el desgaste político derivado de la represión, ya que niveles elevados de restricciones pueden erosionar la legitimidad y generar oposición social (Mozur et al., 2019).

Para evaluar la aplicación del ICE, se analizaron los casos de la RPC y Nigeria, dos Estados con diferentes grados de consolidación del control digital. En el caso de la RPC, los valores empíricos reflejan una percepción de seguridad alta ($\boldsymbol{S = 85{,}4}$), un sistema de vigilancia digital total ($\boldsymbol{V = 100}$) y restricciones severas a las libertades ($\boldsymbol{L = 98{,}4}$). Con coeficientes ajustados de $\boldsymbol{\alpha = 0{,}8}$, $\boldsymbol{\beta = 1{,}2}$ y $\boldsymbol{\gamma = 1{,}5}$, se obtiene:

$$\boldsymbol{I_c = (0{,}8 \times 85{,}4) + (1{,}2 \times 100) - (1.5 \times 94{,}8)}$$

$$\boldsymbol{I_c = 68{,}32 + 120 - 142{,}2}$$

$$\boldsymbol{I_c = 46{,}12}$$

Los hallazgos obtenidos confirman que la RPC mantiene un ICE elevado, evidenciando la eficiencia de su infraestructura de vigilancia para garantizar estabilidad política y consolidar el dominio del PCCh. La integración del SCS y la red de videovigilancia *Skynet* ha fortalecido la capacidad gubernamental para monitorear el comportamiento ciudadano y moldearlo a través de sistemas algorítmicos de incentivos y sanciones (Nguyen et al., 2023; Xi, 2014). La institucionalización de este esquema ha sido respaldada por marcos regulatorios promovidos por el Consejo de Estado de la RPC (2012), estableciendo un marco normativo que legitima la

aplicación de tecnologías de supervisión para restringir el acceso a servicios y consolidar un modelo de gobernanza digital altamente centralizado.

Por otro lado, Nigeria, la adopción de infraestructura de vigilancia financiada por la RPC ha sido parcial y con menor consolidación tecnológica. Los datos reflejan una percepción de seguridad baja ($\boldsymbol{S = 58{,}4}$), un nivel de vigilancia moderado ($\boldsymbol{V = 55}$) y restricciones significativas a las libertades ($\boldsymbol{L = 74{,}5}$). Aplicando la ecuación con los mismos coeficientes:

$$\boldsymbol{I_c = (0{,}8 \times 58{,}5) + (1{,}2 \times 55) - (1{,}5 \times 74{,}5)}$$

$$\boldsymbol{I_c = 46{,}8 + 66 - 111{,}75}$$

$$\boldsymbol{I_c = 1{,}05}$$

El **ICE** para Nigeria es **1,05**, reflejando un control estatal débil pese a la implementación parcial de vigilancia digital financiada por Beijing. La baja percepción de seguridad y la falta de legitimación social han impedido consolidar un modelo efectivo (Feldstein, 2019). En contraste, la RPC presenta un **ICE** de **46,12**, reflejando la efectividad de su infraestructura de monitoreo, basada en el SCS y *Skynet*, para fortalecer la estabilidad política y reforzar el control gubernamental (Nguyen et al., 2023; Xi, 2014).

La comparación entre ambos países muestra una diferencia sustancial en la gestión de la vigilancia digital. Mientras que en la RPC la combinación de I. A., análisis predictivos y mecanismos de supervisión ha permitido un control estatal altamente consolidado, Nigeria, con una percepción de seguridad de **58,4**, un nivel de vigilancia de **55** y restricciones de libertades de **74,5**, no ha logrado establecer una estructura de control similar. La ausencia de una infraestructura tecnológica robusta y la falta de cohesión en sus políticas de supervisión han dificultado la proyección de autoridad estatal mediante estos sistemas (Feldstein, 2019).

Más allá del caso específico de Nigeria, la expansión de modelos de monitoreo digital plantea un desafío geopolítico, en el que la supremacía tecnológica emerge como un nuevo factor en la competencia por el dominio estatal. A medida que más países adopten esquemas de control basados en IA y algoritmos predictivos, la disputa por la información se intensificará, configurando un escenario donde la línea entre seguridad y opresión será cada vez más difusa.

Consideraciones para el diseño de marcos regulatorios internacionales

La expansión acelerada de la IA y las infraestructuras de vigilancia digital ha evidenciado la urgencia de desarrollar marcos regulatorios internacionales que establezcan límites claros a su implementación y prevengan su uso con fines autoritarios. La ausencia de una normativa global coherente ha permitido que algunos Estados estructuren modelos de supervisión basados en tecnologías avanzadas, priorizando el control estatal por encima de la seguridad ciudadana y la protección de datos. Esto ha facilitado la consolidación de regímenes de vigilancia masiva con implicancias directas en los derechos humanos y en la estabilidad del sistema internacional (Ding, 2018; Stanger et al., 2024).

La concentración del poder digital en la RPC ha convertido su modelo de gobernanza en un referente para aquellos gobiernos que buscan fortalecer sus mecanismos de supervisión y administración de la información. Esta tendencia ha impulsado un debate sobre la necesidad de regulaciones que concilien el avance tecnológico con la protección de libertades fundamentales, evitando que la expansión de la IA derive en herramientas de represión política y control social a gran escala (Pearson et al., 2022).

El **GDPR** en la Unión Europea y la **Ley Federal de Privacidad** en EE. UU. han buscado establecer marcos regulatorios para restringir el uso abusivo de la vigilancia digital y la explotación masiva de datos. Sin embargo, estos esfuerzos presentan limitaciones, ya que no abordan de manera integral las implicancias de la I. A. en la esfera pública y privada (Goodman & Flaxman, 2016).

En contraste, la **RPC** ha desarrollado normativas que refuerzan el control estatal sobre los flujos de información y la actividad en línea, consolidando un modelo replicado en Estados con tendencias autoritarias, como Irán, Venezuela y la Federación Rusa (Aoyama, 2022; Vickers, 2022). La tabla 12 presenta una comparación entre distintas jurisdicciones, resaltando la brecha

entre regulaciones orientadas a la privacidad y aquellas diseñadas para fortalecer la supervisión gubernamental.

Tabla 12. *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).

Los marcos regulatorios adoptados por los Estados determinan el grado de supervisión gubernamental y redefinen el nivel de autonomía digital y participación ciudadana en el espacio público (He, 2023). En la RPC, el control tecnológico ha convergido con la política educativa, facilitando la homogenización del discurso y la eliminación de narrativas contrarias al PCCh (Vickers, 2022). Esta dinámica se ha extendido a gobiernos que han recibido asistencia tecnológica de Beijing mediante la BRI, integrando mecanismos de vigilancia en sus modelos de gobernanza (Oliveira et al., 2020). El uso estratégico de la educación como vehículo de control ideológico ha fortalecido la cohesión interna del régimen y consolidado su influencia sobre la estructura sociopolítica nacional (Aoyama, 2022). En entornos con menor capacidad regulatoria, esta combinación entre supervisión digital y estandarización del discurso genera un ecosistema propicio para la replicación de modelos de vigilancia sistémica con mínima resistencia institucional.

Desde una perspectiva de gobernanza global, la regulación de la IA debe considerar los riesgos asociados a su instrumentalización para fines autoritarios. Organismos internacionales han planteado la urgencia de establecer marcos normativos que permitan un equilibrio entre innovación y salvaguarda de derechos fundamentales (Gomes Rêgo de Almeida & Dos Santos Júnior, 2025). La tabla 13 presenta una comparación entre enfoques regulatorios en el ámbito público y privado, destacando la proyección del modelo chino en entornos con menor solidez democrática.

Tabla 13. *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 diseño de marcos regulatorios globales debe contemplar la necesidad de supervisión supranacional para evitar que la IA se convierta en una herramienta de vigilancia sin restricciones. La gobernanza tecnológica no puede quedar supeditada a regulaciones nacionales fragmentadas, sino que requiere mecanismos multilaterales que garanticen transparencia, rendición de cuentas y protección de derechos fundamentales (Stanger et al., 2024). La reciente propuesta de la ONU para establecer un organismo internacional de supervisión de la IA

supone un avance en esta dirección, aunque su implementación enfrenta obstáculos debido a la resistencia de Estados con modelos de gobernanza centralizados (Ding, 2018).

La dimensión geopolítica de la regulación tecnológica es ineludible. La concentración de infraestructuras digitales en manos de actores estatales con agendas expansionistas ha creado asimetrías de poder en el sistema internacional. La dependencia de plataformas de origen chino o estadounidense ha convertido el acceso a la información en un instrumento de influencia estratégica, con implicaciones directas en la seguridad y la estabilidad global (Pearson et al., 2022).

El desarrollo de estándares regulatorios internacionales debe impedir la consolidación de monopolios tecnológicos y frenar la expansión de modelos que emplean la IA como herramienta de represión y vigilancia masiva. Un marco normativo eficaz requiere garantizar la protección de la privacidad y la autonomía digital, al tiempo que prevé mecanismos para contrarrestar la censura algorítmica y establecer auditorías independientes que mitiguen los riesgos derivados de la concentración del poder tecnológico. La capacidad de la comunidad internacional para enfrentar estos desafíos determinará el equilibrio futuro entre el avance tecnológico y el respeto a los derechos fundamentales en un contexto de creciente automatización.

La consolidación de modelos de vigilancia digital basados en IA ha intensificado la capacidad del Estado para modelar el comportamiento social, generando nuevas dinámicas de control que van más allá de la seguridad pública. En la RPC, herramientas como *Skynet* y el SCS han sido utilizadas para condicionar la movilidad, limitar el acceso a servicios y establecer sistemas de puntuación social que refuerzan la obediencia ciudadana (Bergdahl et al., 2023; Shum & Lau, 2024). Esta estrategia se ha expandido a través de la Iniciativa de la Franja y la Ruta, facilitando la adopción de infraestructuras de monitoreo en entornos con regulaciones débiles, donde la tecnología china ha sido instrumentalizada para consolidar regímenes autoritarios (Mozur et al., 2019; Tuzov & Lin, 2024).

En contraste, los Estados democráticos han implementado marcos regulatorios con enfoques divergentes. Mientras la UE ha desarrollado normativas como el *AI Act* para mitigar los riesgos asociados a la automatización, otras jurisdicciones han permitido la expansión de la vigilancia digital bajo el pretexto de la ciberseguridad y la lucha contra el terrorismo (Cancela-Outeda, 2024; Goodman & Flaxman, 2016). Sin embargo, la ausencia de estándares internacionales impide una regulación eficaz, lo que abre la puerta a la proliferación de sistemas de supervisión sin restricciones y a la consolidación de monopolios tecnológicos con agendas políticas definidas. Frente a este escenario, la gobernanza de la IA debe priorizar la transparencia, la supervisión independiente y la protección de la autonomía digital, evitando que el avance tecnológico derive en un instrumento de represión global (Reynoso Vanderhorst et al., 2024). Además, la evolución de los modelos de supervisión en China muestra cómo la intervención estatal ha sido determinante en la transformación de su ecosistema digital, convirtiendo la recopilación masiva de datos en un pilar de su estrategia de desarrollo y consolidando su influencia tecnológica a nivel global (Yang & Liu, 2024).

CONCLUSIONES

La vigilancia digital en la RPC ha trascendido la supervisión estatal tradicional. Se ha consolidado como una estructura omnipresente donde la IA, el *big data* y el SCS han configurado un ecosistema de control sin precedentes. Cada interacción, cada transacción y cada desplazamiento quedan registrados en un sistema que, además de observar, predice, clasifica y sanciona. La seguridad y la estabilidad política han sido los pilares discursivos que justifican la expansión de este modelo. Sin embargo, la pregunta persiste: ¿es viable una sociedad de esta magnitud sin mecanismos de supervisión avanzada, o el costo de este orden es la erosión total de la autonomía individual?

El impacto de este paradigma ha rebasado las fronteras chinas. Estados con regímenes autoritarios han integrado estas infraestructuras bajo el pretexto de fortalecer su seguridad nacional. Venezuela, Irán, Rusia, Arabia Saudita. La implementación de estos sistemas ha dejado en evidencia su verdadero propósito. No fortalecen la seguridad pública. No garantizan

la estabilidad. Configuran una arquitectura de vigilancia permanente, diseñada para controlar la disidencia, restringir el acceso a la información y perpetuar regímenes con legitimidad cuestionable. La percepción de seguridad en estos países ha crecido, pero a costa de censura sistemática, restricciones de movilidad y la eliminación progresiva del espacio público como un entorno libre de monitoreo estatal.

El dilema no se limita a regímenes autoritarios. Las democracias liberales enfrentan su propia contradicción. En nombre de la lucha contra el terrorismo y la ciberseguridad, la supervisión masiva ha sido adoptada sin resistencia por agencias como la NSA, el FBI o la CIA. Programas como PRISM han revelado el alcance de esta intrusión en la privacidad ciudadana. La Unión Europea ha respondido con marcos regulatorios como el *AI Act*, estableciendo mecanismos de mitigación de riesgos y transparencia algorítmica. La diferencia fundamental con la RPC radica en la existencia de controles institucionales. Sin embargo, ¿hasta qué punto estos límites son efectivos? ¿Cuánto tiempo antes de que la seguridad se imponga sobre las libertades civiles en sociedades que hoy se perciben como democráticas?

La estabilidad ha sido utilizada como justificación para sacrificar el derecho a la privacidad. En China Continental, la expansión de la vigilancia digital ha anulado cualquier noción de anonimato. Sistemas como *Skynet* y el SCS no se limitan a supervisar. Configuran un modelo de ingeniería social donde la conducta individual se regula a través de algoritmos que determinan quién accede a servicios, quién es confiable y quién se convierte en un marginado digital. La IA ha potenciado la capacidad del Estado chino y el poder de Xi Jinping para modelar comportamientos. Ha introducido un sistema de incentivos y sanciones que refuerza la obediencia, desincentiva la participación política y estructura la vida cotidiana en función de la calificación estatal. Lo que comenzó como una herramienta de supervisión se ha convertido en un mecanismo de domesticación ciudadana.

En el escenario global, la gobernanza de la IA se ha convertido en una prioridad geopolítica. La RPC y la UE representan polos opuestos en este debate. Mientras una prioriza el control total sobre la información y los flujos de datos, la otra opta por regulaciones orientadas a la transparencia y la rendición de cuentas. Este choque de modelos definirá el futuro de la gobernanza digital. En paralelo, la BRI ha servido como canal para exportar infraestructuras de vigilancia a países con baja capacidad regulatoria, facilitando la adopción de herramientas de supervisión en contextos donde la democracia es frágil o inexistente.

El problema ya no es la vigilancia digital en sí misma. Es la ausencia de límites efectivos. La falta de estándares internacionales ha permitido que estos sistemas se expandan sin restricciones, sin mecanismos de supervisión independientes y sin garantías de derechos. La comunidad internacional enfrenta un desafío inminente. Sin regulaciones globales que establezcan líneas rojas, la tecnología se consolidará como una herramienta de represión antes que un medio para el desarrollo humano.

A medida que la influencia china crece, la posibilidad de replicar su modelo en otras latitudes se vuelve más tangible. Sin resistencia, sin restricciones, sin oposición real. La pregunta ya no es si el mundo puede permitirse modelos de vigilancia como el chino. La pregunta es si, en la ausencia de límites claros, estos modelos se volverán la norma en lugar de la excepción.

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.