DOI: 10.59794/rscd.2025.v11i11.151
Sección internacional

La inteligencia artificial como arma de dominación global: ¿Quién controla la seguridad humana en el siglo XXI?
Artificial intelligence as a weapon of global domination: Who controls human security in the 21st century?

Fabricio Cabrera Ortiz[1] ORCID: 0000-0002-7065-7943

[1]Universidad Nacional de Colombia, Colombia, facaor@gmail.com

Autor para correspondencia: Fabricio Cabrera Ortiz, facaor@gmail.com

Resumen

Este ensayo examina cómo la inteligencia artificial (IA) se ha convertido en una herramienta de dominación global que afecta profundamente la seguridad humana. A través de un enfoque multidimensional –que abarca aspectos económicos, personales, comunitarios, ambientales, políticos, alimentarios y sanitarios– se analiza cómo la IA reproduce desigualdades históricas y refuerza nuevas formas de poder. El artículo identifica cuatro vectores de amenaza: el sesgo geopolítico, la supremacía tecnológica del Norte Global, el uso de IA en conflictos híbridos, y la privatización de la seguridad a través de algoritmos. Se expone cómo América Latina enfrenta una doble condición de vulnerabilidad: dependencia digital y debilidad institucional. Además, se advierte sobre la erosión de derechos fundamentales ante el uso de sistemas automatizados opacos. Finalmente, se plantea la necesidad de una soberanía tecnológica regional basada en marcos éticos, capacidades propias y regulación democrática.

Palabras clave: Inteligencia artificial, seguridad humana, control algorítmico, soberanía digital, conflictos híbridos

Abstract

This essay examines how artificial intelligence (AI) has become a tool of global

domination that profoundly affects human security. Through a multidimensional approach, one which encompasses economic, personal, community, political, food and health aspects, it analyses how AI reproduces historical inequalities and reinforces new forms of power. The article identifies four threat vectors: geopolitical bias, the technological supremacy of the Global North, the use of AI in hybrid conflicts, and the privatization of security through algorithms. It highlights how Latin America faces a double condition of vulnerability: digital dependence and institutional weakness. In addition, it warns about the erosion of fundamental rights in the use of opaque automated systems. Finally, it argues for the urgent need to build regional technological sovereignty grounded in ethical frameworks, local capacities, and democratic regulation.

Keywords: Artificial intelligence, human security, algorithmic control, digital sovereignty, hybrid conflicts

Recibido: 29/ 05/ 2025
Revisado: 23/ 07/ 2025
Aprobado: 17/ 09 / 2025

1. Introducción

Durante las últimas décadas, la inteligencia artificial (IA) ha sido presentada por gobiernos, empresas tecnológicas y organismos multilaterales como el catalizador de una nueva era de desarrollo humano. La promesa de automatizar procesos, optimizar decisiones y resolver problemas complejos ha sido abrazada con entusiasmo en sectores tan diversos como la salud, la educación, el transporte, la justicia y la seguridad. Bajo esta narrativa tecnoptimista, la IA aparece como una herramienta universalmente beneficiosa, una suerte de “inteligencia aumentada” puesta al servicio del progreso social.

Sin embargo, este discurso oculta dimensiones mucho más problemáticas. Numerosas investigaciones (Zuboff, 2019; Eubanks, 2018) han advertido que la expansión

acelerada de sistemas algorítmicos se está realizando sin controles democráticos, sin transparencia en su funcionamiento y sin marcos éticos adecuados. Lejos de democratizar el conocimiento, la IA está reforzando estructuras de poder preexistentes, exacerbando desigualdades, socavando derechos fundamentales y propiciando nuevas formas de control social.

La centralización de datos, la opacidad de los algoritmos y la concentración del poder tecnológico en manos de un puñado de corporaciones y Estados han abierto la puerta a una distopía algorítmica: un modelo de gobernanza no deliberativa, en el que las decisiones sobre seguridad, movilidad, salud o ciudadanía no son tomadas por personas, sino por modelos matemáticos entrenados con sesgos históricos y diseñados con lógicas económicas utilitarias. Como señala Harari (2018), el control sobre los flujos de datos se ha convertido en la nueva fuente de poder global, desplazando a la soberanía territorial tradicional.

Esta evolución tecnológica plantea interrogantes de gran calado para la seguridad humana. ¿Quién controla los algoritmos que deciden qué es una amenaza? ¿Qué impacto tiene el uso de IA en contextos militarizados, autoritarios o desiguales? ¿Puede una tecnología no regulada comprometer los principios básicos de la dignidad humana, la libertad y la autodeterminación colectiva?

Este artículo se propone analizar la IA no como una herramienta neutral, sino como una tecnología política. Aborda su potencial de convertirse en un instrumento de dominación global que socava la seguridad humana en sus múltiples dimensiones: desde la económica hasta la política, desde la comunitaria hasta la personal. Lo hace desde un enfoque multidimensional e interdisciplinario, combinando estudios críticos de tecnología, geopolítica de los datos, derecho internacional de los derechos humanos y teoría de la seguridad. La tesis central es disruptiva: si la IA no se democratiza, regulariza y socializa, podría consolidar un nuevo régimen de poder silencioso, tecnocrático y global, que trascienda incluso las capacidades de vigilancia de los Estados autoritarios del siglo XX.

2. Desarrollo

Marco conceptual: seguridad humana e inteligencia

artificial

El concepto de seguridad humana surge en la década de los noventa como respuesta a los límites del paradigma tradicional de seguridad centrado en el Estado y la amenaza militar externa. Propuesto formalmente en el Informe sobre Desarrollo Humano del Programa de las Naciones Unidas para el Desarrollo (PNUD, 1994), este enfoque desplaza el centro de gravedad hacia el individuo y reconoce que la inseguridad puede derivarse tanto de la violencia directa como de carencias estructurales, exclusión social o situación de vulnerabilidad tecnológica. La seguridad humana comprende siete dimensiones interdependientes: económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política.

Desde esta perspectiva, la seguridad ya no se limita a la ausencia de guerra, sino que implica la posibilidad de vivir sin miedo ni miseria, con acceso a los bienes fundamentales y con plena garantía de derechos. Esta reconceptualización exige, por tanto, un enfoque holístico e interdisciplinario para abordar las amenazas contemporáneas que afectan la vida cotidiana de las personas.

En este marco, la inteligencia artificial representa una amenaza emergente que no encaja fácilmente en las categorías convencionales de análisis. Su carácter difuso, su capacidad de operar de manera transnacional y su implementación muchas veces silenciosa la convierten en un desafío inédito. La IA puede afectar simultáneamente múltiples dimensiones de la seguridad humana: puede propiciar desempleo estructural (seguridad económica), facilitar la desinformación masiva (seguridad política), amplificar patrones de discriminación algorítmica (seguridad personal y comunitaria) y erosionar la soberanía informativa (seguridad política).

De igual modo, la naturaleza predictiva y automatizada de muchos sistemas de IA desafía los principios de agencia humana y deliberación democrática. Las decisiones que antes requerían responsabilidad pública –como conceder un crédito, vigilar a un sospechoso, asignar un recurso o autorizar un tratamiento médico– ahora pueden ser delegadas a sistemas entrenados con datos históricos, plagados de sesgos estructurales (Noble, 2018; Eubanks, 2018) .

Por otro lado, desde una perspectiva geopolítica, la concentración de capacidades en unos pocos actores globales configura una nueva forma de poder estructural, en el

cual la soberanía tecnológica se vuelve esencial para preservar la autonomía política y el bienestar social. Así como el control del petróleo definió la geopolítica del siglo XX, el control de los datos y la capacidad de procesamiento algorítmico definen la del siglo XXI (Morozov, 2012).

Este artículo parte entonces de un marco conceptual que articula tres nociones clave: (1) Seguridad humana, como paradigma que centra la atención en los derechos, libertades y necesidades vitales de las personas. (2) IA como tecnología política, cuyo desarrollo, diseño y aplicación están atravesados por relaciones de poder. (3) Soberanía digital, entendida como la capacidad de los Estados y pueblos para ejercer control legítimo sobre sus infraestructuras tecnológicas, sus datos y las decisiones automatizadas que afectan a su población.

Desde esta perspectiva, el análisis que sigue identifica cómo la IA, en su uso actual, compromete estos tres pilares y configura nuevas formas de inseguridad estructural. No se trata simplemente de una disfunción tecnológica, sino de una arquitectura de dominación en construcción, donde los algoritmos reemplazan a las armas como instrumentos de control, exclusión o sumisión.

3. Inteligencia artificial y sesgo geopolítico: una herramienta de poder global

La inteligencia artificial, a menudo presentada como un avance universal y objetivo, es en realidad una tecnología profundamente geopolítica. Su desarrollo, implementación y gobernanza no solo están determinados por capacidades técnicas, sino por relaciones asimétricas de poder, intereses estratégicos y modelos ideológicos de sociedad. Desde sus inicios, la IA ha sido monopolizada por un grupo reducido de actores globales –principalmente empresas estadounidenses y chinas–, cuyas agendas comerciales y geoestratégicas terminan imponiendo estándares tecnológicos y normas de facto sobre el resto del mundo (Kwet, 2019).

Esta concentración de poder tecnológico produce lo que se podría llamar un sesgo geopolítico estructural. A diferencia del sesgo algorítmico clásico –aquél que refleja prejuicios en los datos o en la programación–, el sesgo geopolítico se refiere al control

de las infraestructuras, los marcos normativos y las arquitecturas de decisión globales. En otras palabras, no solo los algoritmos pueden discriminar, sino también las condiciones globales de su producción y circulación.

Hoy, más del 90 % de la infraestructura de cómputo en la nube, las plataformas de aprendizaje automático y los centros de datos están en manos de empresas del Norte Global (Google, Amazon, Microsoft, Baidu, Tencent, Alibaba). Esto implica que los datos de miles de millones de personas del Sur Global son procesados, almacenados y monetizados fuera de sus países, sin garantías de soberanía informativa, sin acceso al conocimiento derivado de esos datos, y sin mecanismos de reparación en caso de abusos.

Así mismo, muchas de las arquitecturas algorítmicas están diseñadas con lógicas que responden a contextos culturales, jurídicos o económicos propios del Norte, pero son exportadas e impuestas como soluciones universales. Por ejemplo, los sistemas de reconocimiento facial desarrollados en China –basados en vigilancia masiva y control estatal– han sido implementados en países de África, Asia Central y América Latina con escaso escrutinio y sin garantías democráticas. Del mismo modo, empresas de Silicon Valley como Palantir Technologies proveen sistemas de inteligencia predictiva a agencias de seguridad en Latinoamérica, importando algoritmos entrenados en contextos de racismo estructural y vigilancia masiva (Feldstein, 2025).

Este sesgo geopolítico se manifiesta también en el desarrollo de normas internacionales. Las principales iniciativas sobre gobernanza de la IA –como el AI Act en Europa, las pautas de la OCDE o los marcos de la UNESCO– están diseñadas en espacios donde los países del Sur Global tienen escasa voz o capacidad de incidencia. A menudo se asume que los principios éticos son “neutrales”, cuando en realidad reflejan prioridades de actores dominantes.

La IA, en ese sentido, está configurando un nuevo orden internacional basado en la asimetría cognitiva y decisional. Quienes controlan los datos y los algoritmos vigilan también las formas de ver, clasificar, predecir e intervenir el mundo. Esto tiene consecuencias profundas para la autodeterminación de los pueblos, para la justicia global y para la seguridad humana. América Latina, en particular, corre el riesgo de ser reducida a una región extractiva de datos –como lo fue de recursos naturales– y a un laboratorio de experimentación algorítmica. Sin capacidad local de auditoría, sin soberanía normativa, sin independencia tecnológica, los países de la región enfrentan una situación de colonización digital silenciosa.

Por lo anterior, es necesario reconceptualizar la IA como un instrumento geopolítico de poder blando, pero también de control duro, que opera mediante infraestructuras invisibles y decisiones automatizadas. El sesgo geopolítico no es un accidente, sino una característica estructural de un sistema tecnológico global que reproduce la desigualdad bajo una nueva forma: el dominio algorítmico.

4. Supremacía tecnológica y dependencia digital del Sur Global

La noción de supremacía tecnológica se refiere al dominio sostenido que ejercen ciertos actores –ya sean Estados, conglomerados empresariales o alianzas transnacionales– sobre los recursos estratégicos, las infraestructuras, los sistemas de innovación y las capacidades normativas en el ámbito de la tecnología. En el caso de la inteligencia artificial (IA), este dominio se manifiesta en términos de liderazgo técnico o comercial, y también en la capacidad de establecer estándares, definir problemas, priorizar agendas de investigación y condicionar la adopción global de soluciones automatizadas (Mazzucato, 2019).

Esta supremacía tiene un correlato directo, la dependencia digital estructural del Sur Global. A diferencia de las brechas tecnológicas convencionales, que pueden ser abordadas con políticas de conectividad o alfabetización digital, la dependencia digital implica una subordinación funcional a sistemas, plataformas y arquitecturas que escapan al control local. En palabras de Couldry y Mejías (2019), asistimos a una nueva forma de colonialismo, donde los datos –el recurso estratégico del siglo XXI– son extraídos de forma masiva sin control soberano, utilizados por plataformas globales para fines comerciales, de seguridad o control social, muchas veces en detrimento del interés público local.

América Latina representa un caso paradigmático de esa dependencia. La región importa casi la totalidad de sus sistemas operativos, servidores, plataformas digitales, software (programa anti-plagio) de IA y servicios de computación en la nube. Las grandes corporaciones tecnológicas que operan en el continente no están sujetas a regulaciones estrictas ni pagan impuestos proporcionales a su volumen de

negocio. La región no cuenta con capacidades autónomas de desarrollo de hardware (equipo informático o componentes físicos) ni con centros de supercómputo de escala global, lo que la condena a ser consumidora de tecnologías "listas para usar" desarrolladas bajo lógicas ajenas a sus contextos sociales y culturales.

Esta situación propicia múltiples riesgos:

1. Soberanía informativa limitada: los gobiernos y las instituciones públicas no tienen control efectivo sobre los datos que se producen dentro de sus territorios, lo que compromete la planificación, la toma de decisiones y la seguridad nacional.
2. Vulnerabilidad estratégica: la dependencia de infraestructuras críticas alojadas en el extranjero deja expuestos a los Estados frente a bloqueos, espionaje, manipulación de sistemas o restricciones geopolíticas.
3. Imposición de arquitecturas opacas: los sistemas automatizados adoptados sin auditoría local, por ejemplo, para salud pública, educación, justicia penal o subsidios sociales, pueden contener sesgos, errores o lógicas que refuercen la exclusión en lugar de resolverla (Eubanks, 2018).
4. Desigualdad cognitiva: la falta de capacidades locales para interpretar, adaptar o construir modelos de IA propios genera una brecha epistémica profunda, en la que los países del Sur quedan relegados al consumo pasivo de tecnologías que no comprenden ni controlan.

Frente a este panorama, algunos autores advierten que estamos transitando hacia una geopolítica de la inteligencia artificial análoga a la de los recursos energéticos del siglo XX. Así como el control del petróleo permitió a ciertos Estados condicionar el desarrollo de otros, hoy el control de los datos, los algoritmos y las plataformas configura nuevas relaciones de dependencia y dominación (Morozov, 2012).

En ese sentido, la lucha por la soberanía tecnológica no es un lujo ni una aspiración idealista: es una necesidad urgente para garantizar la autonomía estratégica, la seguridad humana y la justicia social en el siglo XXI. La región necesita invertir en capacidades locales de desarrollo de IA, promover redes regionales de cooperación científica y establecer políticas públicas que prioricen el interés general sobre los intereses de mercado. Sin estas acciones, el Sur Global seguirá atrapado en una arquitectura tecnológica diseñada por otros, para otros, y muchas veces en su contra.

5. IA en conflictos híbridos: armas silenciosas en guerras no declaradas

En la era digital, las guerras no siempre se libran con balas. La noción de conflicto híbrido ha emergido como una categoría clave para comprender las formas contemporáneas de confrontación entre Estados, actores no estatales y coaliciones transnacionales. Estos conflictos combinan medios militares tradicionales con operaciones cibernéticas, campañas de desinformación, sabotaje digital, presión económica y manipulación algorítmica de la opinión pública. En este nuevo campo de batalla, la inteligencia artificial se ha convertido en un arma silenciosa, ubicua y cada vez más autónoma.

Uno de los elementos más preocupantes sobre el uso de IA en conflictos híbridos es su capacidad para realizar acciones ofensivas sin supervisión humana directa. En 2021, un informe del Panel de Expertos del Consejo de Seguridad de la ONU (Organización de Naciones Unidas) reveló que un dron autónomo de combate habría atacado a un objetivo humano en Libia sin intervención humana, marcando un hito inquietante en la automatización letal (United Nations, 2021). Aunque el caso aún produce debate, lo cierto es que el desarrollo de sistemas de armas autónomas letales (LAWS, por sus siglas en inglés) plantea desafíos jurídicos y éticos de gran magnitud.

Por otra parte, la IA ha sido integrada de forma creciente en operaciones de ciberinteligencia y guerra informacional. Algoritmos de aprendizaje automático son utilizados para diseñar campañas de desinformación hipersegmentadas, manipular narrativas públicas mediante bots (robots de cuentas automatizadas) y trolls (robots de usuarios reales), generar deepfakes (falsificaciones profundas o ultrafalsos) indistinguibles de la realidad y detectar patrones de conducta en opositores políticos o líderes sociales. Estas tácticas al igual que se emplean entre potencias globales, también han sido adaptadas por grupos armados, empresas de seguridad privada e incluso gobiernos autoritarios en contextos locales.

El caso de Cambridge Analytica (Carole y Graham-Harrison, 2018), donde millones de perfiles de Facebook fueron utilizados para influir electoralmente mediante IA, es apenas la punta del iceberg. En América Latina, existen reportes crecientes sobre el uso de algoritmos para vigilancia masiva de opositores, monitoreo predictivo de

protestas sociales, y diseminación de noticias falsas durante procesos electorales. Lo preocupante es que muchas veces estas herramientas se adquieren bajo contratos confidenciales, sin supervisión parlamentaria ni debate ciudadano.

Desde la perspectiva de la seguridad humana, la implicación de la IA en conflictos híbridos introduce amenazas profundas a la libertad de expresión, al derecho a la protesta, al acceso a la información veraz y a la privacidad. Además, su uso puede derivar en acciones encubiertas que socaven la soberanía de los Estados, afecten la estabilidad política o exacerben conflictos sociales preexistentes.

En este nuevo escenario bélico, los adversarios ya no necesitan invadir territorios ni derramar sangre para obtener ventajas estratégicas. Pueden desestabilizar democracias, paralizar servicios públicos, deslegitimar liderazgos o sembrar el caos informativo desde la distancia, con bajo costo y alta eficacia. La IA convierte la información en una munición de precisión y convierte la invisibilidad en ventaja táctica.

Frente a este panorama, la región de América Latina y el Caribe se encuentra en una situación crítica. La falta de capacidades técnicas para detectar, mitigar o responder a estas amenazas, sumada a la escasa integración regional en materia de ciberdefensa, deja a los países expuestos a una nueva generación de guerras invisibles. Es urgente incorporar la dimensión algorítmica y cognitiva en las doctrinas de defensa nacional y diseñar políticas públicas que regulen el uso de IA en contextos de seguridad interna, defensa y orden público. La IA en conflictos híbridos no es una amenaza futura: ya está aquí. Y su espacio de operaciones no son solo los campos de batalla, sino las redes, las emociones, las narrativas y los sistemas automatizados que organizan nuestra vida cotidiana.

6. Privatización de la seguridad: algoritmos que deciden quién es una amenaza

La seguridad, tradicionalmente concebida como una función esencial del Estado, ha experimentado en las últimas décadas un proceso de externalización y privatización progresiva. Este fenómeno ha sido impulsado por el auge de las empresas de seguridad privada, el outsourcing de funciones militares y de inteligencia, y más

recientemente, por la incorporación de tecnologías emergentes gestionadas por corporaciones tecnológicas globales. En este contexto, la inteligencia artificial no solo ha transformado la manera cómo se concibe la seguridad, sino también quién la controla y cómo se ejerce.

Uno de los elementos más disruptivos es la proliferación de sistemas de vigilancia predictiva, también conocidos como "predictive policing". Estos sistemas se basan en algoritmos entrenados con grandes volúmenes de datos históricos –muchas veces cargados de sesgos raciales, geográficos o socioeconómicos– para anticipar comportamientos considerados riesgosos. Como han demostrado diversos estudios (Brantingham, Valasik y Mohler, 2018), esta lógica tiende a replicar patrones de discriminación estructural, ubicando a ciertas comunidades bajo sospecha permanente y reproduciendo lo que se ha denominado "racismo algorítmico".

A esta problemática se suma el hecho de que muchos de estos sistemas son desarrollados, operados o licenciados por empresas privadas, cuyas prioridades responden a intereses comerciales, no necesariamente a principios democráticos, derechos humanos o transparencia institucional. Empresas como Palantir Technologies, ShotSpotter o Clearview AI han vendido sus productos a agencias policiales, migratorias y militares en América Latina, sin que exista una normativa clara que regule su uso, audite sus impactos o garantice rendición de cuentas (AI Now Institute, 2021).

La privatización de la seguridad a través de la IA también implica un deslizamiento funcional: algoritmos que antes servían para recomendaciones comerciales o segmentación de clientes son ahora utilizados para establecer perfiles de riesgo, gestionar fronteras, determinar prioridades de patrullaje o decidir si una persona merece vigilancia adicional. Esta lógica de "seguridad como servicio" no solo transforma las capacidades estatales, sino que plantea dilemas éticos sobre la delegación de decisiones que afectan derechos fundamentales a entidades opacas, automatizadas y sin responsabilidad legal.

El riesgo más profundo es que se consolide una arquitectura de vigilancia algorítmica en la que los Estados actúan como simples consumidores de tecnología, mientras que las grandes plataformas definen unilateralmente cuáles conductas son sospechosas, cuáles territorios deben ser vigilados y cuáles poblaciones son peligrosas. Este modelo erosiona el principio republicano de que la seguridad debe estar sometida al imperio de la ley, al control democrático y al respeto por los derechos humanos.

En América Latina, esta tendencia es particularmente peligrosa debido a tres factores: (1) la debilidad institucional para regular el uso de tecnologías emergentes, (2) la alta desigualdad social que amplifica los impactos discriminatorios de los algoritmos, y (3) la fragmentación del sistema judicial que impide establecer mecanismos eficaces de reparación ante violaciones.

Por su parte, la privatización algorítmica de la seguridad puede facilitar nuevas formas de autoritarismo tecnológico. Gobiernos que enfrentan descontento social o crisis de legitimidad pueden utilizar estas herramientas para vigilar opositores, anticipar protestas o reprimir movimientos sociales bajo el pretexto de mantener el orden. La frontera entre seguridad y represión preventivas se diluye peligrosamente cuando las decisiones son tomadas por modelos matemáticos entrenados con datos sesgados.

Frente a este escenario, se requiere una doctrina pública de seguridad digital y algorítmica que recupere el control estatal, garantice los principios de legalidad y proporcionalidad, y prohíba la adopción de tecnologías que no sean auditables, explicables y respetuosas de los derechos humanos. La seguridad no puede estar gobernada por cajas negras. Ni por mercados. Debe estar regida por la ética, la ley y la deliberación democrática.

7. Implicaciones para América Latina y el Caribe

América Latina y el Caribe se encuentran en un punto de inflexión frente al avance acelerado de la inteligencia artificial y su penetración en los distintos ámbitos de la vida pública y privada. A diferencia de otras regiones que han logrado posicionarse como productoras de tecnología, la región latinoamericana continúa siendo, en gran medida, una importadora neta de sistemas, plataformas y soluciones algorítmicas diseñadas en contextos culturales, políticos y económicos distintos. Esta situación conlleva riesgos no solo tecnológicos, sino también políticos, jurídicos, sociales y estratégicos.

El principal problema no es la adopción de la tecnología en sí, sino la ausencia de un marco soberano, ético y estratégico para guiar su incorporación. Como advierten

Couldry y Mejías (2019), el Sur Global enfrenta una nueva forma de colonialismo: el colonialismo de datos, mediante el cual las infraestructuras digitales y los sistemas de inteligencia artificial se imponen sin control soberano, extrayendo valor informacional para intereses externos. América Latina se enfrenta así a una doble condición de vulnerabilidad estructural: por un lado, la carencia de capacidades locales de diseño, auditoría y desarrollo de IA; por otro, la exposición creciente a sistemas de control automatizado que pueden ser utilizados para fines autoritarios, extractivos o discriminatorios.

Entre las principales implicaciones que se derivan para la región se destacan las siguientes:

a. Riesgo de colonización digital

La región puede convertirse en un nuevo laboratorio de experimentación para tecnologías de vigilancia, control social y gestión algorítmica importadas del Norte Global. Esto ya se ha observado en la instalación de sistemas de reconocimiento facial en espacios públicos sin debate ciudadano ni estudios de impacto en derechos fundamentales, como ha ocurrido en ciudades de Argentina, Brasil y México. La imposición silenciosa de estas tecnologías puede replicar lógicas coloniales bajo una nueva fachada: la dependencia algorítmica.

b. Erosión de la soberanía informativa

El almacenamiento y procesamiento de datos personales, financieros, biométricos y conductuales de millones de ciudadanos en infraestructuras alojadas fuera de la región impide el ejercicio efectivo de soberanía. Esto compromete la capacidad de los Estados para proteger a sus poblaciones, tomar decisiones basadas en evidencia local y garantizar el cumplimiento de normas nacionales de privacidad y seguridad.

c. Fragmentación institucional y desarticulación regional

La falta de políticas públicas integrales sobre IA, sumada a la escasa cooperación entre países latinoamericanos, dificulta el desarrollo de respuestas comunes. Mientras potencias como China, Estados Unidos y Unión Europea definen estrategias nacionales y bloques normativos sobre IA, en América Latina predominan las iniciativas aisladas, los vacíos legales y la dependencia de estándares externos.

d. Amplificación de las desigualdades internas

La IA no actúa en el vacío: se alimenta de los datos disponibles y reproduce los sesgos existentes en la sociedad. En regiones marcadas por profundas desigualdades socioeconómicas, raciales y de género, el uso acrítico de sistemas algorítmicos puede

reforzar exclusiones históricas y consolidar nuevas formas de discriminación automática. Esto es especialmente grave en el ámbito de los servicios públicos, la justicia penal, la asistencia social y la seguridad ciudadana.

e. Condición de vulnerabilidad frente a amenazas híbridas

Como se argumentó anteriormente, la IA es ya un componente central de los conflictos híbridos y de las estrategias de guerra informacional. América Latina, con sistemas de ciberdefensa incipientes y escasa capacidad de detección, se encuentra particularmente expuesta a operaciones de desinformación, manipulación electoral, sabotaje digital y espionaje algorítmico. La ausencia de protocolos conjuntos de respuesta amplifica esta amenaza.

Frente a este escenario, es urgente que América Latina y el Caribe desarrollen una agenda regional de soberanía digital e inteligencia artificial, articulada sobre tres ejes estratégicos:

a. Normativo: elaboración de marcos jurídicos comunes que regulen el uso de la IA en función del interés público, los derechos humanos y la transparencia algorítmica. Esto incluye establecer principios de explicabilidad, auditoría externa, proporcionalidad y no discriminación.

b. Institucional: fortalecimiento de capacidades estatales para supervisar, auditar y eventualmente producir tecnologías propias, mediante agencias nacionales y redes de cooperación regional.

c. Epistémico: promoción de una visión latinoamericana de la IA que reconozca las especificidades culturales, sociales y económicas de la región, y que impulse un pensamiento tecnológico descolonizador, autónomo y orientado al bienestar colectivo.

Solo así será posible enfrentar el nuevo orden algorítmico global con dignidad, justicia y autodeterminación. La región no puede resignarse a ser un consumidor pasivo de tecnologías ajenas. Debe convertirse en actor, en creador y en garante de una IA ética, soberana y profundamente humana.

8. Conclusiones

¿Seguridad humana o algoritmos de control?

La inteligencia artificial se ha convertido en un elemento constitutivo del poder global contemporáneo. Ya no es simplemente una herramienta técnica, sino una arquitectura invisible que organiza flujos de información toma decisiones automatizadas y moldea conductas individuales y colectivas. Esta transformación no es neutra: está cargada de relaciones de poder, conflictos de interés, lógicas de mercado y estrategias de dominación. En este contexto, la pregunta que da título a esta conclusión se vuelve urgente: ¿Nos dirigimos hacia un horizonte de seguridad humana potenciada por la tecnología, o hacia un modelo de control algorítmico que erosiona nuestras libertades fundamentales?

A lo largo de este artículo se ha argumentado que, en su configuración actual, la IA no solo no garantiza la seguridad humana, sino que amenaza sus fundamentos. La concentración del poder tecnológico en manos de un puñado de actores, la opacidad de los sistemas de decisión automatizados, la externalización de funciones soberanas a empresas privadas y el uso creciente de IA en conflictos híbridos y en contextos de vigilancia social, configuran un escenario de inseguridad estructural global.

Desde una perspectiva crítica, la IA no puede ser tratada como una herramienta meramente técnica, ni como un destino inevitable. Es, ante todo, un campo de disputa: una construcción política y social que puede ser orientada hacia fines emancipadores o hacia formas cada vez más sofisticadas de control, exclusión y subordinación. La alternativa entre seguridad humana o algoritmos de control no es una disyuntiva tecnológica, sino profundamente ética y geopolítica.

América Latina y el Caribe, como parte del Sur Global, enfrentan el desafío histórico de no repetir la lógica de dependencia que caracterizó su relación con los recursos naturales, el capital financiero o las tecnologías industriales del siglo XX. La región tiene la oportunidad –y la obligación– de construir una soberanía digital basada en principios democráticos, derechos humanos, justicia social y cooperación regional. Esto implica no solo regular y limitar los riesgos de la IA, sino también imaginar y producir formas alternativas de inteligencia tecnológica centradas en el cuidado de la vida, el bien común y la dignidad humana.

Para ello, se requieren políticas públicas integrales, instituciones fuertes, marcos jurídicos sólidos, capacidad científica local, pensamiento crítico y voluntad política. La IA no es en sí misma ni buena ni mala: su significado dependerá del proyecto civilizatorio al que se adscriba. Lo que está en juego no es solo la eficiencia de los servicios públicos o la competitividad económica, sino el tipo de sociedad que

queremos construir.

En última instancia, el poder de los algoritmos debe estar subordinado al de los pueblos. La seguridad humana, entendida desde su enfoque multidimensional –económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política– no puede ser delegada a sistemas automatizados ni reducida a parámetros de eficiencia técnica. Estos algoritmos, si no son diseñados, regulados y supervisados bajo principios éticos y democráticos, corren el riesgo de erosionar las bases mismas de la dignidad humana. Por ello, es indispensable recuperar el sentido político, ético y humanista de la tecnología. Solo así será posible orientar la inteligencia artificial hacia un modelo civilizatorio que garantice libertad, justicia social y autodeterminación de los pueblos en el siglo XXI.

Referencias

AI Now Institute. (2021, 4 de diciembre). *Enfrentando las cajas negras: un informe paralelo del Grupo de Trabajo del Sistema de Decisiones Automatizadas de la Ciudad de Nueva York.* AI Now Institute. https://ainowinstitute.org/publications/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated

Brantingham, P. J., Valasik, M., y Mohler, G. O. (2018). ¿Conduce la vigilancia predictiva a arrestos sesgados? Resultados de un ensayo controlado aleatorio. *Statistics and Public Policy,* 1-6. https://www.tandfonline.com/doi/pdf/10.1080/2330443X.2018.1438940

Carole, C., y Graham-Harrison, E. (2018, 17 de mayo). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Couldry, N., y Mejias, U. A. (2019). Data colonialism: Rethinking Big Data's relation to the contemporary subject. *Television & New Media,* 20(4), 336–349. https://journals.sagepub.com/toc/tvna/20/4

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor.* St. Martin's Press.

Feldstein, S. (2025, 8 de mayo). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/files_WP-Feldstein-AISurveillance_final1.pdf

Harari, Y. N. (2018). *Homo Deus.* Debate.

Kwet, M. (2019). Colonialismo digital: el imperio estadounidense y el nuev o imperialismo en el sur global. *Race & Class*, 60(4), 3-26.

Mazzucato, M. (2019). *El valor de las cosas: quién produce y quién gana en la economía.* Taurus.

Morozov, E. (2012). *The net delusion*. PublicAffairs.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Programa de las Naciones Unidas para el Desarrollo (PNUD). (1994). *Informe sobre desarrollo humano 1994.* Fondo de Cultura Económica de México.

United Nations. (2021, 8 de marzo). *Security Council: Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council.* https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_229.pdf

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