



Edición Nº 9 – Julio de 2026

Capítulo de Derecho Constitucional y Derechos Humanos

www.aidca.org/revista

La inteligencia artificial como catalizador de la vigilancia masiva: desafíos jurídicos para la privacidad, la libertad y el Estado de Derecho

Por Bianca Ancillai y Lucas Insaurrealde

La inteligencia artificial (IA) ha dejado de ser una tecnología limitada a ámbitos experimentales para convertirse en una herramienta transversal utilizada por gobiernos, empresas y organizaciones en la toma de decisiones, la automatización de procesos y el análisis de grandes volúmenes de información. Su desarrollo ha impulsado avances significativos en sectores como la salud, la educación, la administración pública y la seguridad. No obstante, las mismas capacidades que han favorecido estos progresos también han generado nuevos interrogantes sobre su impacto en el ejercicio y la protección de los derechos fundamentales.

Uno de los ámbitos en los que estas tensiones resultan más evidentes es el de la vigilancia. La incorporación de sistemas de IA ha ampliado las posibilidades de recopilación, análisis y utilización de datos personales, planteando desafíos inéditos para el derecho a la privacidad, la protección de datos personales, la libertad de expresión, la libertad de reunión y el principio de igualdad. Como consecuencia, el debate jurídico contemporáneo ya no se limita a determinar la legitimidad de determinadas medidas de vigilancia, sino también a establecer cuáles son los límites que deben regir cuando estas son potenciadas mediante tecnologías capaces de automatizar decisiones, identificar personas y procesar información a gran escala.

El aumento en la utilización de estas herramientas ha dado lugar a respuestas regulatorias heterogéneas. Mientras algunos Estados han incorporado tecnologías de vigilancia basadas en IA con fines de seguridad pública o control social, otros, como la Unión Europea, han comenzado a desarrollar marcos normativos destinados a limitar determinados usos por los riesgos que pueden representar para los derechos fundamentales. Paralelamente, organismos internacionales como las Naciones Unidas, la UNESCO y el Consejo de Europa han insistido en la necesidad de que el desarrollo y la utilización de la IA se ajusten a un enfoque basado en los derechos humanos.

En este contexto, el presente trabajo tiene por objeto analizar de qué manera la IA ha transformado la vigilancia masiva y cuáles son los principales desafíos jurídicos derivados de su utilización.

La vigilancia masiva en la era digital.

La digitalización de las comunicaciones y de la vida cotidiana transformó profundamente la forma en que se ejerce la vigilancia. Mientras que durante gran parte del siglo

XX las actividades de monitoreo estuvieron limitadas por la disponibilidad de recursos humanos y materiales, la expansión de Internet, los dispositivos móviles y las plataformas digitales permitió la generación constante de información sobre prácticamente todas las actividades de las personas. Hoy, acciones tan habituales como utilizar una aplicación de navegación, realizar una compra electrónica o interactuar en redes sociales dejan un rastro digital susceptible de ser almacenado y analizado.

En este marco surge el concepto de **vigilancia masiva**, que Amnistía Internacional define como *"el control de las comunicaciones por Internet y telefónicas de un gran número de personas —a veces de países enteros— sin que existan indicios suficientes de conducta delictiva¹".* A diferencia de la vigilancia dirigida, basada en una sospecha individualizada y generalmente sujeta a control judicial, la vigilancia masiva supone la recopilación indiscriminada de información con el objetivo de identificar posteriormente posibles riesgos, patrones o comportamientos de interés.

La consolidación de la economía digital ha ampliado significativamente las fuentes de obtención de datos personales. Teléfonos inteligentes, aplicaciones móviles, plataformas digitales, dispositivos conectados (*Internet of Things*) y servicios basados en la nube generan información relativa a la ubicación, hábitos de consumo, interacciones y actividades de sus usuarios. Paralelamente, empresas tecnológicas y corredores de datos (*data brokers*) recopilan, procesan y, en determinados casos, comercializan esta información, que puede ser posteriormente utilizada por organismos públicos o privados para distintos fines. Como consecuencia, es posible reconstruir perfiles detallados sobre la vida cotidiana de las personas a partir de la integración de múltiples fuentes de información.

¹ AMNISTÍA INTERNACIONAL. Guía sencilla sobre vigilancia masiva. Marzo, 2015. <https://www.amnesty.org/es/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/>

Desde una perspectiva protectora de los derechos humanos, este escenario plantea importantes desafíos para la protección de los mismos. La recopilación indiscriminada de datos personales puede afectar el derecho a la privacidad y producir un **efecto inhibitorio** (*chilling effect*) sobre libertades como la expresión, la reunión o la asociación. En efecto, cuando las personas perciben que sus comunicaciones, desplazamientos o actividades pueden ser objeto de monitoreo permanente, es posible que modifiquen su comportamiento o restrinjan el ejercicio de sus derechos por temor a ser observadas o identificadas.

Sobre esta infraestructura de recopilación masiva de datos se desarrollan actualmente los sistemas de IA, cuya capacidad para procesar, relacionar y analizar grandes volúmenes de información ha ampliado considerablemente el alcance de la vigilancia contemporánea.

La inteligencia artificial como amplificador de la vigilancia masiva.

La IA ha transformado la vigilancia masiva al dotarla de capacidades de análisis y procesamiento que exceden ampliamente las posibilidades humanas. A diferencia de las tecnologías tradicionales, que requerían una intervención constante para examinar la información recopilada, los sistemas de IA permiten automatizar estas tareas, identificar patrones, relacionar datos provenientes de distintas fuentes y generar inferencias sobre el comportamiento de las personas en tiempo real.

Entre sus aplicaciones más relevantes se encuentran el reconocimiento facial, la identificación biométrica, el reconocimiento de voz y los sistemas de análisis predictivo. Estas herramientas pueden contribuir legítimamente a fines como la prevención del delito o la búsqueda de personas desaparecidas; sin embargo, su utilización también incrementa los riesgos para los derechos fundamentales cuando se implementan sin controles adecuados o de forma indiscriminada.

Asimismo, la utilización de IA en actividades de vigilancia plantea desafíos adicionales para la protección de los derechos fundamentales. La **Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos** ha señalado que determinadas aplicaciones de IA, especialmente aquellas destinadas al

reconocimiento biométrico y al tratamiento masivo de datos personales, pueden generar inferencias arbitrarias o ilegítimas en la privacidad, así como

afectar el ejercicio de libertades fundamentales cuando su utilización no se encuentra sujeta a controles efectivos y a los principios de legalidad, necesidad y proporcionalidad

Como consecuencia de esto, organismos internacionales han insistido en la necesidad de establecer límites al empleo de estas tecnologías. La **UNESCO**, en su *Recomendación sobre la Ética de la Inteligencia Artificial*,² sostiene que los sistemas de IA deben desarrollarse y utilizarse respetando los derechos humanos y evitando aplicaciones que favorezcan formas de vigilancia incompatibles con la dignidad humana. En la misma línea, el **Reglamento de Inteligencia Artificial de la Unión Europea (AI Act)** restringe determinados usos de la identificación biométrica remota en espacios públicos, al reconocer los riesgos que estas tecnologías pueden representar para la privacidad y otras libertades fundamentales.

Por consiguiente, la IA no solo incrementa la eficiencia de la vigilancia, sino que modifica su alcance y complejidad, planteando nuevos desafíos para el Derecho en materia de privacidad, protección de datos y control del ejercicio del poder público.

[Impacto sobre los derechos humanos.](#)

La utilización de la IA en la vigilancia plantea importantes desafíos para la protección de los derechos humanos, en particular cuando estas tecnologías permiten la recopilación y el tratamiento masivo de datos personales sin las garantías adecuadas. Si bien los Estados pueden adoptar medidas de vigilancia para perseguir fines legítimos, como la seguridad pública o la prevención del delito, dichas injerencias deben ajustarse a los principios de legalidad, necesidad y proporcionalidad, conforme a los estándares del Derecho Internacional de los Derechos Humanos.

El derecho a la vida privada constituye uno de los principales bienes jurídicos comprometidos. El **artículo 11 de la Convención Americana sobre Derechos Humanos** establece que toda persona tiene derecho al respeto de su honra y de su dignidad, prohibiendo las injerencias arbitrarias o abusivas en su vida privada, su familia, su domicilio o su correspondencia. En el mismo sentido, el **artículo 17 del Pacto Internacional de Derechos Civiles y Políticos** dispone que nadie será objeto de injerencias arbitrarias o ilegales en su vida

² **UNESCO**. Recomendación sobre la Ética de la Inteligencia Artificial. 2021.

https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa .

privada, imponiendo a los Estados la obligación de brindar protección jurídica frente a tales prácticas. Estos estándares adquieren una relevancia particular frente a sistemas capaces de recopilar, cruzar y analizar información personal de manera permanente.

En nuestro ordenamiento jurídico interno, la protección de la privacidad encuentra sustento en el **artículo 19 de la Constitución Nacional**, que consagra el principio de reserva de las acciones privadas, así como en el **artículo 43**, que incorpora la acción de *habeas data* para garantizar el acceso, rectificación y supresión de datos personales. A ello se suma la jerarquía constitucional que otorga nuestra Carta Magna a los tratados internacionales de derechos humanos por el **artículo 75, inciso 22**, que fortalece aún más la tutela frente a posibles injerencias derivadas del uso de tecnologías de vigilancia.

La utilización de sistemas de IA en actividades de vigilancia puede comprometer el ejercicio de diversos derechos humanos más allá del derecho a la privacidad. La recopilación, el tratamiento y el análisis automatizado de datos personales pueden incidir sobre la libertad de expresión, la libertad de reunión y la libertad de asociación cuando las personas son sometidas a mecanismos de monitoreo incompatibles con los principios de legalidad, necesidad y proporcionalidad. Asimismo, el empleo de sistemas automatizados para la identificación, clasificación o elaboración de perfiles (*profiling*) plantea desafíos respecto del principio de igualdad y no discriminación. La utilización de modelos algorítmicos para adoptar o respaldar decisiones puede generar impactos desproporcionados sobre determinados grupos si no existen mecanismos que garanticen la transparencia, la supervisión humana y la posibilidad de revisar o impugnar las decisiones automatizadas.

Casos a nivel internacional.

La incorporación de IA a los sistemas de vigilancia ha dado lugar a respuestas regulatorias heterogéneas, reflejando distintas concepciones sobre el equilibrio entre seguridad, innovación tecnológica y protección de los derechos fundamentales.

Uno de los ejemplos más representativos es el de **China**, donde las autoridades han desarrollado un sistema de vigilancia basado en la **Integrated Joint Operations Platform (IJOP)**, una plataforma que centraliza información obtenida de múltiples fuentes como datos biométricos, registros administrativos, geolocalización, cámaras de videovigilancia y aplicaciones móviles para elaborar perfiles individuales e

identificar personas consideradas potencialmente riesgosas. La aplicación utilizada por la policía de Xinjiang recopila información sobre conductas cotidianas plenamente lícitas como utilizar determinadas aplicaciones de mensajería, evitar relacionarse con vecinos o adquirir ciertos productos y las incorpora a un modelo de evaluación que puede derivar en investigaciones, interrogatorios o detenciones arbitrarias. Este sistema constituye uno de los ejemplos más avanzados de utilización de IA y análisis masivo de datos con fines de vigilancia y control social, especialmente sobre la población uigur y otras minorías musulmanas de la Región Autónoma de Xinjiang.

En **Estados Unidos**, el desarrollo de tecnologías de vigilancia ha estado impulsado principalmente por el sector privado, siendo **Clearview AI** uno de los casos más controversiales. La empresa desarrolló un sistema de reconocimiento facial alimentado por una base de datos construida mediante la recopilación masiva de miles de millones de imágenes obtenidas de Internet y redes sociales sin el consentimiento de sus titulares, con el objetivo de facilitar tareas de identificación para organismos encargados de la aplicación de la ley. Este modelo de negocio ha sido objeto de investigaciones, litigios y sanciones en distintos Estados por los cuestionamientos que suscita respecto de la privacidad y la protección de los datos biométricos. La expansión de estas herramientas también se refleja en su creciente utilización por organismos públicos. A principios de 2026, la **Oficina de Aduanas y Protección Fronteriza de los Estados Unidos (CBP)** suscribió un contrato con Clearview AI para incorporar su tecnología de reconocimiento facial en tareas de *"focalización táctica"* y *análisis estratégico de redes*. El acuerdo prevé el acceso a una base de datos de millones de imágenes de acceso público con el propósito de fortalecer las capacidades de inteligencia y análisis de la agencia.

En contraste, la **Unión Europea** ha optado por un enfoque preventivo y basado en los derechos fundamentales. El **Reglamento N°2024/1689 (AI Act ³)** clasifica determinados sistemas de identificación biométrica remota como de alto riesgo y, en ciertos supuestos,

³ **CONSEJO DE LA UNIÓN EUROPEA Y PARLAMENTO EUROPEO.** Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, Artificial Intelligence Act, 12 de julio de 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

prohíbe su utilización en espacios de acceso público con fines policiales, salvo excepciones estrictamente previstas por la norma.

Estos casos mencionados evidencian que, si bien la IA ofrece herramientas cada vez más sofisticadas para la vigilancia, los distintos ordenamientos jurídicos han adoptado respuestas profundamente divergentes respecto de los límites que deben imponerse a su utilización. Esta ausencia de criterios uniformes a nivel internacional constituye uno de los principales desafíos para la construcción de estándares convencionales de protección de los derechos humanos en esta nueva era digital.

Conclusión.

La IA está transformando significativamente la vigilancia contemporánea al permitir el procesamiento automatizado de grandes volúmenes de información, la identificación biométrica y la elaboración de perfiles con un nivel de eficiencia que excede las capacidades humanas. Si bien estas tecnologías pueden contribuir legítimamente a objetivos como la seguridad pública o la investigación penal, su utilización también incrementa los riesgos de afectación a derechos fundamentales, especialmente cuando se implementan sin controles adecuados.

El principal desafío no reside en la existencia de mecanismos de vigilancia, sino en la necesidad de garantizar que su empleo se ajuste a los principios de **legalidad, necesidad, proporcionalidad y rendición de cuentas**, conforme a los estándares establecidos por el Derecho Internacional de los Derechos Humanos. La privacidad, la protección de los datos personales, la libertad de expresión, la libertad de reunión y el principio de igualdad constituyen derechos especialmente sensibles frente a la expansión de sistemas de vigilancia asistidos por IA.

Las experiencias comparadas demuestran que no existe actualmente un consenso internacional sobre los límites jurídicos de estas tecnologías. Mientras algunos Estados privilegian su utilización con fines de seguridad o control social, otros han comenzado a desarrollar marcos regulatorios específicos orientados a minimizar sus riesgos. En este contexto, instrumentos como el **AI Act** de la Unión Europea constituyen un antecedente relevante, aunque todavía insuficiente para responder a los desafíos derivados de una tecnología cuyo desarrollo supera con frecuencia la velocidad de la regulación.



A nuestro juicio, el desafío regulatorio no consiste en impedir el desarrollo de estas tecnologías, sino en garantizar que su utilización permanezca sometida a los mismos límites constitucionales que históricamente han regido toda injerencia estatal sobre la esfera privada de las personas. De lo contrario, la capacidad técnica de la inteligencia artificial corre el riesgo de desdibujar principios esenciales del Estado de Derecho.

Bibliografía

AMNISTÍA INTERNACIONAL. Guía sencilla sobre vigilancia masiva. Marzo, 2015. <https://www.amnesty.org/es/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/>

AMNISTÍA INTERNACIONAL. Global: Google's shameful decision to reverse its ban on AI for weapons and surveillance is a blow for human rights. 2025. <https://www.amnesty.org/es/latest/news/2025/02/global-googles-shameful-decision-to-reverse-its-ban-on-ai-for-weapons-and-surveillance-is-a-blow-for-human-rights>

CONSEJO DE LA UNIÓN EUROPEA Y PARLAMENTO EUROPEO. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, Artificial Intelligence Act, 12 de julio de 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

CONSTITUCIÓN DE LA NACIÓN ARGENTINA.

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS (Pacto de San José de Costa Rica). San José de Costa Rica, 1969.



HUMAN RIGHTS WATCH. China's Algorithms of Repression: Reverse

Engineering a Xinjiang

Police

Mass

Surveillance

App.

2019.

<https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>

DARAGH, Murray et al. “The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe”. Journal of Human Rights Practice, vol. 16, n.º 1, February 2024.

<https://academic.oup.com/jhrp/article/16/1/397/7234270>.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS

HUMANOS (OHCHR). El derecho a la privacidad en la era digital. Informe A/HRC/48/31, 13 de septiembre de 2021. <https://docs.un.org/es/A/HRC/48/31>.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). OECD

Digital Economy Outlook 2024. Volume 1: Embracing the Technology Frontier, 2024.