



Revista Científica General José María Córdova
Revista Colombiana de Estudios Militares y Estratégicos

Bogotá D.C., Colombia
ISSN 1900-6586 (impreso), 2500-7645 (en línea)
<https://doi.org/10.21830/19006586.1520>

ARTÍCULO DE INVESTIGACIÓN

Inteligencia artificial en seguridad: desafíos para la protección de los derechos humanos y la democracia

Artificial intelligence in security: challenges for the protection of human rights and democracy

Ethel Nataly Castellanos Morales

Universidad Nacional Abierta y a Distancia (UNAD), Bogotá D.C., Colombia
encastellanosm@unal.edu.co

Alejandro Abondano Romero

Universidad Externado de Colombia, Bogotá D.C., Colombia
alejandro.abondano@est.uexternado.edu.co

Citación APA: Castellanos Morales, E. N., & Abondano Romero, A. (2026). Inteligencia artificial en seguridad: desafíos para la protección de los derechos humanos y la democracia. *Revista Científica General José María Córdova*, 24(53), 83-104.
<https://doi.org/10.21830/19006586.1520>



Publicado en línea: 19 de enero de 2026



Enviar un artículo a la Revista

Responsabilidad de contenidos: La responsabilidad por el contenido de los artículos publicados por la Revista Científica General José María Córdova (Revista Colombiana de Estudios Militares y Estratégicos) corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Militar de Cadetes “General José María Córdova”, el Ejército Nacional, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.



Los artículos publicados por el Sello Editorial ESMIC y la Revista Científica General José María Córdova (Revista Colombiana de Estudios Militares y Estratégicos) son de acceso abierto bajo una licencia Creative Commons: **Atribución - No Comercial - Sin Derivados**.



Revista Científica General José María Córdova
Revista Colombiana de Estudios Militares y Estratégicos

Bogotá D.C., Colombia

Volumen 24 número 53, enero-marzo 2026, pp. 83-104

<https://doi.org/10.21830/19006586.1520>

ARTÍCULO DE INVESTIGACIÓN

Inteligencia artificial en seguridad: desafíos para la protección de los derechos humanos y la democracia

Artificial intelligence in security: challenges for the protection of human rights and democracy

Ethel Nataly Castellanos Morales 

Universidad Nacional Abierta y a Distancia (UNAD), Bogotá D.C., Colombia

Alejandro Abondano Romero 

Universidad Externado de Colombia, Bogotá D.C., Colombia

RESUMEN. Las crecientes aplicaciones de inteligencia artificial en el ámbito de la seguridad implican tensiones con los derechos humanos, especialmente en Estados en consolidación democrática y de la paz. Este artículo aborda dichas tensiones desde un marco jurídico y ético, no para limitar el desarrollo tecnológico, sino para legitimarlo mediante la promoción de sus beneficios y la prevención de daños potenciales, contribuyendo al desarrollo del constitucionalismo digital. Para ello, se desarrolla una revisión teórica sobre la consolidación democrática, un análisis normativo desde el Derecho Internacional de los Derechos Humanos y un examen conceptual de la inteligencia artificial y algunas de sus aplicaciones en seguridad. Se argumenta que las categorías clásicas de los derechos humanos siguen siendo útiles para enfrentar estos desafíos, en particular si se adopta el juicio de proporcionalidad como herramienta interpretativa central, con los ajustes necesarios ante la novedad tecnológica.

PALABRAS CLAVE: democracia; derechos humanos; imperio de la ley; inteligencia artificial; paz; seguridad del Estado

ABSTRACT. The increasing applications of artificial intelligence in the field of security raise tensions with human rights, especially in states undergoing democratic consolidation and peacebuilding. This article addresses these tensions from a legal and ethical framework, not to limit technological development, but to legitimize it by promoting its benefits and preventing potential harms, thus contributing to the development of digital constitutionalism. To this end, it presents a theoretical review of democratic consolidation, a normative analysis from the perspective of International Human Rights Law, and a conceptual examination of artificial intelligence and some of its security applications. It argues that classical human rights categories remain helpful in addressing these challenges, particularly when the proportionality test is adopted as a central interpretive tool, with necessary adjustments to account for technological innovation.

KEYWORDS: artificial intelligence; democracy; human rights; national security; peace; rule of law

Recibido: 29 de abril de 2025 • **Aceptado:** 22 de diciembre de 2025

CONTACTO: Ethel Nataly Castellanos Morales  encastellanosm@unal.edu.co

Introducción

La situación de derechos humanos en diversos países, que ha sido ampliamente estudiada, ahora vive desafíos tecnológicos que generan reflexiones permanentes sobre las nuevas condiciones para la garantía de estas prerrogativas. En el caso de los Estados que buscan la consolidación democrática y de la paz, pero que a la vez afrontan necesidades en materia de seguridad, surgen numerosos retos, uno de los cuales es el uso de la inteligencia artificial (IA) en distintas dimensiones de la seguridad estatal frente a los derechos humanos y su protección.

Este estudio se propone identificar si los desafíos que plantean las aplicaciones de IA en seguridad pueden abordarse desde la dogmática y la hermenéutica clásicas de los derechos humanos. El artículo sostiene que estas categorías siguen siendo útiles, pues el marco básico de análisis de estas medidas se fundamenta en el principio de legalidad y en los debates tradicionales sobre los márgenes de intangibilidad de los derechos. Frente a aspectos novedosos y posiblemente no regulados, será necesario precisar qué elementos de ciertos derechos son intangibles y cómo deben interpretarse. Sin embargo, el enfoque de derechos humanos resulta valioso para asegurar el aporte de estas tecnologías a la seguridad sin renunciar al respeto por las prerrogativas fundamentales, aspectos centrales en contextos de consolidación democrática y de paz.

Para tal fin, una vez presentada la metodología, se abordan nociones básicas sobre las categorías centrales de análisis: 1) la democracia en consolidación y su relación con los derechos humanos; 2) la IA y algunas de sus aplicaciones en seguridad frente a los derechos humanos; 3) los elementos centrales de un marco analítico con enfoque de derechos para la aplicación adecuada de la IA a la seguridad; y 4) una síntesis de categorías fundamentales para identificar y hacer seguimiento a los desafíos en el uso de la IA en tales contextos. Estos elementos contribuyen al desarrollo de una dogmática que promueva el uso de estas tecnologías mientras garantiza los derechos fundamentales, además de plantear eventuales líneas de investigación futuras.

Metodología

Se emplea una metodología cualitativa, con enfoque principalmente conceptual¹, desarrollada mediante revisión documental y análisis normativo fundamentado en el Derecho Internacional de los Derechos Humanos (DIDH). Se abordan categorías propias del derecho, la ciencia política, los derechos humanos y la teoría de la interpretación constitucional, así como la conceptualización que se ha hecho de la IA y su relación con la seguridad desde estas disciplinas. En un momento inicial, estos conceptos ilustran los supuestos de los que parte este trabajo y permiten identificar las relaciones entre las diferentes categorías teóricas explicadas.

1 Sobre la metodología de reconstrucción conceptual en la filosofía del derecho, véase García Yzaguirre (2023).

Por tratarse de un análisis con preponderancia jurídica, es importante recordar que el derecho puede ser visto, al menos, desde las siguientes aproximaciones: 1) el derecho como valor (que conduce a los problemas de legitimidad y justicia tratados por la filosofía del derecho y las teorías de la justicia), 2) el derecho como norma (enfocado en el problema de la validez tratado por la teoría del derecho en sentido estricto) y 3) el derecho como hecho (centrado en el problema de la eficacia tratado por la sociología del derecho).

Así, se propone un análisis conceptual del derecho desde dos enfoques: 1) como valor, a través de categorías —algunas provenientes de la ciencia política— que lo conciben como algo más que un ejercicio de poder, a saber: el Estado constitucional y democrático de derecho, la democracia y los derechos humanos; y 2) como norma, mediante la selección de ciertos derechos con base en normativa internacional y una mención tangencial a los avances normativos europeos sobre IA. En cambio, 3) la perspectiva del derecho como hecho no será abordada debido a la novedad de los debates y normas existentes, y a la falta de datos empíricos sobre situaciones aún no reguladas, que escapan a la medición y al alcance jurídico.

En consecuencia, se emplea una metodología eminentemente teórica, basada en nociones fundamentales sobre las categorías centrales de análisis: consolidación democrática y de la paz, derechos humanos, IA y sus aplicaciones en seguridad. Inicialmente, se aborda el concepto de consolidación democrática y de la paz, incluyendo algunos fundamentos empíricos tomados de fuentes secundarias para caracterizar estos regímenes y justificar la selección de ciertos derechos humanos relevantes para este texto. Para ello, se utilizan índices actualizados de medición democrática, considerando la reciente aceleración de los avances en IA, con amplia cobertura geográfica y un enfoque en variables vinculadas a garantías fundamentales. Los derechos seleccionados se definen según la dogmática del DIDH, conforme a lo dispuesto en sus tratados.

Adicionalmente, se ha construido un marco conceptual sobre la IA y sus aplicaciones en seguridad, basado en doctrina reciente (no mayor de ocho años) publicada en índices académicos reconocidos, y producida en regiones democráticas occidentales con mayor desarrollo tecnológico y normativo, priorizando Estados Unidos y Europa, y excluyendo a China. También se recurre a pronunciamientos de autoridades internacionales en derechos humanos, como el Relator Especial sobre la libertad de opinión y expresión de la ONU (2018)², y a los escasos cuerpos normativos existentes, como la Ley de Inteligencia Artificial del Parlamento Europeo (2024). Este marco aporta los conceptos, criterios y referentes teóricos, normativos y hermenéuticos necesarios para formular propuestas jurídicas prescriptivas sobre IA y seguridad, con enfoque de derechos y orientadas a la consolidación de la democracia y la paz.

2 Según el sitio web de la relatoría, en 1993 la Comisión de Derechos Humanos de la ONU estableció el mandato del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, tanto en línea como fuera de línea, conforme al DIDH. Tras sustituir a la Comisión, el Consejo de Derechos Humanos extendió el mandato en marzo de 2008 (res. 7/36) y lo renovó por tres años adicionales en 2011 (res. 16/4), 2014 (res. 25/2), 2017 (res. 34/18), 2020 (res. 43/4) y 2023 (res. 52/9).

El Estado en consolidación democrática y de la paz y su relación con los derechos humanos

Este apartado analiza la relación entre el Estado constitucional de derecho, los derechos humanos y el ejercicio de la ciudadanía, con el fin de identificar algunas características de los Estados en consolidación democrática y de la paz. Se considera que esta consolidación no es posible sin el respeto a los derechos humanos, incluidos aquellos que pueden verse afectados por el uso de la IA (Dieu & Montasari, 2022).

Si bien existe amplia bibliografía sobre la definición de democracia, se adopta la del Programa de las Naciones Unidas para el Desarrollo (PNUD, 2010): un método de organización del poder que, mediante el ejercicio de la ciudadanía, busca avanzar en la realización efectiva de los derechos. Se ejerce a través de las instituciones republicanas y está regulado por el Estado democrático de derecho. Su fundamento es la soberanía popular que, al delegar el poder, exige mecanismos de control ciudadano sobre su ejercicio, alternancia y duración. Aunque contextual y perfectible, la democracia requiere unos mínimos universales (elecciones libres, plurales y periódicas, y garantía de derechos humanos), cuya ausencia puede debilitar o sustituir el régimen democrático, una preocupación constante en democracias en consolidación que buscan la paz.

Para Tilly (2010), la consolidación democrática depende del nivel de respuesta del Estado a las demandas ciudadanas. Para analizar las variaciones entre regímenes, se enfoca en las relaciones entre el Estado y la ciudadanía en cuatro dimensiones clave: 1) amplitud de la inclusión política; 2) igualdad entre ciudadanos; 3) protección frente a la arbitrariedad estatal; y 4) consulta mutuamente vinculante, que se presenta cuando los funcionarios reparten beneficios basándose en criterios previamente establecidos y sin corrupción. En contextos de desdemocratización³, la respuesta estatal a las demandas ciudadanas disminuye; por ejemplo, los Estados que toleran violaciones de derechos humanos tienden a mostrar rasgos antidemocráticos.

Su propuesta sugiere que, aunque la seguridad es imperiosa, el respeto a los derechos humanos es indispensable para consolidar un Estado constitucional y democrático de derecho. Este modelo exige, como mínimo, que toda autoridad pública se someta a la ley, lo que refuerza la protección de los derechos ciudadanos al permitir su exigibilidad ante una autoridad (Donnelly, 2006). La ciudadanía, entendida como el derecho a tener derechos, es clave para el fortalecimiento democrático. Para Tilly (2010), la democracia puede aparecer en regímenes cuya capacidad estatal⁴ varía notablemente; por ello, los clasifica en cuatro grupos (Figura 1).

3 La desdemocratización implica procesos que reducen el carácter democrático de un régimen, como la suspensión de elecciones libres, y lo acercan a la autarquía u otras formas de organización política.

4 La capacidad del Estado de influir en la (re)distribución de los recursos, las actividades y las relaciones interpersonales, y sus subsecuentes dinámicas.



Figura 1. Tipos de regímenes políticos
Fuente: Tilly (2010, p. 52)

Esta caracterización muestra que los derechos humanos son fundamentales en todos los escenarios planteados, así como en las situaciones intermedias, dentro de las que se encuentran las democracias en consolidación. La seguridad también es central, pues las democracias requieren niveles de violencia política que tiendan a la baja. En el caso de las democracias con baja capacidad, es característica la existencia de actores semilegales o ilegales en la política pública, así como la presencia de violencia letal, con la consecuente afectación a la paz.

Algunas investigaciones cuantitativas también han explorado la relación entre la democracia y la mejora en derechos humanos. Como concluyen Bueno de Mesquita et al. (2005), 1) la participación política en un sistema multipartidista es clave para reducir abusos; 2) los avances en democratización no garantizan por sí mismos un mayor respeto a estas prerrogativas, salvo en democracias más consolidadas; y 3) la rendición de cuentas de los funcionarios es esencial para garantizar estos derechos.

Los rasgos de las democracias en consolidación también se pueden constatar en los índices de democracia. Para este estudio, se retoman los índices de Varieties of Democracy (V-Dem), Global State of Democracy (GSoD) y Freedom in the World, por ofrecer mediciones actualizadas (en el contexto de aceleración de los avances de la IA)⁵, amplia cobertura geográfica y un abordaje con un mayor número de variables⁶, lo que evita sobresimplificaciones en la medición (Pulido, 2024).

5 García del Blanco destaca el creciente debate global sobre la regulación de la IA al mencionar la nueva Ley de IA de la Unión Europea, iniciativas en países como Estados Unidos, China y Brasil, y algunos esfuerzos internacionales (Ilustre Colegio de Abogacía de Madrid, 2024, 54:30).

6 Freedom in the World mide un número moderado de variables, pero fue elegido sobre el Democracy Index por su antigüedad (década de 1970) y porque ofrece un balance relevante frente a los otros dos índices seleccionados, más recientes.

Los tres índices de democracia establecen diferentes rangos en los que se ubican los Estados, según el puntaje obtenido en las mediciones (Tabla 1).

Tabla 1. Sistemas de puntuación de los índices de democracia

Índice de democracia	Sistema de puntuación
V-DEM*	• Democracia - liberal: “Se cumplen los requisitos de la democracia electoral; limitaciones judiciales y legislativas al Ejecutivo junto con la protección de las libertades civiles y la igualdad ante la ley”. - electoral: “Las elecciones multipartidistas para el Ejecutivo son libres y justas; grados satisfactorios de sufragio, libertad de expresión, libertad de asociación”. • Autocracia - electoral: “Existen elecciones multipartidistas para el Ejecutivo; niveles insuficientes de requisitos fundamentales como la libertad de expresión y asociación y elecciones libres y justas”. - cerrada: “No habrá elecciones multipartidistas para el Ejecutivo; ausencia de componentes democráticos fundamentales como la libertad de expresión, la libertad de asociación y elecciones libres y justas”. (Nord et al., 2024, p. 12)
GSoD	Presenta resultados para cada una de las siguientes áreas, sin establecer una puntuación unificada: • Representación: acceso libre y equitativo a la representación política • Derechos: libertades y recursos individuales • Rule of law: aplicación predecible y equitativa de la ley, y pesos y contrapesos al poder gubernamental • Participación: participación política activa de la ciudadanía Los resultados para cada una de estas áreas van de 0 a 1. GSoD considera que un puntaje mayor a 0,7 puede entenderse como “alto”, mientras que uno menor a 0,4 sería “bajo” (International Institute for Democracy and Electoral Assistance [IDEA], 2023).
Freedom in the World	Se sustenta en la medición de dos categorías de indicadores para clasificar los Estados como libres, parcialmente libres o no libres: - Derechos políticos: procesos electorales, pluralismo político y participación, y funcionamiento del Gobierno. - Libertades civiles: libertad de expresión y creencia, derechos de asociación y organizacionales, rule of law, y autonomía personal y derechos individuales.

* Los reportes de V-DEM se centran en el índice de democracia liberal e instituciones “básicas” de la democracia electoral (Nord et al., 2024).

Fuente: Elaboración propia con base en Nord et al. (2024); IDEA (2023; 2024) y Freedom House (2024a; 2024b)

Este artículo entiende por democracias en consolidación aquellos países 1) clasificados como democracias electorales por V-Dem, 2) ubicados entre 0,4 y 0,7 en el índice GSoD y 3) considerados Estados parcialmente libres según Freedom in the World. Son Estados que, sin ser autocracias, enfrentan amenazas a su democracia.

Los tres índices consideran los derechos humanos, en especial las libertades civiles, como elemento central de medición. Para V-Dem, su respeto constituye un umbral mínimo; para GSoD y Freedom in the World, representan un pilar para definir el grado de democratización. Además de las libertades civiles, los tres valoran el papel de la participación ciudadana en el fortalecimiento democrático mediante distintos atributos incluidos en sus sistemas de puntuación (Tabla 2).

Tabla 2. Atributos medidos en relación con los derechos humanos y la participación

Atributo	Presencia en los índices	Conceptualización (categorización)
Libertades civiles y acceso a la justicia	V-DEMa	Libertades de: asociación expresión y fuentes alternativas de información movimiento Igualdad de clase y grupos sociales en el goce de libertades civiles Acceso a la justicia
	GSoD	Libertades de: asociación y reunión expresión (incluye privacidad en la red) prensa Partidos políticos libres Integridad personal y seguridad Sociedad civilb Participación en sociedades de la sociedad civil y sindicatos (civic engagement)
	Freedom in the World	Libertades de: expresión movimiento (según la pregunta G1 de la encuesta) organización de partidos políticos (según la pregunta B1) Derechos de: asociación y organización debido proceso
Participación ciudadana y pluralismo político	V-DEM	Sufragioc Elecciones transparentes Jefe del poder ejecutivo y legislatura elegidos popularmente (elected officials) Participación de la sociedad civil Voto popular directo
	GSoD	Participación electoral Elecciones creíbles Sufragio inclusivo Gobierno electo Igualdad política
	Freedom in the World	Proceso electoral Oportunidades reales de que oposición llegue al poder mediante elecciones populares (según la pregunta B2) Goce de derechos políticos para varios sectores poblacionales (según la pregunta B4)

^a Por operatividad, solo se tienen en cuenta las agregaciones de V-DEM para las definiciones de democracia: electoral, liberal, participativa, deliberativa e igualitaria.

^b Grado en que una vida social organizada, voluntaria, autogenerada y autónoma es institucionalmente posible (IDEA, 2023).

^c Mide el porcentaje aproximado de personas adultas emancipadas en edad de votar (Coppedge et al., 2024a; 2024b).

Fuente: Elaboración propia con base en IDEA (2023), Coppedge et al. (2024a; 2024b) y Freedom House (2024a)

Estos índices evalúan derechos humanos especialmente vulnerables frente al uso de la IA en seguridad, agrupados en dos categorías: libertades civiles y derechos políticos. Las primeras abarcan la libertad de expresión, de prensa, de asociación, de privacidad, de mo-

vimiento y de integridad personal, así como el acceso a la justicia y al debido proceso, elementos esenciales para garantizar su ejercicio efectivo ante posibles abusos. Los derechos políticos, por su parte, remiten a una concepción más formal y electoral de la democracia, vinculada con la participación en distintos niveles de gobierno y con la distribución del poder entre diversos grupos. Esta participación fortalece el control ciudadano sobre el uso de la IA como ejercicio de poder, en particular cuando están en juego derechos fundamentales.

En síntesis, los elementos mínimos de la democracia formal, como la separación de poderes y los controles al Ejecutivo, no bastan para evaluar escenarios de consolidación democrática. Resulta clave considerar si el Estado responde a las demandas ciudadanas y garantiza efectivamente los derechos humanos. La participación política y la celebración de elecciones libres, plurales y periódicas son también componentes esenciales. Como se verá a continuación, algunos de estos derechos, fundamentales para la democratización, adquieren especial relevancia frente al uso de la IA en el ámbito de la seguridad.

La IA y sus aplicaciones en seguridad frente a los derechos humanos

Dado el papel central de los derechos humanos en la consolidación democrática y la construcción de la paz, este apartado explora algunas aplicaciones de la IA en el ámbito de la seguridad estatal. Asimismo, analiza los desafíos que estas tecnologías plantean a derechos fundamentales estrechamente ligados al fortalecimiento democrático, como la intimidad, la protección de datos personales y las libertades de expresión, reunión, asociación y protesta pacífica, así como su impacto en la celebración de elecciones libres⁷.

La IA y otras tecnologías vinculadas para aplicaciones en seguridad

La definición de la IA es objeto de debate y permanente reformulación (Bakiner, 2023; Lualhé Shaelou & Razmetaeva, 2023). La Organización para la Cooperación y el Desarrollo Económico (OCDE, 2023) define un sistema de IA como aquel basado en máquinas que, con objetivos implícitos o explícitos y distintos grados de adaptabilidad, infiere determinados resultados (recomendaciones, predicciones, decisiones, entre otros) a partir de datos ingresados. Teo (2024) subraya que se trata de un conjunto de tecnologías que no requieren necesariamente control humano continuo para operar.

El Relator Especial (2018) reconoce la creciente velocidad e independencia de la IA, pero advierte que el término puede inducir a error al sugerir que las máquinas replican la inteligencia humana. Aunque se ha planteado la posibilidad de una IA general, actualmente solo existe una IA restringida, limitada a ejecutar algoritmos definidos por humanos. Bakiner

7 Otros derechos, como el derecho a un juicio justo o al debido proceso en general, a la presunción de inocencia, etc., no se abordan debido al objetivo preciso de este artículo.

(2024) explica que estos sistemas operan principalmente mediante modelos estadísticos. Si bien la intervención humana sigue siendo clave —al diseñar los sistemas, definir objetivos, seleccionar datos y establecer criterios de clasificación—, la automatización elimina su participación en partes del proceso decisorio. Como señala el Relator Especial (2018), corresponde a los humanos definir “el grado en que complementan o reemplazan la adopción de decisiones humanas” (p. 4).

Una de las principales tecnologías que ilustra estas dinámicas es el aprendizaje automático (*machine learning*), que permite a los algoritmos identificar y resolver problemas a partir de datos (Relator Especial, 2018). Su adaptabilidad les permite reconocer progresivamente nuevos patrones y generar soluciones imprevistas para sus programadores. No requieren ser completamente programados, pues pueden modificar su comportamiento según los datos que reciben del entorno (Zech, 2021).

Otro avance relevante en el ámbito de la seguridad es el uso de datos biométricos, que Teo (2024) describe como resultado de la datificación, es decir, la transformación de fenómenos —como el cuerpo— en datos. Los datos biométricos permiten identificar a una persona, por lo que son considerados datos personales, e incluyen, entre otros, microexpresiones, tono de voz, ritmo cardíaco, temperatura corporal y rasgos faciales (Raposo, 2023b; Lualhé Shaelou & Razmetaeva, 2023).

A partir de estos desarrollos, el reconocimiento facial se usa para el análisis estadístico de datos biométricos faciales (Raposo, 2023b). Esta tecnología permite detectar rostros en imágenes, categorizar personas, realizar vigilancia automatizada e incluso se ha empleado para intentar inferir emociones a partir de microexpresiones (Raposo, 2023a; 2023b; Stahl et al., 2023). Estos usos ilustran cómo la IA amplía las capacidades estatales en materia de seguridad.

Algunas aplicaciones de la IA, el aprendizaje automático y el reconocimiento de datos biométricos en seguridad

Estos y otros progresos de la IA han transformado las estrategias de seguridad, especialmente en las acciones policiales, de vigilancia y de aplicación de la ley (Raposo, 2023a). A partir de un informe regional del PNUD (2013), la seguridad ciudadana puede definirse como el conjunto de políticas y acciones del Estado y de otros actores orientadas a garantizar la convivencia pacífica y a reducir la violencia y el delito, aspectos que algunos autores catalogan como parte de los impactos a nivel funcional de la IA (Neves & De Almeida, 2024; Stahl et al., 2023). La conceptualización sobre la democracia permite establecer, además, la relevancia de la seguridad en los Estados en consolidación democrática como condición para fortalecer el ejercicio de derechos y responder a las demandas ciudadanas.

Uno de los usos más controvertidos de la IA en este campo es la vigilancia, que algunos autores defienden como una herramienta para mejorar la seguridad y reducir el crimen (Stahl et al., 2023). La IA ha transformado esta práctica al automatizar el análisis de datos

biométricos y facilitar el rastreo masivo de personas. Por ejemplo, existen cámaras que capturan esta información de forma autónoma e inadvertida (Teo, 2024; Saheb, 2023). Se ha planteado que integrar el reconocimiento facial en cámaras policiales podría fortalecer la legitimidad institucional y promover un ambiente de respeto mutuo al registrar las interacciones con la ciudadanía (Ringrose, 2019).

Antes solo era posible monitorear a uno o pocos individuos; ahora, el aprendizaje automático y el reconocimiento facial, combinados con el uso masivo de cámaras, han posibilitado formas de vigilancia comunitaria (Stahl et al., 2023). El reconocimiento facial plantea ventajas y retos particulares: el rostro es una parte especialmente visible del cuerpo, lo que facilita aún más la identificación de individuos. Por ello, su uso remoto conlleva riesgos de vigilancia masiva y de erosión de las libertades individuales. Lualhé Shaelou y Razmetaeva (2023) advierten que estos sistemas generan desbalances de poder al otorgar a las autoridades un acceso privilegiado a información personal. Además, la creciente datificación de la vida cotidiana y la integración de macrodatos (*big data*) permiten monitorear comportamientos, intenciones y preferencias individuales (Saheb, 2023).

Otra aplicación clave es la policía predictiva (*predictive policing*), que implica el análisis de datos y patrones delictivos para anticipar crímenes y optimizar la intervención policial (Stahl et al., 2023). Esta tecnología no solo predice zonas de mayor riesgo, sino que también identifica individuos con mayor probabilidad de cometer o de ser víctimas de delitos. A su vez, podría utilizarse para examinar datos sobre criminalidad y evidenciar sesgos en las estadísticas delictivas. No obstante, Stahl et al. (2023) advierten que la policía predictiva puede concentrar la atención policial en personas que habitan zonas desfavorecidas, con independencia de su vinculación efectiva con la comisión de un delito.

El reconocimiento facial en cámaras policiales puede utilizarse incluso para generar puntuaciones de riesgo automatizadas. Sin embargo, múltiples estudios advierten sobre los sesgos presentes en el entrenamiento de estas tecnologías, especialmente en la identificación de poblaciones minoritarias (Teo, 2024; Relator Especial, 2018). Estas limitaciones incrementan el riesgo de errores, con implicaciones particularmente sensibles dada la naturaleza de los derechos humanos en juego.

Posibles impactos en derechos humanos y democráticos

Aunque la IA y sus diversas aplicaciones en seguridad aportan beneficios indiscutibles, también conllevan riesgos claros para los derechos humanos y los valores democráticos a lo largo de todo su ciclo de vida: planificación, diseño, desarrollo y despliegue (Garriga, 2024). De ahí la importancia de adoptar los derechos humanos como marco jurídico, ético y político para su análisis. Si bien el debate se relaciona con la dignidad humana —derecho transversal ligado a la autonomía, la identidad y la autodeterminación—, el análisis se centra en los derechos a la intimidad y a la protección de datos personales, y en su relación

con las libertades de expresión, reunión, asociación y protesta pacífica⁸, por su impacto en la confianza en el Estado y en la celebración de elecciones libres. Estos aspectos resultan fundamentales para la consolidación democrática y de la paz, especialmente en contextos con retos en materia de seguridad y orden público.

Aun así, es importante partir de elementos comunes aplicables a cualquier reflexión sobre la IA y los derechos humanos. Esta tecnología no es neutral, pues es creada por personas cuyos sesgos, incluso inconscientes, pueden manifestarse en distintos momentos del proceso: 1) en la generación o el muestreo de datos, 2) en la formulación del problema o la clasificación, 3) en el análisis de los datos o la selección de la muestra, o 4) en la validación y prueba de los resultados (Dieu, 2023; Benzie & Montasari, 2023).

En este contexto, el derecho a la intimidad adquiere especial relevancia. La Convención Americana sobre Derechos Humanos (CADH, art. 11) lo define como la protección de la honra y la dignidad, y prohíbe injerencias arbitrarias o abusivas en la vida privada. Lualhé Shaelou y Razmetaeva (2023) advierten que los algoritmos de perfilamiento y predicción—como los impulsados por *machine learning*—requieren grandes volúmenes de datos sensibles. Para Saheb (2023), el reconocimiento facial biométrico resulta especialmente preocupante, pues puede facilitar la vigilancia masiva para el control del crimen mediante el acceso automatizado a imágenes faciales sin consentimiento. Aunque es difícil medir los daños concretos de estas aplicaciones, Teo (2024) señala que su normalización progresiva amenaza el fundamento mismo del derecho a la privacidad: la posibilidad de que cada persona decida cómo y qué parte de sí muestra al mundo. Los ejemplos mencionados evidencian la relación directa entre la intimidad y la protección de los datos personales.

Los sistemas de IA utilizan datos que van desde los no personales hasta los de identificación personal, aunque la mayoría se sitúa en algún punto intermedio: datos inferidos a partir de información personal o anonimizados (a menudo de forma imperfecta) (Relator Especial, 2018). La IA desafía las formas convencionales de consentimiento, propósito definido, limitación, transparencia y responsabilidad en el uso de la información. Por ejemplo, el uso masivo de cámaras con captura biométrica anónima exige nuevos métodos para obtener el consentimiento en la recolección y el tratamiento de datos (Saheb, 2023). A su vez, estos sistemas aprovechan bases de datos existentes, pero también generan nuevas bases cuyo origen y exactitud no siempre son claros, lo que dificulta la rectificación o eliminación de la información por parte de sus titulares.

A estos desafíos se suman riesgos técnicos como fallos del sistema, márgenes de error y problemas de transparencia. Entre ellos destacan la recolección encubierta de datos, su uso sin control o para fines no previstos, como decisiones automatizadas, predicción de

8 Se adoptan las definiciones de la Convención Americana sobre Derechos Humanos (CADH), similares a las de otros instrumentos regionales en el mundo y que abarcan los contenidos sustantivos de cada uno de los derechos seleccionados.

comportamientos o cruces con información no consentida (Stahl et al., 2023). Aunque la IA identifica correlaciones, estas no implican causalidad, lo que puede generar resultados erróneos y discriminatorios difíciles de detectar (Relator Especial, 2018). El temor constante ante posibles identificaciones incorrectas a partir de los datos recolectados restringe el ejercicio de la autonomía y la autodeterminación como pilares de la democracia y la paz.

Los estudios sobre IA evidencian una relación entre este derecho y la integridad física y psicológica (Dieu, 2023), protegidas como parte del derecho a la integridad personal (CADH, art. 5). La integridad física se vería amenazada por la posibilidad de que el Estado visualice constantemente características corporales, mientras que la integridad psicológica estaría en riesgo por la sensación de vigilancia continua y la angustia que esta produce. De hecho, varios autores coinciden en que contar con cierta protección frente al escrutinio externo es fundamental para la salud mental (Stahl et al., 2023). Como afirma Dieu (2023), estas intensas afectaciones a la esfera privada inciden en la capacidad para desarrollar libremente la personalidad, pensar y formar opiniones.

La CADH vincula la libertad de expresión (art. 13), de reunión (art. 15), de asociación (art. 16) y de protesta pacífica con la posibilidad de expresar libremente el pensamiento. Por lo tanto, prohíbe la censura previa y la restricción de la libertad de expresión por medios indirectos, aunque también proscribe la propaganda bélica y los discursos de odio. Si bien la IA puede ser de gran utilidad para materializar estos mandatos, también puede usarse para quebrantarlos; por ejemplo, herramientas como el *machine learning* pueden emplearse para identificar activistas que intentan evadir la censura (Correia & Rodrigues, 2024).

La delgada línea entre el uso legítimo y el abuso plantea retos adicionales. Algunos autores analizan cómo el reconocimiento facial en el transporte público puede terminar utilizándose con fines policiales (Saheb, 2023), o cómo el análisis de datos genéticos, concebido inicialmente para fines médicos, puede servir posteriormente para identificar sospechosos (Stahl et al., 2023). Esta distinción es clave, pues las implicaciones en términos de derechos cambian cuando los datos se reutilizan con propósitos distintos a los originalmente previstos. Como advierten Stahl et al. (2023), una vez digitalizados, los datos son difíciles de contener, lo que facilita su uso indebido.

Por razones comprensibles, la CADH no previó el *chilling effect*, o autocensura, derivado de la vigilancia constante (Teo, 2024; Dieu, 2023; Stahl et al., 2023). El reconocimiento facial combinado con tecnologías biométricas remotas facilita la vigilancia masiva y refuerza este efecto inhibitorio, que debilita la democracia y obstaculiza la consolidación de la paz. Incluso en democracias consolidadas, su uso se percibe como un riesgo grave. Lo mismo ocurre con los derechos de reunión, asociación y protesta pacífica, profundamente afectados por la normalización de la vigilancia. Frente a este panorama, cabe preguntarse cómo aprovechar los beneficios de la IA, fortalecer la democracia como camino hacia la paz y, al mismo tiempo, proteger los derechos humanos.

Algunos elementos para un marco analítico de aplicaciones de la IA en seguridad

Como se ha visto, los debates sobre derechos humanos e IA impactan incluso a democracias consolidadas, lo que los hace aún más relevantes en Estados en proceso de fortalecimiento democrático y de construcción de paz, donde garantizar derechos, participación y rendición de cuentas es más urgente y desafiante. Algunos autores proponen regular la IA desde un enfoque de derechos humanos e incluso identificar nuevas prerrogativas que respondan al contexto cambiante (De Asís Roig, 2024; Lualhé Shaelou & Razmetaeva, 2024), mientras que otros consideran insuficiente tal enfoque en este ámbito (Teo, 2024).

No obstante, una revisión básica de ciertas prerrogativas sugiere que no es necesario crear nuevos derechos, sino reinterpretar los existentes. Por ejemplo, se ha planteado la extensión de la protección del cuerpo físico (*habeas corpus*) al cuerpo digital (*habeas data*) (Pagallo, 2023). Los llamados “derechos nuevos” suelen ser desarrollos, a menudo necesarios, de garantías ya reconocidas. De Asís Roig (2024) propone la accesibilidad universal a la IA para personas con discapacidad, que puede entenderse como una expresión del derecho a la igualdad. Lualhé Shaelou y Razmetaeva (2024) plantean derechos como influir en la propia huella digital, no ser objeto de decisiones automatizadas ni de vigilancia masiva, todos ellos vinculados al debido proceso, la intimidad y la protección de datos personales.

Sin necesidad de crear nuevas categorías, los elementos clave para un marco analítico del uso de la IA en seguridad —especialmente en contextos de consolidación democrática— ya existen en el marco normativo e interpretativo de los derechos humanos. Principios como la legalidad y la proporcionalidad, así como derechos como la intimidad, la protección de datos personales, la igualdad, la no discriminación y la dignidad, son especialmente pertinentes. Este enfoque puede fortalecer la aún limitada respuesta ética inicial frente a los desafíos que plantea la IA (Bakiner, 2023; Relator Especial, 2018). Además, tanto los Estados como los actores privados comparten las mismas obligaciones en materia de derechos humanos, como sucede con otras tecnologías (Relator Especial, 2018).

Como señalan Benzie y Montasari (2023) y Neves y de Almeida (2024), diversos principios éticos con amplio consenso orientan la creación e interpretación de normas sobre IA: 1) el respeto a la intimidad, 2) la responsabilidad de los actores, 3) la seguridad de la información, 4) la transparencia, 5) la justicia e imparcialidad, 6) la no discriminación, 7) el control humano y 8) la promoción de valores humanos y del bienestar colectivo. Aun así, existen cláusulas jurídicas que permiten complementarlos, de lo cual es pionero el esfuerzo de la Unión Europea con la Ley de Inteligencia Artificial (Parlamento Europeo, 2024).

Los principios éticos mencionados encuentran respaldo jurídico en las interpretaciones de los derechos humanos, aunque con distintos matices de novedad. A su vez, este marco ofrece una posible respuesta a la pregunta sobre quién y con qué fundamento decide qué usos de la IA son legítimos.

El principio de proporcionalidad constituye una herramienta valiosa, pues distintos usos de la IA requieren ponderaciones diferenciadas de los valores en juego (Stahl et al., 2023). El Relator Especial resume los criterios del juicio de proporcionalidad aplicables para legitimar el uso de la IA en seguridad⁹. Cualquier restricción de derechos humanos en este contexto debe: 1) perseguir un fin legítimo (por ejemplo, garantizar el orden público), 2) ser necesaria y proporcional, en el sentido de implicar la menor restricción posible e imprescindible para alcanzar el objetivo, y 3) no afectar la esencia del derecho restringido. Además, debe cumplir estándares mínimos de legalidad, ser clara y precisa, y estar sujeta a control judicial independiente. Aun cuando exista un fin legítimo, debe considerarse que su uso en la aplicación de la ley (por ejemplo, reconocimiento biométrico, policía predictiva e investigaciones criminales, entre otros), la administración de justicia y los procesos democráticos ha sido calificado como altamente riesgoso (Comisión Europea, 2021).

El derecho a la intimidad y el tratamiento de datos personales también resultan determinantes en las aplicaciones de la IA a la seguridad en estas democracias, debido al riesgo del *chilling effect* asociado a la vigilancia masiva. Aunque la extensa literatura sobre estos derechos se ha ampliado con el avance de la IA, destacan algunos puntos relevantes: 1) el respeto a la intimidad es un requisito para legitimar los sistemas de IA, incluso aquellos aplicables a la seguridad estatal; 2) en este contexto, implica garantizar la privacidad, la calidad, la integridad y el acceso a los datos; y 3) exige el cumplimiento de principios básicos del tratamiento de datos personales, como la licitud (fundamento legal), la lealtad, la transparencia, la finalidad delimitada, la minimización de datos, la exactitud, la limitación del plazo de conservación, la seguridad y la responsabilidad (Stahl et al., 2023; Relator Especial, 2018).

La seguridad en el manejo de la información es crucial para preservar la privacidad y prevenir la discriminación en entornos tecnológicos (Stahl et al., 2023). La creciente datificación genera riesgos no solo por su uso en vigilancia, sino también por la vulnerabilidad a ciberataques (Saheb, 2023) o filtraciones de datos. Más allá del cifrado, se requieren niveles de seguridad que prevengan el procesamiento no autorizado, la pérdida accidental, el daño o la destrucción de los datos durante todo el ciclo de la IA, asegurando su calidad e integridad en cada etapa.

Algunos autores proponen marcos de gobernanza para la IA aplicada a la vigilancia estatal, con un enfoque colaborativo e interdisciplinario que refuerce la responsabilidad social y política de las compañías tecnológicas (Saheb, 2023). Para Teo (2024), estos marcos deben incorporar una perspectiva sociotécnica que considere el contexto y los valores promovidos por estas tecnologías, en coherencia con el principio de proporcionalidad. La gobernanza debe construirse mediante consultas amplias con la sociedad civil, personas expertas en IA, ética y derechos humanos, así como con representantes de poblaciones minoritarias (Teo, 2024; Relator Especial, 2018).

9 El informe plantea estos criterios de juicio en el contexto de las restricciones de la libertad de expresión, pero es aplicable a este contexto al permitir la ponderación.

Esta participación es clave para evaluar la necesidad de utilizar la IA, especialmente cuando su aplicación afecta a poblaciones vulnerables (Saheb, 2023). En democracias en consolidación, también es clave para identificar demandas ciudadanas, prevenir abusos, garantizar la igualdad, promover consultas mutuamente vinculantes y contribuir a la paz (Tilly, 2010). Se trata de un mínimo democrático que refuerza la protección de los derechos humanos y, con ello, la democracia misma.

Varios investigadores proponen, además, hacer evaluaciones de impacto en derechos humanos. Stahl et al. recomiendan análisis específicos sobre protección de datos desde las etapas tempranas del desarrollo de la IA, con el fin de identificar riesgos, definir bases legales—incluido el consentimiento informado—y delimitar los fines del tratamiento de datos, así como valorar la idoneidad de las medidas de protección. Asimismo, sugieren evaluaciones más amplias sobre los efectos de la IA, que incorporen impactos en la democracia e integren una visión centrada en los derechos.

Ahora bien, la complejidad y la opacidad de los sistemas de IA dificultan su comprensión y, por lo tanto, la participación democrática y la rendición de cuentas. También facilitan prácticas como la recolección encubierta de datos y su uso más allá de los fines previstos, por ejemplo, para la toma de decisiones automatizadas, la predicción de comportamientos o el cruce de información sin consentimiento. En este contexto, la transparencia y la responsabilidad resultan fundamentales para generar confianza pública y posibilitar el ejercicio de prerrogativas ciudadanas esenciales para la democracia.

La transparencia exige que la información sobre un acto sea accesible, de modo que terceros puedan supervisar su ejecución (Dieu & Montasari, 2022). Para fortalecerla, se recomienda la auditoría de los sistemas por equipos interdisciplinarios independientes que identifiquen errores, sesgos y vulnerabilidades, dejando constancia documentada del proceso (Dieu & Montasari, 2022; Relator Especial, 2018). Aunque el secreto industrial puede restringir el acceso a cierta información, no exime a los Estados ni a los actores privados que operan en el sector público de sus deberes de transparencia. Para conciliar estos intereses, se proponen mecanismos como la exigencia de confidencialidad a auditores externos o el uso de pruebas de conocimiento cero, que permiten verificar las propiedades de un algoritmo sin revelar su funcionamiento.

La IA también debe ser comprensible y contar con advertencias claras para garantizar los derechos, la participación y la rendición de cuentas (Dieu, 2023; Relator Especial, 2018). Las personas deben ser informadas cuando: 1) una decisión se adopta mediante el uso de IA, incluso si existe revisión humana; 2) sus datos contribuyen a decisiones automatizadas, explicando su lógica y posibles consecuencias; y 3) su información personal se integra en bases de datos utilizadas por sistemas de IA, precisando las condiciones de uso, almacenamiento y eliminación. Estas explicaciones no siempre requieren detallar aspectos técnicos; mensajes claros sobre el propósito, el impacto, las entradas y las salidas del sistema resultan valiosos para el debate público.

Stahl et al. (2023) señalan que, aunque las categorías protegidas como raza, sexo o edad han sido útiles para prohibir la discriminación en muchas jurisdicciones, su aplicación a los sistemas de IA requiere precauciones específicas. Estas categorías no son fijas y pueden surgir nuevas formas imprevistas de discriminación. Asimismo, entrenar modelos con datos provenientes de contextos estructuralmente desiguales perpetúa sesgos, pero excluir datos asociados a dichas categorías puede resultar ineficaz: la IA puede utilizar variables *proxy* y producir decisiones igualmente discriminatorias, aunque menos detectables. Además, esta exclusión puede reducir la calidad del entrenamiento, generar errores y comprometer gravemente otros derechos, especialmente en aplicaciones de seguridad.

Para mitigar estos riesgos, el Relator Especial (2018) recomienda identificar y corregir la discriminación en los datos de entrada y de salida, subsanar errores de muestreo y compensar sesgos estructurales. Stahl et al. (2023) proponen un diseño ético que incorpore valores compartidos y reconozca la discriminación estructural desde las etapas iniciales del desarrollo de la IA. Igualmente, destacan el potencial de la IA explicable para facilitar la comprensión de los procesos de clasificación y detectar sesgos. Estas medidas deben ir acompañadas de un monitoreo activo que permita prevenir y mitigar riesgos.

Las propuestas revisadas subrayan la importancia de mantener el *control humano* sobre la IA, especialmente en contextos donde los riesgos para los derechos humanos son elevados. Así lo reconoce el Relator Especial (2018), quien advierte que una confianza excesiva en la automatización puede debilitar la transparencia y la rendición de cuentas, ambas esenciales para proteger a la ciudadanía frente a arbitrariedades, asegurar consultas mutuamente vinculantes y garantizar los derechos mencionados (Tilly, 2010; Bueno de Mesquita et al., 2005).

Este control debe reforzarse en democracias en consolidación, donde los niveles de protección de estas prerrogativas suelen requerir un fortalecimiento adicional. Además, toda afectación a derechos debe ser susceptible de reparación. Para ello, la transparencia resulta imprescindible, pues las personas solo pueden exigir remedios si conocen cuándo son objeto de decisiones algorítmicas y comprenden su lógica (Relator Especial, 2018; Stahl et al., 2023). La responsabilidad enfrenta desafíos derivados de la velocidad del desarrollo tecnológico, el número de actores implicados y la opacidad de los sistemas. Aun así, nociones como la culpa o la negligencia siguen siendo útiles frente a daños causados por la IA, ya que detrás de estos suele existir alguna intervención humana (Parlamento Europeo, 2020).

La dignidad, como fundamento de los derechos humanos, exige que las personas sean consideradas fines en sí mismas; por lo tanto, la IA no puede constituir un fin, sino un medio orientado al bienestar. Esto implica excluir usos destructivos e incorporar el valor de la vida y del bienestar humano en su diseño. Para considerarse seguros, los sistemas deben cumplir estándares de: 1) precisión (resultados correctos), 2) fiabilidad (funcionamiento adecuado con distintos datos y en diversas situaciones, lo que facilita su escrutinio), 3) seguridad (resistencia a vulnerabilidades, explotación y ataques) y 4) robustez (enfoque preventivo del riesgo) (Stahl et al., 2023).

Estos elementos muestran la construcción de lo que se ha denominado constitucionalismo digital (Pagallo, 2023), un régimen en el que coexisten múltiples y diversos sistemas normativos que operan en un mismo campo, como el mercado, las normas sociales, los Estados, los organismos internacionales, las organizaciones no gubernamentales y el sector financiero, entre otros.

Conclusiones

Las oportunidades y los desafíos de la IA en materia de seguridad, y su relación con los derechos humanos en países en consolidación democrática que buscan la paz, son notables. Los avances tecnológicos en IA constituyen herramientas poderosas frente a delitos extendidos, como la suplantación de identidad, o especialmente atroces, como el secuestro, que pueden enfrentarse mediante aplicaciones de reconocimiento facial (Dieu & Montasari, 2022). Otro ejemplo es el uso del *machine learning* para detectar propaganda terrorista, la difusión de material de explotación sexual infantil o la guerra cibercriminal (Correia & Rodrigues, 2024). En este sentido, la IA ofrece oportunidades para fortalecer las capacidades estatales, reducir amenazas a la paz y alcanzar los niveles de seguridad que exigen las democracias.

Sin embargo, estas aplicaciones también generan tensiones con los derechos humanos, cuya garantía constituye un mínimo esencial para el fortalecimiento democrático. El uso de la IA en seguridad implica riesgos particularmente altos para derechos como la privacidad y la protección de datos personales, en estrecha relación con las libertades de expresión, reunión, asociación y protesta pacífica. Estas prerrogativas inciden directamente en la realización de elecciones libres —como mínimo democrático— y en la amplitud de la inclusión política, aspectos clave para la consolidación democrática (Tilly, 2010).

A pesar del desarrollo vertiginoso de estas tecnologías, la revisión conceptual presentada permite concluir que estos retos sustantivos y hermenéuticos pueden abordarse desde los debates clásicos sobre los derechos humanos y sus márgenes de intangibilidad. En ese sentido, no parece necesario hablar de “nuevos derechos”, pues los derechos innominados suelen constituir desarrollos ajustados de prerrogativas ya existentes en Estados democráticos. Sin embargo, las ventajas indiscutibles de la IA hacen necesario precisar los aspectos intangibles de ciertos derechos, sus relaciones con otros y sus mecanismos de interpretación.

Desde esta perspectiva, no es admisible considerar la seguridad y los derechos humanos como conceptos excluyentes. Por el contrario, el respeto por los derechos humanos constituye una herramienta clave frente a los riesgos asociados a estas tecnologías. La aplicación de un enfoque ético y de derechos humanos en el diseño y en las evaluaciones de impacto de la IA en materia de seguridad abre oportunidades para legitimar su uso. Como advierten Stahl et al. (2023), estas alternativas difícilmente podrían implementarse sin el reconocimiento de la intimidad y la protección de datos personales como derechos fundamentales.

El estudio de los conceptos de la teoría de la democracia y de sus mecanismos de medición, la normativa del DIDH y el marco teórico de la IA y de algunas de sus aplicaciones en seguridad permite, además, cumplir con el objetivo principal de este artículo: identificar elementos fundamentales para un marco de análisis de estas aplicaciones en seguridad desde un enfoque de derechos humanos. El principio de legalidad, el juicio de proporcionalidad y los derechos fundamentales mencionados constituyen elementos centrales en contextos de consolidación democrática, por su vínculo con la participación ciudadana y las elecciones.

Aun así, es evidente que se trata de un campo de estudio incipiente, pues la reflexión ética y desde los derechos humanos es reciente, a diferencia del desarrollo técnico, como señalan Benzie y Montasari (2023). Desde la perspectiva del derecho como valor, este artículo identifica desafíos éticos actuales; sin embargo, es necesario continuar abordando los retos éticos, tanto permanentes como cambiantes. Para ello, resulta clave mantener una mirada desde los derechos humanos, dada su capacidad para fortalecer la respuesta ética en este contexto (Bakiner, 2023).

Un análisis más comprensivo del derecho como norma podría incluir el estudio comparado de regulaciones internas en Estados en consolidación democrática. Este tipo de aproximación permitiría identificar rasgos comunes en sus ordenamientos, así como oportunidades y desafíos frente a las aplicaciones de la IA. Con el avance de la regulación, también será relevante estudiar de forma comparada normativas y jurisprudencia específicas sobre estas tecnologías, tanto en estos Estados como a nivel internacional.

En el corto plazo, podría incorporarse la revisión de la legislación europea y otros desarrollos normativos recientes. Estos no se incluyeron debido a su novedad y al propósito de centrar la reflexión en el marco general de los derechos humanos, de aplicación universal. La experiencia en la aplicación normativa permitirá, además, una aproximación desde el derecho como hecho, orientada a examinar los impactos y las reacciones de los distintos actores frente a la implementación de la regulación y la jurisprudencia desarrolladas en la materia.

Con todo, se destaca el juicio de proporcionalidad como un posible método hermenéutico para abordar las constantes tensiones de derechos que pueden surgir. Ello supone que siempre estará presente la pregunta sobre la mejor manera de aprovechar el innegable valor de las nuevas tecnologías para la seguridad y, al mismo tiempo, garantizar el respeto a las prerrogativas fundamentales. La gran variedad de escenarios y aplicaciones de la IA, incluso cuando se limita a fines de seguridad, exige análisis contextualizados. Esto implica considerar aquellos ámbitos en los que los riesgos asociados a su uso son más altos, como ciertos empleos en la aplicación de la ley y en la administración de justicia. En este marco, el principio de legalidad cumple un rol preponderante, pues exige, como mínimo, claridad, precisión y controles judiciales sobre las restricciones de derechos.

El principio de proporcionalidad también es clave para establecer lineamientos que permitan distinguir los usos legítimos de la IA de aquellos que no lo son. Al incorporar los

derechos humanos y el bienestar humano en la ponderación de los valores en juego, es posible que, en determinados escenarios, el uso de ciertos sistemas de IA deba ser descartado, limitado o sometido a controles específicos. Todas estas opciones contribuyen a un uso democrático de estas tecnologías e impulsan su perfeccionamiento; por ejemplo, la corrección de un algoritmo discriminatorio puede prevenir resultados erróneos que no solo afectan los derechos humanos, sino también la fiabilidad del sistema.

Existen tres grandes riesgos generales en los desarrollos de la IA en materia de seguridad: 1) los modelos de “caja negra” o de nula transparencia, es decir, aquellos que no permiten responder a las preguntas básicas de qué, por qué, quién y cuándo se aplican estas tecnologías; 2) las violaciones a la intimidad y a la protección de datos personales; y 3) los sesgos y la consecuente discriminación. Estos desafíos requieren especial atención en contextos de fortalecimiento democrático y de la paz, pues generan el riesgo de medidas de seguridad desconectadas de las demandas ciudadanas y ajenas al control público.

Por ello, estos retos pueden y deben ser abordados desde ciertas exigencias mínimas: 1) la transparencia en los algoritmos y la provisión de explicaciones comprensibles para las personas; 2) la generación de algoritmos para preservar la intimidad o *data cooperatives*; y 3) la equidad en los algoritmos, de modo que no se limiten, por ejemplo, a determinados factores demográficos (Benzie & Montasari, 2023, p. 18) que pueden acentuar sesgos discriminatorios y peligrosistas. En todo caso, el mantenimiento de estas exigencias y el monitoreo activo durante todo el ciclo de vida de la IA contribuyen a mejorar sus resultados y a mitigar riesgos.

La entidad de los derechos involucrados, así como la capacidad de daño eventual de la IA y de sus aplicaciones en seguridad, exigen un debate público sobre las regulaciones actuales y futuras. En efecto, la innovación no es axiológicamente neutra ni está exenta de escrutinio ético, y es imperativo reconocer que no constituye un fin en sí misma. Su propia naturaleza convierte a la participación en un medio para verificar en qué medida su desarrollo y utilización se ajustan a las demandas ciudadanas y a la promoción de la convivencia pacífica, en el caso de las aplicaciones en seguridad ciudadana.

Los postulados básicos para esta reflexión se resumen en la visión “humano-céntrica” de la IA. La estrategia frente a la posible tensión entre derechos humanos y aplicaciones de la IA en seguridad, en Estados en consolidación democrática y de la paz, es el establecimiento de un marco regulatorio jurídico y ético, no para limitar el desarrollo de la IA, sino para legitimarlo mediante la promoción de sus beneficios para los seres humanos y la prevención de potenciales daños. Para ello, es fundamental adoptar como marco los valores y principios de la humanidad, así como la protección de los derechos humanos. Además, las tensiones persistentes pueden resolverse mediante el juicio de proporcionalidad, con las adecuaciones sustantivas necesarias dada la novedad de algunas tecnologías. Todos estos elementos resultan relevantes en el concepto de constitucionalismo digital, que evidencia un esfuerzo fundacional en la regulación europea y plantea no solo un camino, sino también un desafío para América Latina.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. No se emplearon herramientas de generación de contenido por inteligencia artificial para su elaboración.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Ethel Nataly Castellanos Morales es doctora en derecho, Universidad Nacional Autónoma de México; magíster en derecho y abogada, Universidad Nacional de Colombia. Con amplia experiencia en la Corte Constitucional, cuenta con diversas publicaciones sobre fortalecimiento del Estado de derecho, derecho constitucional, teoría del derecho, derechos humanos, derecho comparado y justicia transicional.

<https://orcid.org/0000-0002-5374-6450>

Contacto: encastellanosm@unal.edu.co

Alejandro Abondano Romero es magíster en derecho privado con énfasis en responsabilidad patrimonial civil y del Estado, Universidad Externado de Colombia, y abogado, Universidad del Rosario. Con experiencia en la rama judicial y en derecho constitucional, ha investigado sobre restitución de tierras, conflicto armado y tenencia de la tierra.

<https://orcid.org/0000-0001-7727-1464>

Contacto: alejandro.abondano@est.uexternado.edu.co

Referencias

- Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, 10(2), 20539517231205476.
- Benzie, A., & Montasari, R. (2023). Bias, privacy and mistrust: Considering the ethical challenges of artificial intelligence. En *Applications for artificial intelligence and digital forensics in national security* (pp. 1-14). Springer Nature Switzerland.
- Bueno de Mesquita, B., Downs, G. W., Smith, A., & Cherif, F. M. (2005). Thinking inside the box: A closer look at democracy and human rights. *International Studies Quarterly*, 49(3), 439-457.
- Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Angiolillo, F., Bernhard, M., Borella, C., Cornell, A., Fish, M. S., Fox, L., Gastaldi, L., Gjerløw, H., Glynn, A., Good God, A., Grahn, S., Hicken, A., Kinzelbach, K., & Ziblatt, D. (2024a). *V-Dem codebook v14*. Varieties of Democracy (V-Dem) Project. https://www.v-dem.net/documents/38/V-Dem_Codebook_v14.pdf
- Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Marquardt, K. L., Medzihorsky, J., Pemstein, D., Fox, L., Gastaldi, L., Pernes, J., Rydén, O., von Römer, J., Tzelgov, E., Wang, Y., & Wilson, S. (2024b). *V-Dem methodology v14*. Varieties of Democracy (V-Dem) Project. https://v-dem.net/documents/39/v-dem_methodology_v14.pdf
- Correia, M., & Rodrigues, L. (2024). Security and privacy. En H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. M. Pereira, E. V. de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary perspectives on artificial intelligence and the law* (pp. 81-101). Springer Nature. https://doi.org/10.1007/978-3-031-41264-6_5

- De Asís Roig, R. (2024). De nuevo sobre inteligencia artificial y derechos humanos. *Revista Derechos y Libertades*, 51. <https://doi.org/10.20318/dyl.2024.8582>
- Dieu, O. (2023). Facial recognition technology, drones, and digital policing: Compatible with the fundamental right to privacy? En *Applications for artificial intelligence and digital forensics in national security* (pp. 39-54). Springer Nature Switzerland.
- Dieu, O., & Montasari, R. (2022). How states' recourse to artificial intelligence for national security purposes threatens our most fundamental rights. En *Artificial intelligence and national security* (pp. 19-45). Springer International Publishing.
- Donnelly, S. (2006). Reflecting on the rule of law: Its reciprocal relation with rights, legitimacy, and other concepts and institutions. *Annals of the American Academy of Political and Social Science*, 603(1), 37-53.
- Freedom House. (2024a). *Freedom in the world 2024. Methodology questions*. <https://tinyurl.com/2b7w74fm>
- Freedom House. (2024b). *Freedom in the world 2024. The mounting damage of flawed elections and armed conflict*. <https://tinyurl.com/23haz5xr>
- García Yzaguirre, V. (2023). Aproximaciones a la seguridad jurídica: una propuesta de reconstrucción. *Cuadernos Electrónicos de Filosofía del Derecho*, 50, 29-49. <https://doi.org/10.7203/CEFD.50.26379>
- Garriga, A. (2024). Los derechos ante los sistemas biométricos que incorporan inteligencia artificial. *Derechos y Libertades: Revista de Filosofía del Derecho y Derechos Humanos*, 51, 117-149.
- Ilustre Colegio de la Abogacía de Madrid. (2024, 13 de noviembre). *Sección Robótica - La Ley Europea de IA: proceso, contenido y futuro* [video]. YouTube. <https://www.youtube.com/live/lK-xXbIKsRo>
- International Institute for Democracy and Electoral Assistance – IDEA. (2023). *The global state of democracy indices methodology: Conceptualization and measurement framework, version 7*. <https://doi.org/10.31752/idea.2023.38>
- International Institute for Democracy and Electoral Assistance (IDEA). (2024). *The global state of democracy 2024 strengthening the legitimacy of elections in a time of radical uncertainty*. <https://doi.org/10.31752/idea.2024.55>
- Lualhé Shaelou, S., & Razmetaeva, Y. (2023). Challenges to fundamental human rights in the age of artificial intelligence systems: Shaping the digital legal order while upholding rule of law principles and European values. *ERA Forum*, 24(4), 567-587. <https://doi.org/10.1007/s12027-023-00777-2>
- Neves, M. P., & De Almeida, A. B. (2024). Before and beyond artificial intelligence: Opportunities and challenges. En H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. M. Pereira, E. V. de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary perspectives on artificial intelligence and the law* (pp. 107-125). Springer Nature. https://doi.org/10.1007/978-3-031-41264-6_6
- Nord, M., Lundstedt, M., Altman, D., Angiolillo, F., Borella, C., Fernandes, T., Gastaldi, L., Good God, A., Natsika, N., & Lindberg, S. I. (2024). *Democracy report 2024: Democracy winning and losing at the ballot* (Altman, D., Huertas-Hernández, S., & Villalobos, F., Trans.). University of Gothenburg; V-Dem Institute. <https://www.v-dem.net/publications/democracy-reports/>
- Pagallo, U. (2023). Dismantling four myths in AI & EU law through legal information 'about' reality. En H. Sousa Antunes, P. M. Freitas, A. L. Oliveira, C. M. Pereira, E. V. de Sequeira, & L. Barreto Xavier (Eds.), *Multidisciplinary perspectives on artificial intelligence and the law* (pp. 251-261). Springer Nature. https://doi.org/10.1007/978-3-031-41264-6_13
- Parlamento Europeo. (2020). *Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence* (2020/2014(INL)). <https://tinyurl.com/2j7zeaxs>
- Parlamento Europeo. (2024, 13 de junio). *Ley de Inteligencia Artificial* (Reglamento (UE) 2024/1689), versión del Diario Oficial. <https://artificialintelligenceact.eu/es/el-acto/>
- Programa de Naciones Unidas para el Desarrollo (PNUD). (2010). *Nuestra democracia*. Colección Obras de Sociología, Fondo de Cultura Económica.
- Programa de Naciones Unidas para el Desarrollo (PNUD). (2013). *Informe regional de desarrollo humano 2013-2014: Seguridad ciudadana con rostro humano: Diagnóstico y propuestas para América Latina*.
- Pulido Rodríguez, C. (2024). Los retos de medir la democracia: una revisión de los índices de democracia. *Revista Española de Ciencia Política*, 64, 155-178. <https://doi.org/10.21308/recp.64.06>

- Raposo, V. L. (2023a). The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal. *European Journal on Criminal Policy and Research*, 29(4), 515-533.
- Raposo, V. L. (2023b). (Do not) remember my face: Uses of facial recognition technology in light of the General Data Protection Regulation. *Information & Communications Technology Law*, 32(1), 45-63. <https://doi.org/10.1080/13600834.2022.2054076>
- Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. (2018). *Promoción y protección del derecho a la libertad de opinión y de expresión: Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (A/73/348)*. Asamblea General de las Naciones Unidas. <https://undocs.org/A/73/348>
- Ringrose, K. (2019). Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns. *Virginia Law Review Online*, 105, 57-66.
- Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: A social science perspective. *AI and Ethics*, 3(2), 369-379. <https://doi.org/10.1007/s43681-022-00196-y>
- Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). *Ethics of artificial intelligence: Case studies and options for addressing ethical challenges*. Springer Nature.
- Teo, S. A. (2024). Artificial intelligence and its 'slow violence' to human rights. *AI and Ethics*, 5, 1-16. <https://doi.org/10.1007/s43681-024-00547-x>
- Tilly, C. (2010). *Democracia*. Akal.
- Zech, H. (2021, abril). Liability for AI: Public policy considerations. *ERA Forum*, 22(1), 147-158. <https://doi.org/10.1007/s12027-020-00648-0>