

Inteligencia artificial como apoyo en la investigación criminal: retos legales y éticos.

Artificial Intelligence as a Tool in Criminal Investigations: Legal and Ethical Challenges.

Silvia Jakeline Rea Manobanda

Abogada y Magister en Criminalística y Ciencias Forenses.
Docente Investigador Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Criminalística, Universidad Estatal de Bolívar

<https://orcid.org/0009-0001-7618-7516>
srea@mailes.ueb.edu.ec

Gonzalo Xavier Vega Chico

Abogado y Magister en Criminalística y Ciencias Forenses.
Docente Investigador Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Criminalística, Universidad Estatal de Bolívar

<https://orcid.org/0009-0003-0821-7730>
gonzalo.vega@ueb.edu.ec

Leslie Alejandra Parra Guilcapi

Abogada y Magister en Derecho Constitucional. Docente Investigador Facultad de Jurisprudencia, Ciencias Sociales y Políticas, Carrera de Criminalística, Universidad Estatal de Bolívar

<https://orcid.org/0000-0002-2444-2626>
leslie.parra@ueb.edu.ec

Jonathan Mesías Guzmán García

Abogado y Magister en Derecho mención en Derecho Notarial y Registral
Investigador independiente

<https://orcid.org/0009-0000-0159-6684>
jhonathanmesias1710@gmail.com



Imaginario Social
Entidad editora
REDICME (reg-red-18-0061)

e-ISSN: 2737-6362
julio-diciembre 2026 Vol. 9-3-2026
<http://revista-imaginariosocial.com/index.php/es/index>

Recepción: 19 de mayo de 2026
Aceptación: 27 de junio de 2026

239-256

Atribución/Reconocimiento-NoComercial- CompartirIgual 4.0 Licencia Pública Internacional — CC

BY-NC-SA 4.0

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.es>

Resumen

La incorporación de la inteligencia artificial (IA) en la investigación criminal y la administración de justicia penal ha generado una transformación significativa en las técnicas de prevención, análisis forense digital y persecución del delito. A través del aprendizaje automático, la minería de datos y el procesamiento del lenguaje natural, las herramientas algorítmicas facilitan la georreferenciación de riesgos delictivos (*predictive policing*), el reconocimiento biométrico y la neutralización de redes criminales cifradas. No obstante, su implementación en el proceso penal plantea severas tensiones procesales, probatorias y éticas. La falta de explicabilidad y la opacidad algorítmica de los modelos de "caja negra" (*black box*) —agravadas por el secreto industrial de los desarrollos privados— limitan la auditabilidad de la prueba, afectando el derecho a la defensa, el principio de contradicción y la igualdad de armas. Asimismo, la presencia de sesgos algorítmicos en los datos de entrenamiento amenaza el derecho a la igualdad y la presunción de inocencia, mientras que las tecnologías de tecnovigilancia impactan el derecho a la privacidad e intimidad. Ante un panorama de vacíos normativos en la región iberoamericana, se concluye que la IA debe actuar únicamente como un instrumento auxiliar sometido a la supervisión humana indelegable (*human-in-the-loop*), bajo estándares de transparencia ("caja blanca") y auditoría pública que garanticen el respeto irrestricto de las garantías constitucionales del debido proceso.

Palabras clave: Inteligencia artificial, investigación criminal, prueba penal, debido proceso, opacidad algorítmica, sesgo algorítmico, derechos humanos.

Abstract

The incorporation of artificial intelligence (AI) into criminal investigation and the administration of criminal justice has brought about a significant transformation in crime prevention techniques, digital forensics, and law enforcement. Through machine learning, data mining, and natural language processing, algorithmic tools facilitate the georeferencing of criminal risks (*predictive policing*), biometric recognition, and the dismantling of encrypted criminal networks. However, its implementation in criminal proceedings raises severe procedural, evidentiary, and

ethical tensions. The lack of explainability and the algorithmic opacity of "black box" models—exacerbated by private trade secrets—hinder evidence auditability, undermining the right to defense, the adversarial principle, and the equality of arms. Furthermore, algorithmic biases in training data threaten the right to equality and the presumption of innocence, while techno-surveillance technologies impact privacy rights. Given the regulatory gaps in the Ibero-American region, this review concludes that AI must act strictly as an auxiliary tool subject to mandatory human oversight (human-in-the-loop), governed by transparency standards ("white box") and public auditing to ensure full compliance with constitutional due process guarantees.

Keywords: Artificial intelligence, criminal investigation, criminal evidence, due process, algorithmic opacity, algorithmic bias, human rights.

Introducción

En la actualidad, las sociedades atraviesan una era de cambio y transformación tecnológica caracterizada por la rápida irrupción de la inteligencia artificial (IA) en diversos sectores, incluido el ámbito jurídico y la administración de justicia penal (García Torres, 2024; Marcos Escobar, 2026; Martínez et al., 2025). La incorporación de esta tecnología busca facilitar tareas que tradicionalmente eran ejecutadas de forma exclusiva por operadores humanos, abarcando desde la automatización de gestiones documentales hasta el desarrollo de técnicas avanzadas para la persecución e investigación del delito. Apoyada en disciplinas como el aprendizaje automático (*machine learning*), el aprendizaje profundo (*deep learning*), el procesamiento del lenguaje natural (PLN) y la minería de datos jurídicos, la IA posee la capacidad de procesar volúmenes masivos de información, detectar patrones ocultos, realizar análisis forenses e inferir probabilidades de reincidencia o riesgos delictivos (Herrera Mamarandi et al., 2026; Martínez et al., 2025; Mendoza-Valladolid & Carrera-Pérez, 2026). No obstante, este despliegue no opera como una simple herramienta neutral, sino que genera una transformación profunda en la práctica del derecho e interpela sus fundamentos normativos y filosóficos (Martínez et al., 2025).

A pesar de los beneficios prometidos en términos de celeridad procesal, reducción de costos y descongestión de los juzgados, el empleo de la IA en la conformación de elementos probatorios y la investigación criminal suscita profundos dilemas éticos y jurídicos (García Torres, 2024; Marcos Escobar, 2026; Martínez et al., 2025). Una de las mayores preocupaciones se centra en la poca o nula transparencia y explicabilidad de los procedimientos algorítmicos automatizados, fenómeno ampliamente conocido como el problema de la "caja negra" (Furingo, 2025; Marcos Escobar, 2026; Mendoza-Valladolid). Esta opacidad responde tanto a la complejidad operativa propia de las redes neuronales profundas como a la protección de los desarrollos tecnológicos bajo el secreto industrial y los derechos de propiedad intelectual de empresas privadas. La imposibilidad de rastrear la secuencia lógica por la cual un algoritmo arriba a un resultado debilita la auditabilidad de la prueba y la trazabilidad de la evidencia, impidiendo que las partes procesales puedan ejercer un contradictorio efectivo y cuestionar de manera fundamentada la fiabilidad del resultado en sede judicial (Gangi Guillen, 2025; Marcos Escobar, 2026; Mendoza-Valladolid).

Asimismo, la literatura científica advierte de manera reiterada sobre el riesgo del sesgo algorítmico y la discriminación automatizada (García Guaranda & Jiménez Guartan, 2025; Mendoza-Valladolid; Miró Llinares, 2018). Puesto que los modelos se entrenan con datos históricos que con frecuencia reflejan prejuicios y desigualdades preexistentes en la sociedad o en las prácticas policiales, la IA tiende a reproducir e intensificar dichos sesgos, asignando, por ejemplo, puntuaciones de riesgo desproporcionadamente altas a minorías étnicas o colectivos vulnerables, tal como se ha documentado ampliamente en casos emblemáticos como el sistema COMPAS en Estados Unidos. A estas problemáticas se añaden las amenazas a la privacidad e intimidad por la recolección masiva de datos y el uso de tecnologías invasivas de reconocimiento biométrico o *deepfakes* (Furingo, 2025; Leal Coy, 2025; Miró Llinares, 2018; Muñoz Rodríguez, 2020). De este modo, la delegación o asistencia desenfundada en herramientas algorítmicas pone en tensión garantías constitucionales estructurantes del proceso penal acusatorio, tales como la presunción de inocencia, el derecho a la defensa, la igualdad de armas, el debido

proceso y la seguridad jurídica (Furingo, 2025; Marcos Escobar, 2026; Moreira Núñez & Conopoima Moreno, 2025; Rojas Rodriguez & Duran Alvarado, 2025).

Esta coyuntura se complica aún más ante la evidente brecha o vacío regulatorio existente. Aunque a nivel internacional han surgido iniciativas pioneras de gobernanza como el Reglamento de Inteligencia Artificial de la Unión Europea (*AI Act*) o los pronunciamientos jurisprudenciales de altas cortes en la región (Furingo, 2025; Gomez Duque et al., 2025; Rojas Rodriguez & Duran Alvarado, 2025), la mayoría de los ordenamientos procesales carecen de normas específicas y robustas que fijen reglas claras para la admisión, producción y valoración de la prueba generada por IA en sede de investigación penal (Garcia Guaranda & Jimenez Guartan, 2025; Marcos Escobar, 2026). Ante la necesidad imperiosa de equilibrar la innovación tecnológica con la tutela de los derechos humanos, el presente artículo de revisión tiene como objetivo analizar los principales retos legales y éticos que plantea el uso de la inteligencia artificial en la investigación criminal, examinando la viabilidad de su implementación bajo la exigencia irrenunciable de una supervisión humana y respetuosa de las garantías del debido proceso.

Metodología

La presente revisión de la literatura se desarrolló bajo un enfoque cualitativo, de diseño no experimental y con un alcance descriptivo-analítico y socio-jurídico (Garcia Guaranda & Jimenez Guartan, 2025; Gomez Duque et al., 2025). La adopción de este enfoque responde a la necesidad de examinar la intersección entre las innovaciones tecnológicas de la inteligencia artificial y las categorías conceptuales del derecho penal y procesal penal, permitiendo comprender la complejidad del fenómeno sin reducirlo a variables numéricas (Gomez Duque et al., 2025; Marcos Escobar, 2026).

Estrategia de Búsqueda y Fuentes de Información

La recolección del acervo documental se llevó a cabo mediante la indagación en bases de datos científicas e indexadas de reconocido prestigio académico tales como Scopus, Web of Science, SciELO, Redalyc, Dialnet, JSTOR y Google Scholar, así como

en repositorios institucionales, normativos y jurisprudenciales nacionales e internacionales.

Para orientar la búsqueda, se utilizaron términos clave y operadores booleanos combinados en español e inglés, entre los que destacan: ("inteligencia artificial" OR "artificial intelligence"), ("investigación criminal" OR "criminal investigation"), ("prueba penal" OR "digital evidence"), ("sesgo algorítmico" OR "algorithmic bias"), ("debido proceso" OR "due process") y ("transparencia" OR "explicabilidad") (García Guaranda & Jiménez Guartan, 2025; Bustamante-Cabrera et al., 2024).

Criterios de Elegibilidad

Para la selección del material bibliográfico se aplicaron criterios rigurosos de inclusión y exclusión orientados a garantizar la calidad, pertinencia metodológica y actualización científica de la información.

Criterios de inclusión: Artículos científicos arbitrados por pares, tratados dogmáticos, informes técnicos de organismos internacionales, cuerpos normativos y sentencias judiciales que abordaran de manera directa la aplicación de la inteligencia artificial en el ámbito penal, la investigación criminal y las garantías procesales. Se priorizaron publicaciones recientes producidas en el periodo 2018–2026, sin perjuicio de incorporar obras de valor histórico o fundacional para la doctrina.

Criterios de exclusión: Publicaciones científicas sin revisión por pares, trabajos con contenido meramente especulativo que carecieran de sustento jurídico o técnico, documentos incompletos, duplicados o cuyo enfoque no guardara relación directa con la investigación penal y sus dimensiones éticas o legales.

Procesamiento y análisis de la información

Para el procesamiento de los datos recopilados se empleó la técnica del análisis documental, el análisis exegético-normativo y el método hermenéutico-crítico (Marcos Escobar, 2026; Gómez Duque et al., 2025). La síntesis temática de la literatura se estructuró a través de fichas bibliográficas y matrices de triangulación de fuentes doctrinales, normativas y jurisprudenciales.

El análisis cualitativo de la información se organizó en torno a cinco ejes temáticos y conceptuales principales.

1. **Aplicaciones técnicas de la IA en la investigación penal:** Análisis predictivo del delito, reconocimiento biométrico, procesamiento de lenguaje natural y cibercriminalidad.
2. **Retos probatorios e idoneidad científica:** Admisibilidad, fiabilidad, cadena de custodia digital y el fenómeno de la "caja negra".
3. **Garantías procesales y debido proceso:** Presunción de inocencia, derecho a la defensa, contradicción, motivación judicial e igualdad de armas.
4. **Desafíos éticos e impactos en derechos humanos:** Sesgos algorítmicos, discriminación automatizada, supervisión humana indelegable y derecho a la privacidad.
5. **Marcos regulatorios y perspectiva comparada:** Evaluación de vacíos normativos, iniciativas legislativas y regulaciones internacionales como el Reglamento de Inteligencia Artificial de la Unión Europea (*AI Act*).

Resultados

La integración de la inteligencia artificial (IA) en la administración de justicia penal representa una transformación profunda que abarca desde la actividad investigativa y policial hasta la valoración probatoria e interpretación de derechos fundamentales (García Torres, 2024; Marcos Escobar, 2026; Martínez et al., 2025). A partir del análisis cualitativo y la triangulación del acervo documental, los hallazgos e interpretaciones críticas se organizan en torno a cuatro ejes temáticos fundamentales:

Aplicaciones de la inteligencia artificial en la investigación criminal: entre la eficiencia operativa y la necesidad de control

La evidencia científica demuestra que la IA se ha consolidado como un componente operativo transformador en las labores de prevención, investigación y persecución del delito (García Torres, 2024; Marcos Escobar, 2026; Pazmiño Alvarez, 2024).

Apoyada en la convergencia del aprendizaje automático (*machine learning*), el aprendizaje profundo (*deep learning*), el procesamiento del lenguaje natural (PLN), la visión por computadora y la analítica masiva de datos (*big data*), la IA permite procesar información no estructurada y detectar patrones complejos a velocidades inalcanzables para la capacidad humana (García Guaranda & Jiménez Guartan, 2025; Mendoza-Valladolid & Carrera-Pérez, 2026; Miró Llinares, 2018).

Vigilancia y policía predictiva

Los modelos predictivos aplican algoritmos sobre bases de datos históricas de criminalidad, registros de denuncias, variables geográficas y temporales para anticipar la ocurrencia de hechos punibles y delimitar "puntos calientes" (*hot spots*). Entre los sistemas institucionales más consolidados destacan PredPol (Estados Unidos y Reino Unido), el *Crime Anticipation System* (CAS) en Países Bajos, Skala en Alemania y KeyCrime en Italia (García Torres, 2024; Ortiz Alarcón, 2025; Pazmiño Álvarez, 2024). En el ámbito latinoamericano sobresalen proyectos e iniciativas de gestión de riesgo como el sistema PRISMA y el software Fiscal Watson en Colombia.

Identificación biométrica y reconocimiento facial

La biometría automatizada mediante IA ha revolucionado la investigación forense y el patrullaje de campo. Herramientas como el *Automated Biometric Identification System* (ABIS) o bases de datos como Clearview AI permiten extraer patrones morfológicos faciales y cotejarlos instantáneamente contra millones de registros policiales (Furingo, 2025; García Torres, 2024; Pazmiño Álvarez, 2024). Asimismo, la IA se aplica a la identificación automatizada de huellas dactilares latentes, otogramas, geometría de la mano y reconocimiento de voz o firma manuscrita (García Torres, 2024; Marcos Escobar, 2026; Perez, 2025).

Análisis forense digital, OSINT y lucha contra la cibercriminalidad

En la investigación del cibercrimen y la delincuencia organizada, la IA facilita el escrutinio de fuentes abiertas (OSINT) y redes sociales (SOCMINT), permitiendo detectar discursos de odio o propaganda extremista mediante herramientas como VERIPOL en España o proyectos europeos como PERICLES (García Torres, 2024;

Miró Llinares, 2018; Ortiz Alarcón, 2025). A nivel operativo, el procesamiento algorítmico ha sido determinante en operaciones multinacionales de Europol y Eurojust como el desmantelamiento de las redes de mensajería cifrada EncroChat, Matrix y la Operación Ghost, donde el análisis automatizado de millones de mensajes encriptados permitió neutralizar estructuras criminales transnacionales (Ortiz Alarcón, 2025).

A continuación, la Tabla 1 sintetiza las principales aplicaciones identificadas en la investigación penal:

Tabla 1: Síntesis de las aplicaciones de la Inteligencia Artificial en la investigación criminal

Ámbito de aplicación	Tecnología / Subdisciplina empleada	Herramientas / Casos de referencia	Utilidad y función investigativa
Policía predictiva y mapeo de riesgo	Aprendizaje automático (<i>Machine Learning</i>), regresión y minería de datos (García Torres, 2024; Miró Llinares, 2018)	PredPol (EE. UU./Reino Unido), CAS (Países Bajos), Skala (Alemania), PRISMA (Colombia) (García Torres, 2024; Gomez Duque et al., 2025; Ortiz Alarcón, 2025)	Georreferenciación de <i>hot spots</i> , anticipación de patrones delictivos espaciotemporales y estimación del riesgo de reincidencia (García Torres, 2024; Miró Llinares, 2018; Pazmiño Alvarez, 2024).
Identificación biométrica y vigilancia	Visión por computadora, redes neuronales y reconocimiento de patrones (García Torres, 2024; Miró Llinares, 2018)	ABIS (España), Clearview AI, análisis de huellas e iris (García Torres, 2024; Pazmiño Alvarez, 2024)	Cotejo automatizado masivo de rostros e impresiones dactilares en tiempo real o diferido para la localización de sospechosos y prófugos (Furingo, 2025; García Torres, 2024; Herrera Mamarandi et al., 2026).
Análisis forense digital y cibercrimen	Procesamiento del Lenguaje Natural (PLN) y analítica de redes (Martínez et al., 2025; Miró Llinares, 2018)	VERIPOL (España), herramientas OSINT/SOCMINT, Proyecto PERICLES (García Torres, 2024; Miró Llinares, 2018; Ortiz Alarcón, 2025)	Extracción automatizada de evidencia digital, detección de denuncias falsas y filtrado de discursos de odio o radicalización en línea (García Torres, 2024; Miró Llinares, 2018; Ortiz Alarcón, 2025).
Intercepción de redes criminales cifradas	Desencriptación algorítmica y analítica de <i>big data</i> (Miró Llinares, 2018; Ortiz Alarcón, 2025)	Operaciones de Europol: EncroChat, Matrix, Operación Ghost (Ortiz Alarcón, 2025)	Procesamiento masivo de comunicaciones cifradas, reconstrucción de estructuras delictivas y neutralización de redes transnacionales (Ortiz Alarcón, 2025).

Frente a estos avances, la discusión teórica evidencia una abierta tensión entre la literatura enfocada en la gestión de la seguridad y la doctrina procesal garantista. Mientras los enfoques gerenciales destacan la capacidad de la IA para descongestionar juzgados y optimizar la asignación de recursos, la doctrina procesalista advierte sobre el peligro de instaurar un "modelo actuarial" de justicia. La celeridad y la eficiencia operativa no pueden erigirse como valores superiores a las garantías procesales. La sustitución de la indagación crítica por inferencias automáticas amenaza con deshumanizar el proceso penal, distanciando al juzgador del contacto directo con los hechos y restando validez jurídica a las actuaciones que restrinjan facultades de defensa sin la debida justificación (Furingo, 2025; Marcos Escobar, 2026; Martínez et al., 2025; Moreira Núñez & Conopoima Moreno, 2025; Mendoza-Valladolid & Carrera-Pérez, 2026).

Retos legales y probatorios: La "Caja Negra" y la explicabilidad en la prueba penal

A pesar del potencial operativo de la IA, su uso genera graves problemas procesales y probatorios en la fase de juzgamiento, condicionando la validez de las decisiones judiciales (Furingo, 2025; Marcos Escobar, 2026; Mendoza-Valladolid & Carrera-Pérez, 2026).

El fenómeno de la "caja negra" y el secreto industrial

Gran parte de los modelos de aprendizaje profundo (*deep learning*) producen resultados cuyas secuencias lógicas e inferenciales ocultas resultan incomprensibles para los seres humanos. Esta opacidad algorítmica o efecto "caja negra" se profundiza cuando los desarrollos tecnológicos provienen del sector privado y se encuentran amparados por el secreto industrial y los derechos de propiedad intelectual. El rehusarse a develar el código fuente a las partes impone un velo que impide auditar la trazabilidad de los datos y el proceso de decisión (Marcos Escobar, 2026; Mendoza-Valladolid & Carrera-Pérez, 2026).

Vulneración del principio de contradicción y la igualdad de armas

En el proceso penal acusatorio, el derecho a la prueba se constituye como una derivación directa del derecho a la defensa y un presupuesto epistemológico para la

averiguación de la verdad (García Guaranda & Jiménez Guartan, 2025; Marcos Escobar, 2026). Cuando la acusación fundamenta un hecho sobre la base de un dictamen u obtención algorítmica opaca, se priva a la defensa de examinar la metodología probatoria. La imposibilidad de cuestionar los datos de entrenamiento o los márgenes de error coloca al investigado en estado de indefensión, quebrantando la igualdad de armas procesal (Furingo, 2025; Marcos Escobar, 2026; Mendoza-Valladolid & Carrera-Pérez, 2026).

Cadena de custodia digital y manipulación sintética

La evidencia tecnológica es volátil, duplicable y susceptible de alteración. La reciente irrupción de la IA generativa amplifica estos riesgos mediante la creación de evidencias sintéticas hiperrealistas o *deepfakes* (alteración de audios, videos e imágenes). La amenaza de los *deepfakes* introduce dudas sistemáticas sobre la autenticidad e integridad de la prueba digital, exigiendo el fortalecimiento de la cadena de custodia informática, el sellado de tiempo y la verificación pericial de metadatos (Herrera Mamarandi et al., 2026; Mendoza-Valladolid & Carrera-Pérez, 2026; Muñoz Rodríguez, 2020).

El dilema de la "caja negra" (*black box*) representa el punto de mayor conflicto dogmático entre la tecnología y el derecho a la prueba. Permitir que la imputación se apoye en herramientas cuyo código fuente o lógica matemática se oculta tras secretos comerciales distorsiona el equilibrio procesal (Furingo, 2025; Marcos Escobar, 2026; Miró Llinares, 2018; Mendoza-Valladolid & Carrera-Pérez, 2026). La literatura coincide en que los resultados algorítmicos no constituyen un medio de prueba autónomo ni gozan de presunción de infalibilidad. Para que la evidencia asistida por IA sea admisible, debe someterse a estándares de idoneidad y validez científica similares a los criterios *Daubert* que exijan operar en entornos de "caja blanca" (*explainable AI*), con tasas de error conocidas y sujetas al escrutinio de peritos independientes en el juicio oral.

El despliegue de la IA en la persecución penal impacta directamente en la dignidad humana y las libertades fundamentales garantizadas internacionalmente (Bustamante-Cabrera et al., 2024; Gangi Guillen, 2025; Leal Coy, 2025).

Sesgo algorítmico y discriminación automatizada

Los algoritmos aprenden a partir de conjuntos de datos históricos que frecuentemente reflejan patrones de desigualdad o sesgos institucionales del pasado. Al ser entrenados con información sesgada, los modelos automatizan, perpetúan y magnifican prejuicios raciales, geográficos y socioeconómicos. El estudio del sistema COMPAS en Estados Unidos constituye el ejemplo de referencia: se demostró que el software asignaba altas puntuaciones de riesgo de reincidencia a personas afroamericanas a una tasa desproporcionadamente mayor que a personas caucásicas con historiales penales similares. La discriminación algorítmica contraviene de forma directa el derecho a la igualdad ante la ley y la no discriminación (Gangi Guillen, 2025; Marcos Escobar, 2026; Moreira Núñez & Conopoima Moreno, 2025).

Riesgo a la presunción de inocencia y la culpabilidad por el hecho

El empleo de estimaciones estadísticas de peligrosidad o probabilidad de reincidencia para fundar decisiones de medidas cautelares (como la prisión preventiva) sustituye el juzgamiento de la conducta individual por perfiles de grupo o comportamientos históricos de terceros. Esta práctica pervierte el principio de culpabilidad por el hecho y vulnera la presunción de inocencia, transformando una proyección algorítmica en una "condena o restricción de libertad anticipada" (Furingo, 2025; Marcos Escobar, 2026; Rojas Rodríguez & Duran Alvarado, 2025).

Afectación a la privacidad e intimidad (tecnovigilancia)

La recopilación ininterrumpida de imágenes, patrones biométricos, geolocalización y rastreo de metadatos mediante la denominada "tecnovigilancia" y el reconocimiento facial masivo en espacios públicos constituye una injerencia grave en la esfera privada. Desplegar estas herramientas sin orden judicial previa ni criterios de proporcionalidad afecta la intimidad informática y el *habeas data* (Furingo, 2025; Leal Coy, 2025; Miró Llinares, 2018; Muñoz Rodríguez, 2020).

Los hallazgos permiten desmitificar la supuesta "neutralidad e imparcialidad" de los sistemas informáticos. Lejos de erradicar la arbitrariedad humana, los algoritmos reflejan y automatizan los prejuicios sociales y policiales de los datos con los que fueron alimentados. Cuando una estimación estadística grupal se traduce en una

decisión restrictiva de la libertad individual, se quiebra la exigencia de evaluar la responsabilidad de la persona por lo que ha hecho y no por lo que el algoritmo supone que hará. La ética algorítmica no es un mero adorno teórico, sino un imperativo jurídico para evitar que la IA se convierta en un instrumento de estigmatización y discriminación automatizada (Bustamante-Cabrera et al., 2024; Gangi Guillen, 2025; Marcos Escobar, 2026; Moreira Núñez & Conopoima Moreno, 2025).

El Modelo de la Unión Europea: Reglamento de IA (AI Act) y GDPR

La Unión Europea lidera la gobernanza global mediante el Reglamento de Inteligencia Artificial (Reglamento UE 2024/1689 - *AI Act*) Bajo un enfoque basado en riesgos (Furingo, 2025; García Torres, 2024):

- **Sistemas Prohibidos:** Se prohíbe de forma general la identificación biométrica remota en tiempo real en espacios públicos por las fuerzas de seguridad (salvo excepciones judiciales estrictas sobre delitos graves o terrorismo inminente) y la evaluación del riesgo individual basada únicamente en la elaboración de perfiles (Furingo, 2025; García Torres, 2024; Ortiz Alarcón, 2025).
- **Sistemas de alto riesgo:** Se clasifica como de alto riesgo a las tecnologías empleadas en la investigación penal y la administración de justicia, condicionando su despliegue a evaluaciones previas de impacto en derechos fundamentales, registros de trazabilidad, transparencia y la garantía de una supervisión humana activa e indelegable (*human-in-the-loop*). En España, la creación de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) y el Real Decreto-Ley 6/2023 complementan esta estructura regulando las actuaciones procesales asistidas y automatizadas (Furingo, 2025; García Torres, 2024; Ortiz Alarcón, 2025).

El panorama en América Latina y los vacíos regulatorios

En la región iberoamericana prevalece la fragmentación legislativa y la falta de normas específicas para la prueba algorítmica en la investigación penal (García

Guaranda & Jimenez Guartan, 2025; Marcos Escobar, 2026; Moreira Núñez & Conopoima Moreno, 2025; Herrera Mamarandi et al., 2026).

- **Colombia:** Aunque existen proyectos de ley marco en trámite (como el Proyecto de Ley 422/2025), la delimitación del uso de la IA en la justicia ha sido establecida por la jurisprudencia de la Corte Constitucional. Mediante la Sentencia T-323/24, la Corte fijó que las herramientas de IA son admisibles únicamente para tareas administrativas, de gestión o soporte documental, prohibiendo categóricamente la sustitución de la motivación judicial y del razonamiento humano del juez (Gomez Duque et al., 2025; Moreira Núñez & Conopoima Moreno, 2025; Rojas Rodriguez & Duran Alvarado, 2025).
- **Ecuador:** Pese a contar con reglas para la pericialidad en el Código Orgánico Integral Penal (COIP) y tutelar el *habeas data* en la Ley Orgánica de Protección de Datos Personales, existe una total ausencia de normas procesales especializadas sobre el uso de la IA en la investigación criminal y la valoración de la evidencia digital. Ello genera incertidumbre jurídica sobre la licitud y admisibilidad procesal del reconocimiento facial y los peritajes automatizados (Herrera Mamarandi et al., 2026; Pazmiño Alvarez, 2024).

La comparación regulatoria refleja dos velocidades de respuesta institucional. Mientras la Unión Europea ha construido un marco garantista restrictivo y preventivo, América Latina enfrenta un escenario de omisión legislativa donde los tribunales constitucionales han tenido que reaccionar para fijar límites infranqueables a la automatización de las decisiones judiciales (Garcia Guaranda & Jimenez Guartan, 2025; Gomez Duque et al., 2025; Moreira Núñez & Conopoima Moreno, 2025; Rojas Rodriguez & Duran Alvarado, 2025).

Ante el obstáculo que representa el secreto comercial de las empresas tecnológicas privadas, cobra especial fuerza la propuesta doctrinal que defiende que las herramientas de IA utilizadas por las autoridades en la investigación penal deben ser desarrolladas bajo la titularidad del sector público (en sede de las propias Fiscalías o Ministerios Públicos. La titularidad pública del software garantiza que los algoritmos sean abiertos, que las partes procesales tengan acceso a los datos de entrenamiento

para su auditoría y que las controversias técnicas se resuelvan sin la barrera de las patentes comerciales, asegurando la transparencia y la confianza ciudadana en la administración de justicia (Marcos Escobar, 2026).

Conclusiones

La presente revisión de la literatura permite sintetizar las principales implicaciones jurídicas, probatorias y éticas derivadas del uso de la inteligencia artificial (IA) en la investigación criminal y la administración de justicia penal, derivando en las siguientes conclusiones:

La inteligencia artificial constituye una herramienta de alto valor técnico y operacional para optimizar las labores investigativas, facilitando el procesamiento masivo de datos no estructurados, el análisis forense digital, la georreferenciación de riesgos y la neutralización de complejas estructuras de cibercriminalidad o redes de comunicación cifrada. Sin embargo, su valor jurídico es estrictamente instrumental e indivisible de la verificación humana, careciendo de autonomía decisoria o probatoria.

La opacidad algorítmica y la reserva del código fuente bajo el secreto industrial privado constituyen un obstáculo insuperable para el ejercicio de las garantías constitucionales del proceso penal acusatorio. La falta de explicabilidad técnica y trazabilidad de los datos impide la auditabilidad de la prueba, menoscabando el principio de contradicción, el derecho a la defensa y la igualdad de armas de la persona investigada.

Los sistemas inteligentes no son neutros; cuando se entrenan con datos históricos sesgados o discriminatorios, replican e intensifican la estigmatización racial, geográfica o socioeconómica. La utilización de proyecciones estadísticas o evaluaciones de riesgo algorítmico para sustentar la privación preventiva de la libertad vulnera la presunción de inocencia, desvirtuando el principio de culpabilidad por el hecho. Del mismo modo, la tecnovigilancia masiva sin control estricto violenta la intimidad e indemnidad digital de la ciudadanía.

Mientras la Unión Europea ha consolidado un modelo regulatorio preventivo mediante el Reglamento de Inteligencia Artificial (*AI Act*), en la región

iberoamericana y latinoamericana con particular énfasis en países como Ecuador prevalece un vacío legislativo en materia de prueba algorítmica. Esta omisión ha obligado a las altas cortes constitucionales a reaccionar, delimitando que la IA solo es admisible como soporte administrativo y prohibiendo la sustitución de la motivación judicial humana.

Referencias Bibliográficas

- Bustamante-Cabrera, G. I., Zuviría-López, Z. R., & Mondragón-Barrios, L. (2024). Desafíos éticos y humanísticos en la inteligencia artificial y la robótica: Metasíntesis. *Apuntes de Bioética*, 7(2), AdB1147. <https://doi.org/10.35383/apuntes.v7i2.1147>
- Furingo, C. I. (2026). La Inteligencia Artificial: ¿innovación o amenaza para las garantías procesales en la justicia penal?. *Revista de Derecho de la UNED (RDUNED)*, (36), 101–132. <https://doi.org/10.5944/rduned.36.2025.47721>
- Gangi Guillen, G. K. (2025). Derechos humanos y derecho penal en la era de la inteligencia artificial. Retos y propuestas. *Cuadernos de RES PUBLICA en Derecho y Criminología*, (8), 1–14. <https://doi.org/10.46661/respublica.11635>
- García Guaranda, J. W., & Jiménez Guartan, J. Á. (2025). El uso y manejo de la inteligencia artificial como herramienta en las pericias en el sistema procesal penal ecuatoriano. Una revisión sistemática. *RECIAMUC*, 9(3), 224–248. [https://doi.org/10.26820/reciamuc/9.\(3\).julio.2025.224-248](https://doi.org/10.26820/reciamuc/9.(3).julio.2025.224-248)
- García Torres, M. L. (2024). La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal. *Ciencia Policial*, (183), 91–132. <https://doi.org/10.14201/cp.32177>
- Gómez Duque, C. A., Cruz, W., & Mendoza Munar, L. (2025). *Implicaciones éticas con la implementación de la inteligencia artificial en el derecho penal colombiano* [Trabajo de grado de pregrado, Universidad Cooperativa de Colombia]. Repositorio Institucional UCC
- Herrera Mamarandi, D. A., Gordón Lucero, B. J., & Gutiérrez Romero, D. P. (2026). Uso de la inteligencia artificial en la investigación criminal y el derecho penal

- ecuatoriano: Retos procesales, probatorios y éticos. *Polo del Conocimiento*, 11(6), 823–838. <https://doi.org/10.23857/pc.v11i6.11796>
- Leal Coy, P. C. (2025). Inteligencia artificial en el derecho penal y los desafíos para la protección de la privacidad. *Revista de Postgrados de Derecho*, 1(1), 57–68. <https://doi.org/10.36314/postgradoderecho.v1i1.5>
- Marcos Escobar, S. E. (2026). El problema de la transparencia y explicabilidad algorítmica de la inteligencia artificial aplicada en la investigación penal y el derecho a la prueba. *IBERO CIENCIAS - Revista Científica y Académica*, 5(2), 3419–3435. <https://doi.org/10.63371/ic.v5.n2.a1258>
- Martínez Villacres, T. D., Llanos García, R. V., Núñez Ribadeneyra, R. A., & Noboa Larrea, G. E. (2025). La inteligencia artificial en el derecho: Transformaciones, desafíos éticos y perspectivas jurídicas. *Código Científico Revista de Investigación*, 6(1), 2044–2057. <https://doi.org/10.55813/gaea/ccri/v6/n1/1010>
- Mendoza-Valladolid, N. G., & Carrera-Pérez, G. E. (2026). La Inteligencia Artificial como herramienta probatoria: Retos y riesgos en el derecho penal contemporáneo. *Space Scientific Journal of Multidisciplinary*, 4(2), 31–47. <https://doi.org/10.63618/omd/ssjm/v4/n2/69>
- Miró Llinares, F. (2018). Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, (20), 87–130. <https://doi.org/10.5944/rdpc.20.2018.26446>
- Moreira Núñez, L. F., & Conopoima Moreno, Y. D. C. (2025). Retos éticos, normativos y prácticos en el uso de inteligencia artificial en los procesos constitucionales. *LEX - Revista de Investigación en Ciencias Jurídicas*, 8(31), 2684–2699. <https://doi.org/10.33996/revistalex.v9i31.436>
- Muñoz Rodríguez, A. B. (2020). El impacto de la inteligencia artificial en el proceso penal. *Anuario de la Facultad de Derecho. Universidad de Extremadura*, (36), 695–728. <https://doi.org/10.17398/2695-7728.36.695>

-
- Ortiz Alarcón, E. A. (2025). *El impacto de la inteligencia artificial en la identificación y prevención del delito* [Trabajo de fin de grado, Universidad Europea de Madrid]. Repositorio Institucional UEM.
- Pazmiño Alvarez, M. B. (2024). El uso de la inteligencia artificial en la investigación criminal. *Polo del Conocimiento*, 9(12), 2236–2244. <https://doi.org/10.23857/pc.v9i12.8616>
- Rojas Rodriguez, L. A., & Duran Alvarado, W. H. (2025). *Introducción a la Inteligencia Artificial en el contexto derecho penal* [Trabajo de investigación de maestría, Universidad Libre]. Repositorio Institucional Unilibre.