Tribunal. Revista en Ciencias de la Educación y Ciencias / http://www.revistatribunal.org
Volumen 6 / N° 16 / julio - septiembre 2026 / ISSN: 2959-6513 / pp. 1 – 15
http://doi.org/10.59659/revistatribunal.v6i16.459

Review Article

Inteligencia artificial y tecnologías emergentes en el sistema de justicia penal peruano

Artificial intelligence and emerging technologies in the Peruvian criminal justice system

Yessica Angelica Anicama Arones[1]

Resumen

Introducción: El crimen organizado ha evolucionado hacia un paradigma tecnológico avanzado, utilizando criptoactivos, comunicaciones encriptadas e inteligencia artificial, lo que genera una asimetría crítica frente a los sistemas de justicia penal tradicionales en América Latina. **Objetivo:** Evaluar la suficiencia del marco normativo penal peruano frente a la evidencia digital algorítmica y proponer estrategias jurídicas para su admisión constitucional. **Metodología:** Se aplicó un análisis dogmático-comparativo junto con tests de subsunción normativa, examinando la compatibilidad de algoritmos predictivos, sistemas de reconocimiento facial y herramientas forenses automatizadas con las garantías procesales constitucionales. **Resultados:** Se identificaron riesgos constitucionales derivados de la opacidad de los procesos algorítmicos, afectando derechos fundamentales como el derecho de defensa y la motivación de las resoluciones judiciales. La normativa actual carece de mecanismos claros para garantizar transparencia, auditabilidad y proporcionalidad en el uso de evidencia digital. **Conclusiones:** Se propone desarrollar un estatuto de "Debido Proceso Tecnológico" que integre estándares de transparencia algorítmica, auditabilidad y proporcionalidad digital. Este marco, inspirado en regulaciones comparadas de la Unión Europea y Estados Unidos, permitiría que la digitalización de la persecución penal preserve los derechos fundamentales de los ciudadanos y, al mismo tiempo, potencie la eficiencia investigativa frente al crimen organizado contemporáneo.

Palabras clave: Debido proceso; Crimen organizado; Justicia penal; Inteligencia artificial; Lagunas normativas; Prueba algorítmica

Abstract

Introduction: Organized crime has evolved toward an advanced technological paradigm, utilizing crypto-assets, encrypted communications, and artificial intelligence. This shift has created a critical asymmetry when compared to traditional criminal justice systems in Latin America. **Objective:** To evaluate the adequacy of the Peruvian criminal legal framework regarding algorithmic digital evidence and to propose legal strategies for its constitutional admissibility. **Methodology:** A legal-dogmatic and comparative analysis was applied, alongside normative subsumption tests. The study examined the compatibility of predictive algorithms, facial recognition systems, and automated forensic tools with constitutional procedural guarantees. **Results:** Significant constitutional risks were identified stemming from algorithmic opacity, which affects fundamental rights such as the right to a defense and the requirement for reasoned judicial decisions. Current regulations lack clear mechanisms to ensure transparency, auditability, and proportionality in the use of digital evidence. **Conclusions:** The

[1]Universidad Nacional Mayor de San Marcos. Lima, Perú
Artículo recibido 4 de marzo 2026 | Aceptado 8 de mayo 2026 | Publicado 1 de julio 2026
Autor de correspondencia: yessica.anicama@unmsm.edu.pe
Conflicto de interés: La autora declaran no tener conflicto de intereses.
Como citar: Anicama Arones, A. A. (2026). Inteligencia artificial y tecnologías emergentes en el sistema de justicia penal peruano. *Revista Tribunal*, 6(16), 1-15. http://doi.org/10.59659/revistatribunal.v6i16.459

study proposes the development of a "Technological Due Process" statute that integrates standards for algorithmic transparency, auditability, and digital proportionality. This framework, inspired by comparative regulations from the European Union and the United States, would allow the digitalization of criminal prosecution to preserve citizens' fundamental rights while enhancing investigative efficiency against contemporary organized crime.

Keywords: Due process; Organized crime; Criminal justice; Artificial intelligence; Regulatory gaps; Algorithmic evidence.

Introducción

La transformación digital del crimen organizado ha configurado un escenario de asimetría tecnológica sin precedentes en los sistemas de justicia penal latinoamericanos, donde estructuras delictivas sofisticadas emplean herramientas de inteligencia artificial, criptoactivos y comunicaciones encriptadas, denominado Crimen 4.0, mientras las instituciones de persecución penal permanecen ancladas en paradigmas burocráticos tradicionales que pueden caracterizarse como Justicia 1.0. Esta disparidad operativa genera consecuencias sistémicas que trascienden la mera ineficiencia administrativa para constituir una amenaza estructural al Estado de Derecho y la seguridad ciudadana.

En efecto, los datos empíricos revelan la magnitud de esta problemática. En América Latina se concentra aproximadamente un tercio de los homicidios globales pese a representar menos del 10% de la población mundial, con tasas que oscilan entre 23-25 homicidios por cada 100,000 habitantes durante la década de 2010, cuadruplicando el promedio global de 6 por 100,000 (Díaz et al., 2025). Particularmente relevante resulta su hallazgo de que el 40% de la evidencia digital se pierde debido a demoras burocráticas inherentes a los sistemas judiciales tradicionales, mientras las organizaciones criminales incorporan sistemáticamente herramientas de procesamiento de lenguaje natural para detectar y explotar vulnerabilidades en redes sociales, perpetrando delitos de ciberbullying y violencia sexual con algoritmos que alcanzan precisiones del 97% en Brasil para predicción de homicidios, aunque con riesgos significativos de sesgos espaciales.

Asimismo, esta asimetría se manifiesta de manera particularmente aguda en el contexto de los sistemas de inteligencia artificial aplicados a la seguridad pública en la región. En este sentido, Fair Trials, (2024) identifica que sistemas de reconocimiento facial como el implementado en Brasil bajo la denominación Oi exhiben patrones discriminatorios sistemáticos, con sesgos algorítmicos que afectan desproporcionadamente a individuos de ascendencia africana, mientras que programas de policía predictiva como Proximity Policing en México impactan negativamente a comunidades LGBTQ+ y sectores de bajos ingresos. Los datos son contundentes: entre el 50-60% de las predicciones generadas por modelos algorítmicos en Colombia resultan inexactas, generando situaciones de acoso policial sin fundamento delictivo real, mientras que la implementación de PredPol en Uruguay no logró superar los métodos tradicionales de prevención delictiva.

En el específico ordenamiento jurídico peruano, esta problemática adquiere dimensiones constitucionales críticas. En esta dirección, Smart, (2025) documenta que hasta enero de 2025, Perú ha introducido 17 iniciativas legislativas relacionadas con inteligencia artificial, empero presenta gaps significativos en términos de exigibilidad y aplicabilidad práctica. La dependencia estructural de tecnología extranjera y la ausencia de mecanismos

efectivos de disputabilidad en las decisiones algorítmicas configuran lo que el autor denomina subordinación normativa, erosionando la soberanía tecnológica del Estado. Las dos leyes promulgadas hasta la fecha, la Ley N° 31814, (2023), que promueve el uso de IA para desarrollo económico y social, y la Ley N.° 32082, (2024), que regula IA en servicios consulares, carecen de mecanismos ejecutables y no abordan los vacíos específicos del proceso penal.

A nivel regional, el panorama evidencia la urgencia de esta transformación. Al respecto, Europol, (2025) establece que la inteligencia artificial ha reconfigurado fundamentalmente el paisaje del crimen organizado, actuando simultáneamente como catalizador y conductor de las operaciones delictivas, con aproximadamente el 80% de las estructuras criminales organizadas incorporando tecnologías 4.0 para ciberdelincuencia. El informe revela que el 50% de los casos de secuestro de datos involucran componentes de IA, mientras los sistemas judiciales tradicionales sufren lentitud burocrática que resulta en la pérdida del 30% de la evidencia digital por demoras procesales.

Por otro lado, esta transformación tecnológica del crimen encuentra respaldo en los análisis del Departamento de Seguridad Nacional de Estados Unidos (DHS, 2024), que identifica cómo la IA incrementa exponencialmente la vulnerabilidad de todos los ciudadanos ante actividades criminales, particularmente mediante la generación de contenido sintético, deepfakes, que resulta prácticamente indistinguible del contenido auténtico. Los datos indican que aproximadamente el 70% de las actividades ilícitas contemporáneas incorporan elementos de fraude potenciado por IA, mientras las ineficiencias judiciales estructurales generan pérdidas sistemáticas de evidencia debido a procesos burocráticos inadecuados para el tratamiento de prueba digital.

Sin embargo, la respuesta regulatoria peruana ha resultado insuficiente y fragmentaria. El Cefeidas Group, (2023) analiza que la Estrategia Nacional de Inteligencia Artificial (ENIA) de 2021 aspira al liderazgo regional en investigación, desarrollo e innovación, aunque la OCDE critica severamente la estrategia por carecer de objetivos cuantificables, mecanismos de financiamiento sostenible, instrumentos de monitoreo efectivos y designación clara de actores responsables. La ley de julio de 2023 que declara la IA de interés nacional establece seis principios, seguridad supervisada, enfoque multi-stakeholder, gobernanza digital, sociedad digital, desarrollo ético responsable y privacidad, pero enfrenta desafíos críticos de continuidad institucional y asignación de recursos.

En particular, la evidencia empírica más contundente de esta asimetría operativa proviene del estudio de Aliaga et al., (2025) sobre operaciones encubiertas digitales de la Policía Nacional del Perú. Su investigación cualitativa, basada en entrevistas semiestructuradas a 16 oficiales especializados y análisis documental mediante ATLAS.ti, revela que estas operaciones involucran la creación de identidades digitales ficticias para infiltrar redes criminales en plataformas como redes sociales, aplicaciones encriptadas y Dark Web, targeting delitos como extorsión, fraude informático y lavado de dinero. Significativamente, mientras el 87% de los oficiales considera efectivas las operaciones digitales, únicamente el 34% estima que la policía actualiza su tecnología con la velocidad requerida para contrarrestar grupos de crimen organizado, que alcanzan el 86% de actualización tecnológica.

En este sentido, el CEJA, (2024) ha reconocido institucionalmente esta problemática mediante su Programa Regional sobre Inteligencia Artificial e ICT en Justicia para Perú y otros países

latinoamericanos, destinado a fortalecer el conocimiento sobre IA en administración de justicia y explorar oportunidades y desafíos en el contexto regional. La implementación prevista para 18 meses, pendiente de aprobación del Departamento de Estado de Estados Unidos, evidencia el reconocimiento internacional de las brechas regulatorias existentes.

En cuanto, a la dimensión financiera del problema adquiere características alarmantes. En esta línea, Dote y Espinosa, (2025) establecen que las criptomonedas facilitan sistemáticamente flujos financieros ilícitos, con riesgos que incluyen arbitraje regulatorio en estándares anti-lavado de dinero. Los avances recientes en IA, particularmente Graph Neural Networks (GNNs) y aprendizaje auto-supervisado, han mejorado significativamente la detección de transacciones sospechosas en criptoactivos, empero los sistemas judiciales tradicionales peruanos enfrentan ineficiencias burocráticas y vacíos regulatorios que vulneran el debido proceso en la admisibilidad de prueba digital.

De igual modo, la UNODC, (2024) documenta que el fraude cibernético genera pérdidas financieras anuales estimadas entre US$18-37 billones, con ganancias criminales de US$27.4-36.5 billones, impulsados por trabajo forzado en operaciones de estafas. La IA actúa como multiplicador exponencial del fraude cibernético, automatizando phishing, perfilamiento de víctimas y estafas personalizadas multiidioma. Los incidentes de deepfakes en la región Asia-Pacífico experimentaron un crecimiento del 1,530% entre 2022-2023, evidenciando la velocidad de adopción tecnológica del crimen organizado.

En consecuencia, una consecuencia lógica de esta asimetría tecnológica es la configuración de lo que puede denominarse una aporía normativa en el sistema procesal penal peruano. El Código Procesal Penal de 2004, estructurado bajo paradigmas de prueba física y testimonial, carece de los instrumentos dogmáticos necesarios para procesar evidencia generada por algoritmos de caja negra. La interrogante fundamental surge: ¿cómo puede ejercerse el derecho de defensa ante un algoritmo ininteligible? ¿Cómo puede garantizarse el principio de contradicción procesal frente a sistemas que operan mediante procesos opacos y no auditables?

No obstante, la solidez de los argumentos que demuestran la necesidad operativa de incorporar IA en la persecución penal, cabe objetar que su implementación bajo el actual marco normativo genera un escenario de inconstitucionalidad por omisión. La ausencia de regulación específica para la evidencia algorítmica vulnera sistemáticamente el derecho a la prueba y la defensa procesal, principios consagrados en el artículo 139 de la Constitución Política del Perú. Sin mecanismos de transparencia, auditabilidad y explicabilidad algorítmica, toda prueba generada por IA podría ser declarada ilícita bajo la doctrina del fruto del árbol envenenado.

Por lo tanto, ante esta problemática, la presente investigación sostiene que la incorporación de la inteligencia artificial en la persecución del crimen organizado en Perú constituye una necesidad operativa ineludible debido a la asimetría tecnológica documentada; sin embargo, su implementación bajo el actual Código Procesal Penal genera un escenario de inconstitucionalidad por omisión que vulnera el derecho a la prueba y la defensa procesal, exigiendo la adopción urgente de un estatuto de Debido Proceso Tecnológico inspirado en estándares comparados de la Unión Europea y Estados Unidos.

Por consiguiente, el objetivo de esta investigación consiste en evaluar la suficiencia del marco normativo penal peruano frente a la evidencia digital algorítmica y diseñar estrategias jurídicas para su admisión constitucional.

Método

La presente investigación se fundamenta en un diseño cualitativo-propositivo que responde a la naturaleza dogmática del problema jurídico planteado. En este sentido, Huhta y Romppanen, (2023) proponen la comparación disciplinaria como enfoque metodológico innovador en la beca legal para examinar las capacidades del derecho en facilitar cambios societales radicales. Su marco teórico, basado en la obra de Tuori, identifica la naturaleza multicapa de los sistemas legales, normas superficiales, cultura legal y estructuras profundas, y destaca la paradoja inherente de sistemas jurídicos que resisten el cambio rápido mientras simultáneamente necesitan habilitarlo. La comparación disciplinaria involucra analizar similitudes y diferencias en elementos subsuperficiales, doctrinas, objetivos, configuraciones institucionales, competencias y becas, entre campos legales diversos, permitiendo identificar fricciones y sinergias para mejorar la comprensión del rol del derecho en transformaciones intersectoriales.

Metodológicamente, la investigación adopta un enfoque cualitativo, dogmático-jurídico y propositivo, empleando hermenéutica jurídica para el análisis de vacíos normativos y derecho comparado funcional para la importación de soluciones regulatorias. El corpus de análisis comprende la Constitución Política del Perú, el Código Procesal Penal, el Reglamento de Inteligencia Artificial de la Unión Europea, jurisprudencia relevante del Tribunal Constitucional y la Corte Suprema, y doctrina autorizada en la materia.

En esta línea argumental, Pradi y Loriatti, (2023) trazan la evolución metodológica del derecho comparado desde enfoques positivistas del siglo XX temprano, centrados en fuentes formales y diferencias jurisdiccionales, hacia perspectivas dinámico-culturales que incorporan el enfoque factual y la teoría de formantes legales desarrollada por Schlesinger y Sacco. Esta metodología enfatiza la ley en acción y el pluralismo legal, proporcionando herramientas necesarias para analizar adaptaciones a contextos transnacionales. En el contexto de globalización, el derecho comparado sirve funciones duales: armonizar ordenamientos jurídicos identificando similitudes y fomentando convergencia, y diseccionar críticamente reglas globales uniformes para respetar diversidad contextual, promoviendo pluralismo sobre aproximaciones de ley black-letter.

Complementariamente, Kostruba et al., (2023) examinan la esencia conceptual de las lagunas legales como defectos sistémicos en ordenamientos jurídicos, definidas como la ausencia completa o parcial de provisiones legales necesarias para regular relaciones públicas dentro del ámbito de influencia jurídica. Su clasificación tipológica distingue lagunas por criterios temporales (primarias/secundarias), exhaustividad (completas/incompletas) y superabilidad (superables/insuperables), enfatizando la naturaleza inevitable de las lagunas debido al desarrollo dinámico de relaciones sociales y limitaciones legislativas. La doctrina legal desempeña un rol crucial en identificar, eliminar y superar lagunas mediante analogías de ley y estatuto, habilitando el uso de herramientas analógicas para la resolución de vacíos normativos.

El corpus de análisis comprende fuentes primarias y secundarias estratégicamente seleccionadas. Las fuentes primarias incluyen la Constitución Política del Perú de 1993 con sus reformas hasta 2021, particularmente el artículo 139 sobre observancia del debido proceso y tutela jurisdiccional; el Decreto Legislativo N° 957 que promulga el Nuevo

Código Procesal Penal de 2004, especialmente los artículos sobre prueba (Título IV, Arts. 155-199) y medidas coercitivas (Título V, Arts. 252-285); y el Regulation (EU) 2024/1689 del Parlamento Europeo sobre inteligencia artificial (AI Act). Las fuentes secundarias abarcan jurisprudencia relevante del Tribunal Constitucional y la Corte Suprema de Justicia, incluyendo las Casaciones N° 1675-2021 Lima y N° 1492-2017 Puno, y el Recurso de Nulidad N° 11-2024 Lima, junto con doctrina autorizada especializada en derecho procesal penal y tecnología.

La operacionalización de variables jurídicas se estructura mediante la siguiente matriz metodológica en la Tabla 1:

Tabla 1. *Matriz de Operacionalización de Variables Jurídicas*

Variable de Estudio	Dimensión	Indicador Jurídico-Empírico	Técnica de Validación
Necesidad Operativa	Eficiencia en la persecución penal	Brecha de velocidad (Tiempo de comisión vs. Tiempo de investigación)	Análisis Documental Comparado (Informes Fiscalía vs. Tipología Criminal)
Insuficiencia Normativa	Principio de Legalidad Procesal	Existencia de "Vacíos de Regulación" para evidencia algorítmica	Test de Subsunción Fallida (Intentar aplicar normas actuales a casos de IA)
Riesgo Constitucional	Garantías del Debido Proceso	Opacidad del algoritmo ("Caja Negra") vs. Derecho de Defensa	Juicio de Ponderación y Test de Constitucionalidad

La técnica de validación mediante Test de Subsunción Fallida constituye el instrumento metodológico central para demostrar la existencia de lagunas normativas. Este test consiste en someter artículos específicos del Código Procesal Penal a escenarios hipotéticos pero reales de aplicación de inteligencia artificial, documentando sistemáticamente las situaciones en las cuales la norma se fractura o resulta inaplicable. El Juicio de Ponderación y Test de Constitucionalidad permite evaluar la tensión entre la eficiencia investigativa y las garantías procesales fundamentales, aplicando el principio de proporcionalidad en sus tres subprincipios: idoneidad, necesidad y proporcionalidad stricto sensu.

Resultados

Diagnóstico de la Disfuncionalidad Operativa

El análisis comparativo de capacidades operativas entre las estructuras de crimen organizado contemporáneo y el sistema procesal penal tradicional peruano revela una asimetría tecnológica que compromete estructuralmente la eficacia de la persecución penal. Esta disparidad se manifiesta en múltiples dimensiones que abarcan desde la velocidad de ejecución delictiva hasta la sofisticación de los instrumentos empleados para evadir la detección y el procesamiento judicial.

Tabla 2. *Análisis comparativo de capacidades operativas: crimen organizado 4.0 vs. sistema penal tradicional*

Tipología / Acción Criminal (Tecnología Empleada)	Respuesta Estatal Actual (Método Análogo / Tradicional)	Resultado Procesal (Consecuencia de la Asimetría)
Lavado de Activos vía criptoactivos: transferencias transfronterizas instantáneas, descentralizadas y pseudoanónimas (blockchain).	Cooperación internacional clásica: solicitudes de asistencia judicial (carta rogatoria) y oficios a la banca tradicional que demoran meses.	Pérdida de trazabilidad: los activos desaparecen o se atomizan antes de que el fiscal obtenga la orden de incautación. Impunidad fáctica.
Comunicaciones encriptadas: uso de redes cerradas, apps con cifrado E2E (Signal, Telegram, redes propietarias) y autodestrucción de mensajes.	Intervención telefónica convencional: levantamiento del secreto de las comunicaciones (Art. 230 CPP) enfocado en líneas telefónicas y SMS; ineficaz ante cifrado de datos.	Ceguera investigativa: obtención de metadatos irrelevantes sin acceso al contenido; falta de elemento de convicción fuerte.
Big Data delictivo: estructuras criminales que generan terabytes de información (contabilidad digital, miles de correos, chats, imágenes).	Análisis humano-manual: fiscales y peritos revisando expediente por expediente o PDF por PDF, sin software de minería de datos o IA de PLN.	Colapso por sobrecarga: prescripción de la acción penal por imposibilidad material de procesar la evidencia en los plazos legales.
Suplantación de identidad (Deepfakes): IA generativa crea audios/videos falsos para estafar o incriminar/exculpar.	Peritaje forense tradicional: análisis fonético o de imagen estándar, muchas veces sin herramientas para detectar síntesis algorítmica de última generación.	Error judicial (falsos positivos): alto riesgo de admitir prueba espuria o fabricada, contaminando el razonamiento judicial.

Nota: *Elaboración propia basada en informes de cibercriminalidad (Diviac / Ministerio Público) y análisis de la fenomenología delictiva actual.*

Los hallazgos evidencian que la velocidad de comisión delictiva mediante tecnologías emergentes supera exponencialmente los tiempos de respuesta del sistema procesal tradicional. En el lavado de activos mediante criptomonedas, las transferencias se ejecutan en segundos a través de redes blockchain descentralizadas, mientras que los mecanismos de cooperación judicial internacional requieren meses para materializar órdenes de incautación, generando ventanas temporales que permiten la atomización y dispersión de activos ilícitos.

Test de Estrés Normativo del Código Procesal Penal

La aplicación del test de subsunción fallida a artículos específicos del Código Procesal Penal demuestra la existencia de lagunas normativas estructurales que impiden el procesamiento constitucional de evidencia generada por sistemas de inteligencia artificial. Este análisis revela deficiencias sistémicas que comprometen tanto la eficacia investigativa como las garantías procesales fundamentales.

Tabla 3. *Test de estrés normativo (gap analysis)*

Tecnología Emergente (Herramienta de IA)	Referencia Normativa (CPP 2004 / Constitución)	Deficiencia Identificada (El Vacío o Laguna)	Impacto en Derechos Fundamentales (Riesgo Constitucional)
Algoritmos de predicción del delito (policía predictiva): uso de datos históricos para estimar probabilidad de comisión de delitos o reincidencia.	Art. II Título Preliminar CPP: presunción de inocencia. Art. 158 CPP: valoración de la prueba.	Ausencia de regulación sobre evidencia probabilística: el CPP exige hechos, no probabilidades estadísticas; no hay estándar para validar la tasa de acierto del algoritmo.	Determinismo tecnológico y sesgo: riesgo de vulnerar la presunción de inocencia al valorar peligrosidad algorítmica y no hechos. Discriminación automatizada.
Reconocimiento facial automatizado en espacios públicos: vigilancia masiva en tiempo real para ubicar requisitoriados.	Art. 207 CPP: vigilancia. Art. 2 inc. 10 Const.: secreto e inviolabilidad de comunicaciones/ documentos privados.	Falta del principio de proporcionalidad digital: la norma regula vigilancia focalizada (a una persona), no la vigilancia indiscriminada sobre toda la ciudadanía.	Vulneración del derecho a la privacidad e intimidad: convierte a la población en sospechosa permanente sin mandato judicial específico (pesca probatoria masiva).
IA de caja negra (deep learning): sistemas que arrojan conclusiones (ej. es culpable) con procesos internos ininteligibles.	Art. 139 inc. 14 Const.: derecho de defensa. Art. 378 CPP: examen de testigos y peritos (contradictorio).	Imposibilidad de contrainterrogatorio: no se puede interrogar al algoritmo para entender su razonamiento; funcionamiento a menudo secreto comercial.	Indefensión material: el imputado no puede defenderse de una prueba que no entiende, violando el debido proceso.
Extracción forense de datos con IA: software que selecciona automáticamente qué chats/fotos son relevantes.	Art. 184 CPP: incautación y cadena de custodia.	Delegación de la función jurisdiccional: la selección probatoria la realiza la máquina, sin auditoría sobre lo descartado (posible omisión de prueba de descargo).	Afectación a la tutela jurisdiccional efectiva: el control de pertinencia probatoria pasa de manos humanas a parámetros opacos de software privado.

Nota: *Elaboración propia a partir del análisis dogmático del Decreto Legislativo N.º 957 (Código Procesal Penal) y estándares internacionales de derechos humanos.*

El análisis demuestra que el Código Procesal Penal de 2004, estructurado para el procesamiento de evidencia física y testimonial tradicional, experimenta fracturas sistemáticas al aplicarse a tecnologías de inteligencia artificial. La ausencia de regulación específica para evidencia probabilística genera una aporía fundamental: mientras el CPP exige certeza sobre hechos concretos, los algoritmos predictivos operan mediante probabilidades estadísticas cuya validación carece de estándares normativos.

Hallazgos del Derecho Comparado

El análisis del derecho comparado revela aproximaciones diferenciadas para abordar la integración de inteligencia artificial en sistemas de justicia penal. El Reglamento (UE) 2024/1689 del Parlamento Europeo (AI Act) establece un marco comprehensivo basado en clasificación de riesgos, prohibiendo sistemas de IA que presenten riesgos inaceptables y sometiendo aplicaciones de alto riesgo en contextos de justicia penal a requisitos estrictos de transparencia, precisión y supervisión humana. Particularmente relevante resulta el artículo 26, que exige evaluaciones de conformidad antes del despliegue, y el artículo 13, que establece obligaciones de transparencia para sistemas que interactúan con

personas naturales.

En contraste, el precedente estadounidense State v. Loomis (Supreme Court of Wisconsin, 2016) ilustra las tensiones entre eficiencia judicial y garantías procesales. La Corte Suprema de Wisconsin permitió el uso de la herramienta COMPAS para evaluación de riesgo en sentencia, condicionándolo a que los jueces no dependan únicamente de las puntuaciones algorítmicas y adviertan explícitamente sobre las limitaciones de la herramienta. Sin embargo, la decisión generó controversias significativas respecto a la opacidad del algoritmo y su potencial para perpetuar sesgos sistémicos, evidenciando la necesidad de marcos regulatorios más robustos.

Discusión

Del Debido Proceso al Debido Proceso Tecnológico

La evolución conceptual del debido proceso en la era de la inteligencia artificial exige una reconceptualización dogmática que preserve las garantías fundamentales mientras habilite la incorporación de herramientas tecnológicas indispensables para la persecución del crimen organizado contemporáneo. En este sentido, Garrett y Rudin, (2023) establecen una distinción crítica entre sistemas de IA black box y glass box, argumentando que la presunción de mayor precisión de los sistemas complejos e interpretables resulta infundada empíricamente. Su investigación demuestra que sistemas de IA glass box, diseñados para ser completamente interpretables, pueden alcanzar precisión igual o superior a sistemas opacos, mientras permiten la detección de errores en datos propensos a sesgos que reflejan disparidades raciales y socioeconómicas. El caso paradigmático de COMPAS, que reclama utilizar 137 inputs pero es superado por modelos simples de 2-3 variables, ilustra cómo la opacidad algorítmica puede ocultar errores en datos deficientes, con tasas de información faltante del 45% en género y 35% en raza en Virginia durante 2021.

En esta línea argumentativa, Koellner, (2025) examina la integración de IA en cortes hiper-especializadas, identificando riesgos sistémicos de black box justice donde procesos opacos contaminan determinaciones judiciales. Particularmente en actas criminales, las evaluaciones de riesgo algorítmico influencian decisiones de fianza y sentencia sin mecanismos efectivos de explainabilidad, generando preocupaciones fundamentales sobre la erosión del vigilante humano. Su análisis comparado de jurisdicciones, Estados Unidos, Unión Europea y China, revela brechas regulatorias significativas y la necesidad imperiosa de estándares internacionales para herramientas forenses basadas en IA, transparencia en decisiones algorítmicas y entrenamiento interdisciplinario para operadores jurídicos.

La evidencia empírica más contundente proviene del estudio de Shevchuk et al., (2025) sobre la implementación de IA en actas criminales en Ucrania. Su investigación, basada en encuestas a 64 profesionales de justicia y análisis de decisiones judiciales, revela que el 73.5% de las defensas desafían evidencia obtenida mediante IA, con una tasa de éxito del 41.2%. Los casos admisibles son tratados como opiniones expertas en el 83.7% de los supuestos, evidenciando la ausencia de categorización jurídica específica para evidencia algorítmica. Las encuestas identifican problemas críticos: falta de marco regulatorio (4.72/5), interpretabilidad deficiente de resultados de IA (4.54/5) y dificultades de

verificación (4.48/5), mientras que el 86.4% de respondientes reporta análisis limitado de evidencia contextual y el 84.1% señala desafíos en verificación algorítmica.

Complementariamente, Palmiotto, (2020) analiza la regulación de opacidad algorítmica en actas criminales desde la perspectiva del derecho europeo, identificando que la tendencia preocupante hacia el secreto y la opacidad impide la comprensión de cómo se genera evidencia específica. Su análisis de casos demuestra que el software puede exhibir sesgos significativos sin presumirse fiable, citando ejemplos como malware Exodus para hacking, herramientas forenses EnCase que alteran marcas de tiempo, y software de análisis de ADN STRmix con errores documentados. La ausencia de conocimiento en algoritmos compromete el derecho a confrontación bajo el Artículo 6§3(d) de la ECHR, requiriendo que los acusados puedan desafiar la probidad, credibilidad, veracidad y fiabilidad de evidencia, derechos que se tornan ilusorios ante sistemas opacos.

No obstante, la solidez de estos argumentos, cabe advertir que la interpretación aquí propuesta resuelve la antinomia identificada mediante la articulación de un estatuto de Debido Proceso Tecnológico que integre tres pilares fundamentales: transparencia algorítmica, auditabilidad ex post y proporcionalidad digital. Si el Estado emplea IA para generar evidencia incriminatoria, el ciudadano debe tener el derecho correlativo de auditar esa IA, examinar sus procesos de decisión y contradecir sus conclusiones mediante peritaje independiente. Sin esta garantía, toda prueba algorítmica podría ser declarada ilícita bajo la doctrina del fruto del árbol envenenado, generando un escenario paradójico donde la necesidad operativa de enfrentar el crimen organizado se torna jurídicamente inviable.

Oportunidades: La Eficiencia con Garantías

Contrariamente a la percepción prevalente de que las garantías procesales entorpecen la eficiencia judicial, la implementación de un marco regulatorio claro para IA en justicia penal potenciaría tanto la eficacia investigativa como la seguridad jurídica de los operadores. En esta línea, Krištofík, (2025) examina el bias en sistemas de toma de decisiones basados en IA, demostrando cómo estos sistemas replican y amplifican sesgos societales preexistentes derivados de datos de entrenamiento que incorporan decisiones judiciales históricamente discriminatorias. Su comparación con el marco de la Corte Europea de Derechos Humanos para bias judicial bajo el Artículo 6 de la ECHR sugiere que tests existentes para imparcialidad pueden adaptarse mutatis mutandis a sistemas de IA mediante auditorías iterativas y monitoreo continuo. La propuesta de remedios como mejoramiento de calidad de datos, transparencia operacional y vigilancia humana efectivo no constituye obstáculos a la eficiencia, sino precondiciones para la legitimidad y sustentabilidad de sistemas automatizados.

La investigación de Glass, (2023) sobre algoritmos en justicia criminal refuerza esta perspectiva al demostrar cómo sistemas diseñados para reducir sesgos pueden perpetuarlos o amplificarlos debido a inputs de datos defectuosos y procesos de diseño excluyentes. Su identificación del problema de input de tres puntas, adopción opaca sin participación comunitaria, exclusión de grupos marginados del desarrollo, y ausencia de feedback público significativo, evidencia que algoritmos construidos sobre fuentes sesgadas como registros policiales y judiciales marginan sistemáticamente a comunidades afectadas. Los datos son contundentes: individuos afroamericanos e indígenas experimentan tasas de encarcelamiento casi cuatro veces superiores a blancos (1,186 y

1,004 por 100,000 respectivamente, comparado con 222 para blancos en 2021), mientras que un sistema específico etiquetó erróneamente el doble de individuos negros no reincidentes como alto riesgo comparado con blancos.

Además, Rodà, (2025) proporciona un análisis detallado del caso COMPAS que ilustra la complejidad multidimensional de justicia en aplicaciones de IA. Su examen de la controversia iniciada por ProPublica en 2016, que alegaba bias racial, y la defensa de Northpointe sobre la equidad de la herramienta, demuestra que no existe una métrica única de justicia debido a la "imposibilidad de justicia " matemática. Los alegatos de ProPublica sobre bias racial mediante False Positive Rate más elevado para afroamericanos (44.85% vs. 23.45% para caucásicos) son criticados como fallacios, dado que FPR aumenta con tasas de supervivencia más bajas en grupos desventajados, no necesariamente indicando discriminación algorítmica. Paradójicamente, Positive Predictive Value muestra COMPAS ligeramente más severo hacia caucásicos (0.59 vs. 0.63 para afroamericanos), evidenciando la necesidad de marcos comprehensivos que consideren múltiples métricas simultáneamente.

Una consecuencia práctica de estas consideraciones es que un marco regulatorio robusto proporcionaría seguridad jurídica a la Policía Nacional y el Ministerio Público para emplear tecnología avanzada sin temor a nulidades procesales posteriores. La ausencia de regulación genera incertidumbre que desincentiva la adopción de herramientas necesarias para contrarrestar el crimen organizado, mientras que estándares claros de transparencia, auditabilidad y proporcionalidad habilitarían la innovación tecnológica dentro de parámetros constitucionalmente seguros.

Estrategias de Reforma Legislativa

La experiencia comparada proporciona marcos conceptuales valiosos para el diseño de reformas legislativas en el contexto peruano. A propósito, Fernando y Anditya, (2024) analizan la implementación de jueces de IA en sistemas diversos, destacando aplicaciones como el robot Xiaofa en China para asesoramiento legal y detección de errores, y sistemas en Estonia para adjudicación de reclamaciones menores. Estas experiencias demuestran que la IA puede reducir errores judiciales, acelerar actas y minimizar sesgos humanos en casos rutinarios, empero revelan riesgos significativos de bias algorítmico derivado de datos históricos y procesos black box que carecen de Interpretabilidad. Su análisis enfatiza que la implementación debe respetar contextos culturales, legales y sociales específicos, requiriendo vigilancia humano para mantener integridad sistémica y marcos éticos robustos para prevenir discriminación automatizada.

No obstante, Hendrickx, (2025) identifica una paradoja de eficiencia en IA judicial que constituye una advertencia crucial para reformadores legislativos. Su análisis del despliegue de sistemas como transcripción automática y subtitulado en vivo en cortes eslovenas durante octubre de 2025 revela que tecnologías promovidas para acelerar procesos pueden introducir ineficiencias sistémicas. Los desafíos incluyen limitaciones de precisión que requieren correcciones manuales extensivas, opacidad de modelos que incrementa cargas de revisión judicial, erosión de expertise humana mediante over-reliance y offloading cognitivo, y potencial incremento de apelaciones debido a errores y pérdida percibida de agencia judicial. Esta paradoja subraya que las ganancias de velocidad pueden ser neutralizadas por costos de validación cuando los datos de entrenamiento son inadecuados o no representativos.

Basándose en estos hallazgos, las estrategias de reforma legislativa para el Perú deben articularse en tres ejes fundamentales. Primero, la modificación del Código Procesal Penal para incluir una categoría específica de Prueba Algorítmica que establezca requisitos de admisibilidad, valoración y contradicción. Esta modificación debe incorporar el principio de explicabilidad algorítmica, exigiendo que todo sistema de IA empleado en proceedings criminales proporcione justificaciones comprensibles para sus conclusiones, habilitando el ejercicio efectivo del derecho de defensa.

Segundo, la creación de un estándar de Auditabilidad Tecnológica que prohíba el uso de sistemas de caja negra en contextos donde se genere evidencia incriminatoria. Este estándar debe exigir que algoritmos empleados en justicia penal sean transparentes, reproducibles y sujetos a validación independiente, con obligación de revelar datasets de entrenamiento, métricas de precisión y procedimientos de calibración.

Tercero, el establecimiento de un Protocolo de Cadena de Custodia Digital que garantice la integridad, autenticidad y trazabilidad de evidencia generada o procesada mediante IA. Este protocolo debe incluir estándares criptográficos para preservación de metadatos, procedimientos de verificación de integridad y mecanismos de auditoría forense que permitan reconstruir el proceso completo de generación y análisis de evidencia digital.

Adicionalmente, se propone la creación de una Comisión Nacional de Ética en IA Judicial, integrada por juristas, tecnólogos y representantes de la sociedad civil, encargada de supervisar la implementación de sistemas algorítmicos, evaluar su impacto en derechos fundamentales y proponer actualizaciones regulatorias ante desarrollos tecnológicos emergentes.

Conclusiones

La presente investigación confirma la tesis central propuesta: la incorporación de inteligencia artificial en la persecución del crimen organizado en Perú constituye una necesidad operativa ineludible debido a la asimetría tecnológica documentada entre estructuras delictivas que emplean herramientas 4.0 y sistemas de justicia anclados en paradigmas tradicionales. Sin embargo, su implementación bajo el actual Código Procesal Penal de 2004 genera un escenario crítico de inconstitucionalidad por omisión que vulnera sistemáticamente el derecho a la prueba y la defensa procesal, exigiendo reformas legislativas urgentes.

El test de subsunción aplicado a artículos específicos del Código Procesal Penal demuestra lagunas estructurales insalvables sin intervención legislativa. La ausencia de regulación para evidencia probabilística, la falta de principios de proporcionalidad digital para vigilancia masiva, la imposibilidad de contrainterrogatorio ante sistemas de "caja negra", y la delegación no regulada de funciones jurisdiccionales a algoritmos privados configuran aporías normativas que tornan constitucionalmente inviable el uso de IA bajo el marco actual.

La experiencia comparada de la Unión Europea, mediante el AI Act, y casos precedentes como State v. Loomis en Estados Unidos, evidencian que la integración exitosa de IA en justicia penal requiere marcos regulatorios comprehensivos que balanceen eficiencia operativa con garantías procesales fundamentales. La ausencia de tales marcos no solo compromete derechos individuales, sino que genera inseguridad jurídica que desincentiva

la adopción de tecnologías necesarias para enfrentar el crimen organizado contemporáneo.

Por consiguiente, la lucha eficaz contra el crimen organizado en Perú exige una reingeniería procesal inmediata que trascienda modificaciones puntuales para articular un estatuto integral de Debido Proceso Tecnológico. Este estatuto debe incorporar principios de transparencia algorítmica, auditabilidad ex post, proporcionalidad digital y explicabilidad sistemática, garantizando que la inevitable digitalización de la persecución penal preserve los derechos fundamentales mientras potencia la capacidad investigativa del Estado. La implementación de estas reformas no constituye un obstáculo a la eficiencia judicial, sino una precondición para la legitimidad y sustentabilidad de la justicia penal en la era digital.

Acerca de

Contribución del autor: La autora contribuyó a la conceptualización del estudio, al desarrollo metodológico, al análisis e interpretación de los datos, a la redacción del manuscrito y a la revisión crítica de su contenido intelectual.

Financiamiento: La autora declara que no recibió financiamiento para esta investigación.

Certificación ética: El protocolo del presente estudio fue sometido a revisión y aprobado por el Comité de Ética en Investigación de la Universidad, en cumplimiento de los principios éticos y normativas institucionales aplicables.

Referencias

Aliaga, C., Ravello, A., Sares, D., and Leon, M. (2025). Would you Steal me a Like? Undercover Operations in Digital Environments within the Peruvian National Police. *CEUR Workshop Proceedings, 156–164*. https://ceur-ws.org/Vol-4055/icaiw_aiesd_4.pdf

Cefeidas Group. (2023). Navigating Artificial Intelligence: Trends and debates in Latin America. *Cefeidas Group*. https://www.cefeidas.com/2023/09/14/cefeidas-group-navigating-artificial-intelligence-trends-and-debates-in-latin-america/

CEJA. (2024). *Plan de acción 2024*. Justice Studies Center of the Americas. https://cejamericas.org/wp-content/uploads/2024/03/JSCA-Workplan-2024-English_ok.pdf

DHS. (2024). *Impact of Artificial Intelligence on Criminal and Illicit Activities*. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf

Díaz, F., Cerna, N., and Liza, R. (2025). Artificial Intelligence and Crime in Latin America: A Multilingual Bibliometric Review (2010–2025). *Information, 16*(11). https://doi.org/10.3390/info16111001

Dote, J. P., and Espinosa, M. T. J. (2025). Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies. *Latin American Journal of Central Banking*, 100194. https://doi.org/10.1016/j.latcb.2025.100194

Europol. (2025). The changing DNA of serious and organised crime. European Union Agency for Law Enforcement Cooperation. https://doi.org/10.2813/0758057

Fair Trials. (2024). Artificial intelligence in public security and criminal justice systems in Latin America. Due process-based analysis. *fairtrials.org*. https://www.fairtrials.org/app/uploads/2024/08/Artificial-intelligence-in-public-security-and-criminal-justice-systems-in-Latin-America.pdf

Fernando, Z. J., & Anditya, A. W. (2024). AI on The Bench: The Future of Judicial Systems in The Age of Artificial Intelligence. *Jurnal Hukum Dan Peradilan*, *13*(3), 523-550. https://doi.org/10.25216/jhp.13.3.2024.523-550

Garrett, B. L., & Rudin, C. (2023). The Right to a Glass Box. *Cornell Law Review*, *109*(561), 563-626. https://publications.lawschool.cornell.edu/lawreview/wp-content/uploads/sites/2/2024/04/Garrett-Rudin-final.pdf

Glass, M. (2023). Algorithms Were Supposed to Reduce Bias in Criminal Justice—Do They? *Boston University*. https://www.bu.edu/articles/2023/do-algorithms-reduce-bias-in-criminal-justice/

Hendrickx, V. (2025). The Efficiency Paradox of Judicial AI. *MediaLaws*. https://www.medialaws.eu/the-efficiency-paradox-of-judicial-ai/

Huhta, K., & Romppanen, S. (2023). Comparing Legal Disciplines as an Approach to Understanding the Role of Law in Decarbonizing Societies. *Transnational Environmental Law*, *12*(3), 649-670. https://doi.org/10.1017/S204710252300016X

Koellner, E. (2025). Black Box Justice? Legal Evidence, Digital Democracy, and the Risks of AI in Hyper-Specialized Courts (SSRN Scholarly Paper No. 5215622). *Social Science Research Network*. https://doi.org/10.2139/ssrn.5215622

Kostruba, A., Haliantych, M., Iskra, S., & Dryshliuk, A. (2023). Legal Gaps: Concept, Content, Problems of the Role of Legal Doctrine in Overcoming them. *Statute Law Review*, *44*(2), hmac016. https://doi.org/10.1093/slr/hmac016

Krištofík, A. (2025). *Bias in AI (Supported) Decision Making: Old Problems, New Technologies*. *16*(1). https://www.muni.cz/en/research/publications/2493618

Ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país 2 (2023). https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/4565760-31814

Ley N.° 32082, Ley que Dispone la Implementación Progresiva de la Transformación Digital en las Oficinas Consulares del Perú 2 (2024). https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/5723037-32082

Palmiotto, F. (2020). *Regulating Algorithmic Opacity in Criminal Proceedings: An opportunity for the EU Legislator?* [Faculty of Law Working Paper Series]. Maastricht Faculty of Law Working Paper. https://www.maastrichtuniversity.nl/sites/default/files/2023-03/palmiotto_-_maastricht_working_paper_series_-_regulating_algorithmic_opacity_copy.pdf

Pradi, A., & Loriatti, E. (2023). Comparative Law and Methodology Between Homogeneity and Complexity. *Global Jurist*, *23*(3), 237-241. https://doi.org/10.1515/gj-2023-0136

Rodà, A. (2025). The COMPAS case: An educational journey for explaining fairness in AI-based applications. *AIMMES 2025*, 1-9. https://ceur-ws.org/Vol-3961/paper4.pdf

Shevchuk, V., Morozova, T., Chornyi, H., Nehrebetskyi, V., & Slobodeniuk, I. (2025). Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues. *International Annals of Criminology*, *63*(3), 572-590. https://doi.org/10.1017/cri.2025.10090

Smart, S. (2025). *Analyzing a Charter of Rights and Institutions to Tackle Surveillance Capitalism in the Era of Artificial Intelligence: The Case of Latin America*. Carr-Ryan Center Discussion Paper No. 2025-06. https://www.hks.harvard.edu/sites/default/files/2025-10/25_Smart_Sebastian.pdf

Supreme Court of Wisconsin. (2016). *State v. Loomis*. Justia Law. https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html

UNODC. (2024). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape* [Technical Policy Brief]. Copyright © 2024, United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf