

Artículo de Investigación DOI: <https://doi.org/10.61154/holopraxis.v10i1.4394>

Responsabilidad de crímenes cometidos por la inteligencia artificial bajo supervisión humana

Liability for crimes committed by artificial intelligence under human supervision

Isabel Alejandra Torres-Montalvo ^a, José Ignacio Guevara-Dávalos ^b, Bartolomé Gil-Osuna ^c

^a Pontificia Universidad Católica del Ecuador, Ibarra, Imbabura, Ecuador, Email: iatorresm@pucesi.edu.ec, Orcid: <https://orcid.org/0009-0002-7301-4182>

^b Pontificia Universidad Católica del Ecuador, Ibarra, Imbabura, Ecuador, Email: jiguevara@pucesi.edu.ec, Orcid: <https://orcid.org/0009-0003-6737-6344>

^c Pontificia Universidad Católica del Ecuador, Ibarra. Imbabura, Ecuador, Email: bagil2@pucesi.edu.ec Orcid: <https://orcid.org/0000-0003-0128-2030>

Recibido: 27 de agosto de 2025

Aprobado: 3 de noviembre de 2025

RESUMEN

La tecnología digital se ha convertido en el potencial indudable de transformación de economías, gobiernos y sociedades civiles de manera acelerada y profunda, incidiendo en la mayoría de los aspectos del desarrollo de las personas, direccionada a construir sociedades digitales inclusivas, éticas y sostenibles con enfoque basado en el respeto y garantía de los derechos humanos y abogando por una metamorfosis digital equitativa y centrada en las personas. En este contexto germinó la iniciativa de este estudio científico que tuvo como objetivo general determinar la responsabilidad de crímenes cometidos por la inteligencia artificial bajo supervisión humana en la legislación penal ecuatoriana en aquellos casos que se afecte la integridad personal, a los fines de garantizar la protección integral de los derechos individuales. Se siguió un proceso metodológico asentado en enfoque cualitativo, nivel de profundidad descriptivo y uso de métodos socio-jurídico, normativista y analítico-sintético para precisar la viabilidad de atribuir responsabilidad

penal a los desarrolladores, operadores/supervisores de sistemas de IA. Bajo la revisión documental de normativa internacional/nacional aplicable a la responsabilidad penal en delitos tecnológicos y de la doctrina penal que ha abordado la atribución de responsabilidad en delitos cometidos mediante IA, se obtuvo resultados que revelan que Ecuador carece de un marco regulatorio específico que permita establecer la responsabilidad penal en casos donde la IA cause daños que atentar contra los derechos fundamentales. Se advierte que, la legislación vigente evidencia necesidad de actualizar el ordenamiento jurídico para incorporar disposiciones que tipifiquen nuevas conductas penalmente relevantes derivadas del uso de esta tecnología.

Descriptores: Responsabilidad jurídica, crímenes informáticos, inteligencia artificial, derecho de la informática, derechos humanos. (Tesauro UNESCO).

ABSTRACT

Digital technology has emerged as a transformative force, instigating rapid and significant changes across economies, governmental structures, and civil societies, thereby impacting various facets of human development. The central objective of this transformation is the establishment of inclusive, ethical, and sustainable digital societies, grounded in the respect for and protection of human rights, while promoting an equitable and people-centered digital evolution. It is within this context that the impetus for this scientific inquiry was generated, with the overarching aim of identifying the accountability for offenses perpetrated by artificial intelligence under human oversight within the framework of Ecuadorian criminal law, particularly in instances that affect personal integrity. To achieve this aim, a rigorous methodological approach was implemented, encompassing a qualitative framework, a descriptive level of analysis, and the utilization of socio-legal, normative, and analytical-synthetic methods. This methodology facilitated an exploration into the plausibility of ascribing criminal liability to the developers and operators/supervisors of AI systems. A comprehensive review of both international and national regulations pertinent to criminal liability in technology-related offenses, alongside an examination of criminal doctrine related to the attribution of liability for crimes involving AI, was conducted. This analysis illuminated a significant gap within the Ecuadorian legal framework, revealing a lack of specific provisions for establishing criminal liability in instances where AI inflicts harm that contravenes fundamental rights. Notably, the existing legislative landscape underscores the imperative of reforming the legal system to integrate provisions that categorize emergent criminally relevant behaviors associated with the utilization of this technology.

Descriptors: Legal liability, cybercrime, artificial intelligence, computer law, human rights. (Thesaurus UNESCO)

INTRODUCCIÓN

Los inicios conceptuales de la inteligencia artificial (en adelante IA) surgen en la década de los 50 del siglo XX, al lado de diversas áreas del conocimiento desde la filosofía, la psicología o biología hasta la computación, las matemáticas, el álgebra, entre otras.

Inicialmente este concepto se vincula a la realización de actos que se generan con cierta inteligencia debido a que requieren cierto grado de razonamiento y comprensión como son la generación de herramientas y de algunos programas que puedan desarrollarla de manera adecuada. Esta amalgama multidisciplinar de tecnologías y de nociones ha hecho complejo el poseer o adherirse a un único concepto claro, preciso y definitivo de lo que debe entenderse por IA.

Por lo que se hace inminente *prima facie* ostentar una definición, desde una *perspectiva jurídica*, que ofrezca elementos confiables para el estudio de la responsabilidad penal de este fenómeno digital, en vez de contar con una definición técnica y estructurada que poco aportaría. También es necesario resaltar que la IA “tiene el potencial de brindar numerosos *beneficios* al campo del derecho (...): Automatización de tareas legales repetitivas; análisis de grandes cantidades de datos; mejora de la precisión y consistencia; optimización de la estrategia legal; mejora la accesibilidad y eficacia de la justicia” (Prigiani, 2023, p. 2). Por lo que esta eclosión de utilización de IA en diversos campos de la vida del ser humano, en particular, el *campus* del derecho implica, de forma unívoca, serias dificultades en el abordaje de problemas derivados de su uso en los derechos fundamentales de las personas.

Los estudios científicos al respecto están apenas aflorando, como el de Vall Prieto (2022), quien asegura que ya hay numerosos ejemplos que evidencian que el uso de la IA está aparejado con un impacto negativo en los derechos fundamentales, reconocidos en las diversas Constituciones a nivel global, “la vida se ve afectada por los vehículos autónomos, los sistemas crediticios discriminan a sectores poblacionales, los sistemas de reconocimiento facial discriminan a negros, la utilización de datos afecta a la privacidad, etc.” (p. 4). O como agrega García Falconí y Barona Pazmiño (2024) “se evidencia que el uso de la IA en el proceso penal también plantea preocupaciones en cuanto a la privacidad y seguridad de datos, así como preguntas sobre cómo la IA afectaría la toma de decisiones judiciales” (p. 101). Esto ha dado lugar a que se inicien varios intentos para determinar *ipso iure* la responsabilidad que pueda derivarse del uso indebido de los sistemas inteligentes que están invadiendo el quehacer diario de los usuarios.

Estos intentos obedecen a que el derecho penal y criminal no debe mantener silencio o situarse al margen frente a la vulneración de los derechos fundamentales o afectación de bienes jurídicos por la práctica de las nuevas tecnologías. De ello puede derivarse que el espectro de derechos y garantías vulneradas sea excesivamente amplio debido a que el derecho es una ciencia dinámica que, por ser garantista, al decir de Ferrajoli (2007), se constituye “en ideología que busca limitar el poder y garantizar los derechos fundamentales” (p. 14). Conscientes de esta realidad jurídica y de la importancia del estudio de la responsabilidad penal del uso de la IA bajo supervisión humana se hizo un análisis centrado en el ciclo de vida de la IA, apoyado en una revisión documental de los aportes de la doctrina penal y de algunos trabajos que ha realizado la Comisión Europea al estudiar la responsabilidad penal, fundamentalmente: las guías éticas sobre inteligencia artificial del grupo de altos expertos y el Reglamento sobre la inteligencia artificial. Es inminente no olvidar, como arguye Laín Moyano (2021), “qué es lo que subyace detrás de la IA, que no sea otra cosa que, pese a quien pese, el ser humano. El algoritmo se retroalimenta y toma decisiones propias, pero no nace de la nada, sino de la voluntad de su autor” (p. 198).

El estudio de la responsabilidad penal de lo realizado por la IA tiene su razón de ser en la inopia de sistemas inteligentes relacionados con la administración de justicia en el Ecuador, lo que induce a que los derechos enunciados en la Constitución de la República del Ecuador (en adelante CRE) se diluyan paulatinamente frente a los avances del desarrollo digital, lo que genera, por vía de consecuencia, vulneración de los derechos y la subsecuente falta de responsabilidad penal. Si bien es cierto, el Código Orgánico Integral Penal (en adelante COIP) aborda ciertos delitos informáticos no explana, de manera específica, como asevera León Párraga (2024) la responsabilidad y sanción para aquellos casos en que la actuación de la IA genere daños y perjuicios.

De allí que, la capacidad de los sistemas inteligentes para tomar decisiones por sí mismos plantea un problema jurídico de vanguardia, aún sin resolverse: ¿Quién debe ser responsable penalmente cuando una IA incurra en un error que genere daños físicos o psicológicos comprometiendo la seguridad de las personas? Por lo que se planteó como objetivo de esta investigación determinar la responsabilidad de crímenes cometidos por la inteligencia artificial bajo supervisión humana en la legislación penal ecuatoriana en

aquellos casos que se afecte la integridad personal a los fines de garantizar la protección integral de los derechos individuales en la era digital.

MÉTODOS

A los fines de dar respuesta al objetivo planteado en la presente investigación se emplearon: el *método socio-jurídico* que permitió contextualizar la problemática dentro de la sociedad digital actual, analizando cómo la IA afecta derechos fundamentales y los debates jurídicos que surgen en torno a su regulación, con “una concepción interdisciplinaria apoyada en enfoques teóricos y metodológicos más plurales” como menciona Gómez 2024, (p. 12); el *método normativista*: se utilizó para examinar la normativa penal ecuatoriana e internacional aplicable al uso de IA y los principios rectores de la responsabilidad penal y; por último, el *método analítico-sintético*: facilitó el estudio crítico de textos normativos, doctrinales y jurisprudenciales, permitiendo una síntesis estructurada sobre la viabilidad de atribuir responsabilidad penal a los desarrolladores, operadores o supervisores de sistemas de IA.

En cuanto a las técnicas de investigación, se aplicó la *revisión documental*, mediante la cual se analizaron: *Normativa internacional y nacional*: Regulaciones de la Comisión Europea sobre inteligencia artificial, guías éticas del grupo de altos expertos en IA, y legislación latinoamericana y ecuatoriana aplicable a la responsabilidad penal en delitos tecnológicos; *doctrina penal*: estudios de autores especializados en derecho penal y tecnología, que han abordado la atribución de responsabilidad en delitos cometidos mediante IA.

Los instrumentos de investigación empleados fueron: *Fichas bibliográficas*, para sistematizar la información extraída de libros, artículos científicos y documentos normativos; *análisis de casos*, que permitió evaluar ejemplos prácticos de impacto de la IA en la vulneración de derechos fundamentales, con especial énfasis en casos donde se han planteado dilemas de responsabilidad penal. Esta metodología permitió un estudio detallado de los fundamentos jurídicos necesarios para delimitar el rol de la IA dentro del derecho penal y evaluar las posibles soluciones legislativas y doctrinales ante la responsabilidad por crímenes cometidos por sistemas inteligentes bajo supervisión

humana. Se aplicó una técnica de análisis crítico-interpretativo que permitió valorar comparativamente la normativa, la doctrina y los casos estudiados, identificando vacíos y criterios relevantes. Esta técnica facilitó la interpretación jurídica de los hallazgos para determinar la viabilidad de atribuir responsabilidad penal en crímenes cometidos por sistemas de IA bajo supervisión humana.

RESULTADOS

En este apartado se indagaron los antecedentes investigativos más relevantes de la doctrina, tanto nacional como internacional, que han expuesto sus trabajos en revistas indexadas de alto impacto, en repositorios y bibliotecas digitales relativos a la responsabilidad criminal de los sistemas inteligentes que por error en su programación inteligente devienen daños a las personas afectando sus derechos fundamentales. Como mencionan Loaiza Moreno, Soto, Hoyos Escaleras (2024) “la evolución de la IA ha abierto nuevas fronteras en la discusión sobre el crimen, no sólo como una herramienta para facilitar delitos, sino también como un posible agente que actúa de manera autónoma en la ejecución de crímenes” (p. 2160). Sin duda, el impacto de los sistemas de inteligencia en el derecho penal está latente y amerita una revisión documental detenida.

a.- Aproximación a una definición de inteligencia artificial en el ámbito jurídico

Este término —inteligencia artificial— fue por primera vez introducido por John McCarthy, informático norteamericano que en el año 1956 estableció una definición embrionaria que afirmaba que es “la ciencia y la ingeniería de crear máquinas inteligentes, especialmente, aquellas programadas con computación inteligente” (Loaiza Moreno et al, 2024, p. 2157). Definición que destaca el aspecto científico de la construcción de máquinas que pueden reproducir comportamientos inteligentes. Por su parte Miró Llinares (2018) patrocina una definición en la que considera que:

La IA no es más que un conjunto de sistemas informáticos avanzados que procesan datos, reconocen patrones y generan predicciones, pero sin alcanzar un nivel real de autonomía o conciencia propia. La inteligencia que poseen no es comparable a la humana, sino una reproducción de procesos matemáticos extremadamente complejos que imitan ciertos aspectos de la toma de decisiones.
(p. 91)

Con una óptica parecida el experto en tecnología Lasse Rouhiainen (2018) predica a la IA como “la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano” (p. 17). Con la experticia suficiente este autor sostiene que la IA emplea los algoritmos necesarios para desplegar máquinas o sistemas inteligentes con capacidad para aprender de su propia experiencia y desarrollar labores similares a las que puede realizar el ser humano. En seguimiento de una *definición* que incida en el *ámbito jurídico* se recurrió a la promovida —recientemente— por el grupo de expertos de alto nivel en inteligencia artificial de la Comisión Europea que redactaron las guías éticas para el uso fiable de la inteligencia artificial, en búsqueda de un concepto de IA, juntamente con el documento de 2021 del Parlamento Europeo y el Consejo, en su propuesta sobre regulación de la inteligencia artificial, que en su Art. 6, párrafo 1 define la IA como:

El *software*, con capacidad para generar, en relación con un conjunto concreto de objetivos definidos por seres humanos, resultados como contenidos, predicciones, recomendaciones o decisiones u otra información de salida que influyan en el entorno con el que interactúa el sistema, ya sea en una dimensión física o digital, en base a un conjunto de datos. (Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, 2021)

Como dice la exposición de motivos de esta propuesta: “redunda en interés de la Unión Europea preservar su liderazgo tecnológico y garantizar que los europeos puedan aprovechar nuevas tecnologías que se desarrollen y funciones de acuerdo con los valores, los derechos fundamentales y los principios de la UE” (Preámbulo, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, 2021).

La inteligencia artificial debe ser concebida como una herramienta al servicio de las personas y un motor de progreso social, cuyo propósito fundamental sea mejorar el bienestar humano. Por ello, las normativas que regulan su desarrollo y aplicación dentro del mercado del país, o aquellas que incidan en su población, deben priorizar un *enfoque*

centrado en el ser humano. Esto garantizará que su uso sea seguro, legal y respetuoso con los derechos fundamentales y en caso de vulneración de estos se estatuya la responsabilidad criminal adecuada.

Este marco regulador necesario, además de proteger los derechos y libertades individuales, debe fundamentarse en una comprensión clara del concepto de inteligencia artificial. Sin embargo, como se ha evidenciado en el análisis de diversas definiciones, la IA es un *fenómeno multidimensional*, al comentar la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO] (2021), que abarca enfoques desde disciplinas como la informática, la filosofía y el derecho. Esta pluralidad de perspectivas demuestra la necesidad de establecer criterios normativos sólidos que permitan delimitar la responsabilidad jurídica en los casos en los que su uso genere impactos adversos en la sociedad.

b.- Marco normativo que regule la IA en el Ecuador

Es menester, en este sentido, analizar y revisar *a priori* algunas regulaciones normativas a nivel mundial dirigidas a la IA, debido a que en Ecuador y en América Latina son escasas, particularmente, en materia de imputación de la responsabilidad penal y del *ius puniendi* que debe ejercer el Estado frente al cometimiento de estos crímenes por parte de IA; todo ello, con el propósito de fortalecer su estudio y contar con más elementos de juicio y de derecho a los fines de ostentar un *marco normativo* que adopte, en cierta medida, sus buenas prácticas.

Brasil ha sido pionero en América Latina, ya que desde 2019 ha intentado regular la IA, lo que se ha cristalizado en 2023, con la Ley 2238/2023, bajo un modelo de riesgos que determina las obligaciones y las responsabilidades para las partes intervinientes en el desarrollo y control de las IA. Del mismo modo *Perú*, *Chile* y *Colombia*, según se desprende del estudio de Sáenz y Terán (2024) están impulsando proyectos de ley que pretenden la regulación de varios aspectos de la IA. Tentativas reguladoras que están en sintonía con el Programa de las Naciones Unidas para el Desarrollo (en adelante PNUD) en su Estrategia Digital 2022-2025, que proporciona a los países miembros herramientas suficientes para la construcción de sociedades digitales, inclusivas, éticas y sostenibles con el propósito de fortalecer los ecosistemas digitales locales para lograr soluciones digitales sostenibles frente a posibles vulneraciones de los derechos humanos. Al

respecto Steiner (2025) asevera que esta nueva Estrategia Digital “seguirá transformando la manera en que la organización responde a los enormes desafíos que enfrenta nuestro mundo” (p. 2).

Sin duda, que la *legislación europea* es la que ha marcado la pauta con avances significativos en la regulación de la IA, como ha sido la aprobación por el Parlamento de la Unión Europea del texto final del *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo*, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial) (Texto pertinente a efectos del EEE). El objetivo del presente Reglamento es

promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (la “Carta”), incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger contra los efectos nocivos de los sistemas de IA en la Unión y apoyar la innovación. (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024)

Además de este Reglamento la UE ostenta las *Directrices Éticas para una IA fiable* (2019), que contiene un conjunto de 7 requisitos clave que deben cumplir los sistemas de IA para ser considerados fiables en el contexto de la UE. Otro aporte, de innegable mención es el *Libro Blanco sobre IA: un enfoque europeo orientado a la excelencia y la confianza*, de la Comisión Europea, de fecha 19.2.2020, en el que la Comisión:

respalda un enfoque basado en la regulación que tiene un doble objetivo de promover la adopción de la inteligencia artificial y de abordar los riesgos vinculados a determinados usos de esta nueva tecnología. (...). La IA conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos. (Libro Blanco sobre IA: un enfoque europeo orientado a la excelencia y la confianza, Comisión Europea, 2020)

Esto se complementa con la Resolución del Parlamento de la Unión Europea *La inteligencia artificial en el Derecho Penal y su uso por las autoridades policiales y judiciales en materia penal*, sancionada en 2020, que ha sido bien analizado por Laguna (2021) quien afirma que

Si un sistema IA vulnerara un bien jurídico protegido por el ordenamiento jurídico penal tendrá relevancia para la individualización de la responsabilidad penal, tomando en cuenta aspectos como prevención del daño por parte de los programadores y diseñadores. Además, en ella se habla de establecer un tipo penal consistente en un delito de riesgo (o de peligro), en el que sea punible no sólo el resultado material típico provocado por un sistema de IA de alto riesgo, sino el mero peligro que supone la creación de un sistema de estas características. (p. 14)

Esta regulación europea se integra con la existente en *EE.UU.* donde se aprobó por parte del Congreso Nacional la *Ley de la Iniciativa Nacional de la Inteligencia Artificial*, que dio nacimiento a la Comisión de Seguridad Nacional sobre Inteligencia Artificial, que en el año 2021 presentó un Informe con referencia a las amenazas emergentes de la IA y riesgos futuros a tomar en cuenta (NIST, 2025), como puede ser la proliferación de armas autónomas letales diseñadas para grupos terroristas de alta peligrosidad. Al mismo tiempo *Reino Unido*, en 2020 presenta el *Barómetro IA*, reforzado por la *Declaración de Bletchley sobre la seguridad de la IA*, de 2023, para hacer frente a los riesgos de los denominados modelos fronterizos de IA y la creación de políticas respectivas basadas en el riesgo entre los países.

Con este *panorama legislativo* en materia de IA se evidencia que *Ecuador* tiene suficiente material normativo para la elaboración de una normativa de vanguardia en IA; no obstante, la realidad es otra, ya que en el país “no existe legislación específica para las IA, salvo la *Ley Orgánica de Protección de Datos Personales* (2021) que hace referencias indirectas a esta tecnología” (León Párraga, 2024, p. 30). Este inicio embrionario ha dado lugar a que se presenten ante la Asamblea Nacional algunos Proyectos de Ley como *El Proyecto de Ley Orgánica de Neuro Protección y Aplicación Ética de las Neuro tecnologías*, en el año 2023 y el *Proyecto de Ley Orgánica de Derechos Digitales*, (Cod. AN-2023-2592 / AN-OVJC-2023-0026-M) del mismo año que pretenden garantizar el

acceso a Internet a todas las personas para cerrar la brecha digital, promoviendo el uso correcto de las redes calificado como un bien común para toda la humanidad. Y la *Ley Orgánica para la Transformación Digital y Audiovisual*, de la Asamblea Nacional, en 2023, cuyo objetivo, entre otros, “es el fortalecimiento del ciberespacio ecuatoriano procurando garantizar la seguridad de la información personal de los ciudadanos” (Asamblea Nacional, Ley Orgánica para la Transformación Digital y Audiovisual, 2023, Art. 1).

A pesar de estos esfuerzos normativos se puede asegurar que Ecuador padece de un vacío legislativo que es inminente *llenar* procurando aplicar la dogmática penal al contexto de los sistemas de IA, ya que estos realizan comportamientos relevantes para la vida social que deben contener el elemento subjetivo de la conducta —dolo o culpa—, como requisito *sine qua non* para determinar la responsabilidad penal del sujeto activo, en este caso de los desarrolladores, operadores o supervisores de la IA. Lo cual implica evaluar si existieron omisiones en la supervisión del sistema, defectos en su diseño o implementación, o la ausencia de medidas de seguridad adecuadas.

La CRE como norma suprema estructura un *marco legal garantista* basado en principios y en un catálogo de derechos y libertades, por lo que en el Art. 76, inciso 3 tipifica que “*Nadie podrá ser juzgado* ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal; si se le aplicará una sanción no prevista por la Constitución o la ley” (Asamblea Nacional Constituyente, CRE, 2008). Subrayado propio. Por orden constitucional se debe obedecer al principio de legalidad y tipicidad, por lo que en aquellos casos donde participan vehículos autónomos en la perpetración de daños a una persona, por este principio de legalidad es, prácticamente imposible atribuirle la responsabilidad a la IA, debido a la carencia de una normativa al respecto; lo cual genera un estado de indefensión a las víctimas de estos sistemas de IA. En esta misma dirección, los Arts. 66 y 341 de la CRE indican que la *integridad personal* y la *protección integral* de sus habitantes “no se limita a la protección contra agresiones físicas, sino que abarca también aspectos psíquicos, morales y sexuales” (Asamblea Nacional Constituyente, CRE, 2008). En estos casos al ser utilizada la IA para vulnerar este derecho, *v.gr.*, derivado de ciberacoso, sexting no consentido, *deepfake* pornográfico, *grooming*, pornografía infantil, invasión de privacidad, manipulación de

datos, entre otros, surge un desafío impostergable de adaptar el marco legal, en este caso el COIP, para abordar, de manera eficaz y efectiva, la responsabilidad penal.

Si bien el COIP ha incorporado dentro de su articulado varios delitos cibernéticos o relacionados con la IA, “el cual ya contempla sanciones para la violación de la privacidad y la seguridad informática en los Arts. 178 y 229” (Villalta León, 2024, p. 525), aún falta mucho por tipificar y por adaptar el Código a los nuevos y desafiantes riesgos emergentes, y a la velocidad en que se desarrollan estos sistemas de tecnología. Es de subrayar que, Ecuador evidencia vulnerabilidades en toda su infraestructura digital que lo expone a riesgos considerables, por lo que la protección cibernética adecuada contra ataque atentatorios de derechos de los ecuatorianos es elemental.

c.- Dilemas y desafíos éticos en el uso de la IA y el Derecho Penal

La aplicación de la IA genera significativos impactos en la administración de justicia, sobre todo, en el proceso penal que, según García y Barona (2024) “tiene por objeto asegurar que los casos que se inicien por el cometimiento de delitos sean resueltos de una manera consistente con los principios de debido proceso, buena fe procesal y respeto por la dignidad humana. Estos principios se ven reforzados o afectados por la aplicación de la IA” (pp. 102-103). Es así como, el uso de la IA en varios aspectos del Derecho Penal ha generado paulatinamente desafíos éticos y legales, particularmente, en el contexto de aplicación del COIP.

Entre los desafíos éticos que se vienen planteando en el uso de la IA es la posible transgresión del derecho a la privacidad de las personas que el COIP tipifica como delito si se implican los datos de las personas y genera daños; del mismo modo la Ley Orgánica de Protección de Datos Personales explana alguna normativa; no obstante, estas regulaciones son de difícil aplicación en el contexto del derecho penal, al establecer la responsabilidad de los sistemas de IA.

Otro de los desafíos es la reproducción de *sesgos algorítmicos* en el procesamiento de datos, lo cual puede conducir a resultados perjudiciales e injustos para determinados grupos vulnerables que se establecen en los algoritmos. Como sucede con el uso del sistema COMPAS —*Correctional Offender Management Profiling for Alternative Sanctions*—, instrumento utilizado para obtener el riesgo de reincidencia de los procesados, lo cual puede estar sesgado y generar resultados ajenos a la realidad penal.

En igual interpretación, se presenta como desafío —a resolver de inmediato— la atribución de responsabilidad legal y de culpa, lo cual hace indispensable la calificación de sujeto de derecho o no —persona natural o jurídica— de la IA.

Los *sistemas predictivos de criminalidad*, el *reconocimiento facial* basado en IA, han sido altamente criticados, debido a que “suscitan preocupaciones sobre la invasión de la privacidad, la falta de consentimiento y el potencial uso para reprimir a la población. Estos casos, ponen de relieve los riesgos de utilizar IA sin un marco sólido de derechos humanos y garantías legales” (Loaiza Moreno et al, 2024, p. 2165). Actualmente frente al incremento del crimen organizado, el narcotráfico y los secuestros la Fiscalía General y organismos competentes están implementando herramientas de IA para optimar la investigación criminal; sin embargo, su uso indiscriminado ha derivado muchas dudas sobre el respeto de los derechos de los acusados dentro del proceso y los eventuales errores algorítmicos.

El análisis de los casos evidencia que, aunque la IA puede optimizar la seguridad y la eficiencia en la administración de justicia, su implementación sin una regulación adecuada conlleva riesgos significativos. Por ello, resulta imperativo que los países de la región, entre ellos Ecuador, adopten marcos normativos de vanguardia que aseguren un uso responsable, ético y conforme a los principios y garantías constitucionales, priorizando en todo momento la protección de los derechos fundamentales de las personas y garantizando mecanismos de supervisión y rendición de cuentas, que conduzcan a la responsabilidad efectiva.

d.- ¿Sobre quién debería recaer la responsabilidad jurídica, ocasionada por una IA?

La determinación de la responsabilidad jurídica por los daños ocasionados por una IA es un tema complejo que ha generado un amplio debate doctrinario, expuesto aquí de manera sucinta. Desde una *perspectiva tradicional* del derecho penal y civil, la responsabilidad recae sobre sujetos jurídicos capaces de actuar con voluntad y conciencia —sujetos con capacidad jurídica—, elementos que la IA no posee. Por ello, autores como Miró Llinares (2018) han propuesto modelos de responsabilidad en función del grado de autonomía de la IA, estableciendo tres categorías: la IA como una herramienta en manos de un operador humano (responsabilidad indirecta del programador o usuario), la IA como agente intermedio con cierto margen de decisión

(responsabilidad compartida) y la IA completamente autónoma, donde se requeriría la creación de un nuevo marco jurídico.

Plantear la cuestión de cómo repartir las responsabilidades entre los agentes que participan en el proceso de los sistemas de IA es fundamental, ya que hay numerosas partes involucradas en el ciclo de vida de un sistema de IA. Entre ellas, el desarrollador, el implementador (la persona que utiliza un producto o servicio provisto de IA) y otras partes potenciales (productor, distribuidor o importador, proveedor de servicios, usuario profesional o particular). Además, es esencial considerar el grado de control y previsibilidad que cada uno de estos agentes tiene sobre el comportamiento del sistema de IA, así como su capacidad para mitigar posibles daños. En este sentido, establecer criterios claros de atribución de responsabilidad permitirá garantizar una regulación efectiva que proteja los derechos fundamentales y prevenga abusos en el uso de la IA en el contexto nacional ecuatoriano.

DISCUSIÓN

La revisión documental, como técnica especializada, permitió analizar las posturas de diversos autores respecto al impacto de la Inteligencia Artificial en el ámbito jurídico. García Falconí y Barona Pazmiño (2024) destacan las ventajas y beneficios que los sistemas de IA pueden aportar en la optimización de procesos, la toma de decisiones y la eficiencia en la administración de justicia. Sin embargo, Vall Prieto (2022) advierte que el uso de esta tecnología también conlleva riesgos significativos, evidenciados en múltiples casos donde la IA ha vulnerado derechos fundamentales consagrados en las Constituciones de distintos países. Esta dualidad entre el potencial positivo de la IA y sus posibles efectos adversos subraya la necesidad de un marco normativo sólido que garantice su implementación ética y responsable.

El estudio de las distintas concepciones sobre la inteligencia artificial revela su carácter multidimensional y la urgencia de un marco jurídico coherente que regule su desarrollo y aplicación en cualquier Estado que donde se tenga como norte el respeto a los derechos constitucionales. En el ámbito jurídico, la IA no debe concebirse desde una herramienta tecnológica, sino como un fenómeno con profundas implicaciones éticas y legales que exige responsabilidad y control normativo. La propuesta europea de 2021 constituye un

referente al situar el enfoque en la protección de los derechos fundamentales y en el uso responsable de la tecnología. Desde esta perspectiva, el derecho debe anticiparse a los posibles riesgos derivados de su aplicación, garantizando la primacía del ser humano sobre la máquina. En consecuencia, la regulación de la IA debe orientarse hacia la justicia, la transparencia y la tutela efectiva de los derechos en un entorno digital en expansión.

Al decir de Villalta (2024), “en el contexto ecuatoriano, la falta de regulación sobre la IA en el COIP implica que no existen precedentes o normativas claras que asignen la responsabilidad en casos donde un sistema automatizado cometa un error que afecte los derechos de un individuo” (p. 532). Al respecto Becerril (2021) ha dicho que “el COIP ya regula los delitos informáticos, pero la incorporación de IA a estas dinámicas introduce un nivel adicional de complejidad” (p. 13), que trae consigo incertidumbre al momento de sancionar e imprimir la responsabilidad al delincuente cibernético debido a que no hay un protocolo o guía sobre cómo aplicar principios legales del proceso penal tradicional a aquellos casos en que la IA juega un papel determinante en las consecuencias derivadas del cometimiento del delito.

Como sostiene Laín (2021) “la necesidad de perfilar un régimen de responsabilidad del uso de la inteligencia artificial, ha llevado a que el Grupo de Expertos en Responsabilidad y Nuevas Tecnologías de la Comisión Europea publique un documento titulado Responsabilidad derivada del uso de la inteligencia artificial y otras tecnologías emergentes, que representa un punto de partida de la UE para el estudio de la responsabilidad por daños derivada de accidentes provocados por sistemas de IA en todo su amplio campo” (p. 218), esto puede ser utilizado por países de América Latina para regular la atribución de responsabilidad criminal.

Los esfuerzos legislativos presentes tanto en Europa, en EEUU y en algunos países de América Latina, contribuyen a la existencia de una normativa que Ecuador puede tomar en cuenta para lograr una debida legislación; ya que, la IA no ha sido regulada con rigor y criterio científico, dejándose de lado aspectos tan importantes como el uso indebido de la IA relativo a los datos personales, los riesgos que enfrenta la IA, la protección de los derechos fundamentales y la responsabilidad de los actos cometidos por la IA con asistencia humana. Aspectos estos que, no deben ser tratados y estudiados, con

superficialidad, sino de manera multidimensional, como acertadamente indica León (2024), para “un justo equilibrio en la regulación, la cual permita aprovechar las bondades de la IA, al mismo tiempo que minimice sus riesgos y proteja los derechos individuales” (p. 32).

Al hacer referencia sobre la interrogante, que resulta de inmediato, sobre quién debería recaer la responsabilidad jurídica, ocasionada por una IA, es pertinente tomar en cuenta el enfoque del garantismo penal de Luigi Ferrajoli (2007) quien resalta que, en la medida en que la IA carece de intencionalidad y autonomía moral, la responsabilidad debe recaer sobre los diseñadores, fabricantes y operadores que tienen control sobre su programación y uso. Esta postura se alinea con el principio de *imputación objetiva*, expuesta por Roxin (2010) y Jakobs (1996), según el cual la responsabilidad penal solo puede atribuirse a sujetos capaces de prever y evitar daños. Sin embargo, ante sistemas de IA que aprenden y toman decisiones sin intervención humana directa, algunos autores como Matthias (2004) sugieren la necesidad de revisar los fundamentos del derecho penal y crear figuras jurídicas que permitan imputar responsabilidad de manera proporcional al grado de control sobre la tecnología. En este sentido, la regulación debe equilibrar la innovación con la protección de los derechos fundamentales, garantizando mecanismos de supervisión y sanción adecuados para mitigar los riesgos asociados a la IA.

Asimismo, la revisión crítica de la literatura evidencia que el debate sobre la responsabilidad penal en el uso de IA bajo supervisión humana no puede desligarse de la discusión sobre la trazabilidad algorítmica y la opacidad de los sistemas de aprendizaje automático. Diversos estudios enfatizan que, ante la ausencia de transparencia en los procesos internos de decisión de la IA, se dificulta determinar el nexo causal entre la conducta humana y el resultado lesivo generado por el sistema. Este fenómeno, conocido como *black box problem*, plantea desafíos significativos para la imputación penal, ya que obstaculiza la precisión probatoria exigida por el estándar de certeza razonable. En este horizonte, autores como Villalta León (2024) han enfatizado la necesidad de integrar principios de *accountability* algorítmica y auditoría tecnológica como condición mínima para garantizar procesos penales justos, especialmente en escenarios donde la IA interviene en decisiones de alto impacto. La ausencia de estos mecanismos pone en

riesgo la vigencia misma del debido proceso, generando una zona gris que el derecho penal contemporáneo aún no alcanza a resolver plenamente.

De igual forma, la discusión sobre la responsabilidad penal por actos cometidos mediante IA se complejiza cuando se considera el rápido avance tecnológico y la inevitable disonancia entre la velocidad del desarrollo científico y la lentitud natural del proceso legislativo. Esta brecha genera lo que autores como Bravo Zapata (2024) denominan déficit de juridicidad tecnológica, entendido como la incapacidad temporal del derecho para regular fenómenos emergentes con la prontitud que exigen los riesgos asociados. En este sentido, la investigación evidencia que Ecuador enfrenta un desafío doble: por un lado, armonizar su normativa penal con los estándares internacionales más avanzados en materia de IA y, por otro, construir un marco jurídico propio que responda a su realidad constitucional garantista. La ausencia de protocolos técnicos, definiciones legales claras y criterios de imputación específicos para escenarios con IA no solo genera inseguridad jurídica, sino que podría propiciar vulneraciones sistemáticas a los derechos fundamentales. Por ello, la discusión invita a repensar el diseño de políticas públicas, estrategias de formación judicial y reformas normativas que permitan responder adecuadamente a la complejidad del ecosistema digital contemporáneo.

CONCLUSIONES

El análisis doctrinario y normativo realizado evidencia que Ecuador aún no cuenta con un marco regulatorio específico que permita atribuir responsabilidad penal en situaciones donde la IA sea empleada para vulnerar los derechos de las personas generando daños a sus bienes protegidos. No obstante, la normativa vigente destaca la necesidad de actualizar el ordenamiento jurídico para incorporar disposiciones que tipifiquen las nuevas conductas penalmente relevantes derivadas del uso de esta tecnología. Esta carencia regulatoria pone de manifiesto la urgencia de adaptar el derecho penal a los desafíos tecnológicos actuales, asegurando así una respuesta efectiva frente a los riesgos asociados a la IA.

Asimismo, el uso de la IA plantea retos éticos y jurídicos de gran relevancia, como la protección de la privacidad, la prevención de la discriminación y la parcialidad, la transparencia en los procesos de toma de decisiones y la equidad en el ámbito penal.

Para garantizar una aplicación responsable y ética de la IA en el procedimiento penal, es fundamental desarrollar marcos de gobernanza específicos, fortalecer la transparencia y la rendición de cuentas, y fomentar la cooperación entre actores públicos y privados. Además, resulta esencial continuar con la investigación en esta materia, a fin de identificar los bienes jurídicos que podrían verse afectados por el impacto de los sistemas inteligentes. Dichos bienes incluyen tanto derechos individuales, como la privacidad, la libertad y el patrimonio, como intereses colectivos, tales como los derechos laborales, el libre mercado y la protección del medio ambiente. En este sentido, la actualización normativa no solo debe enfocarse en la atribución de responsabilidad penal, sino también en la creación de mecanismos que garanticen el respeto a los principios éticos y jurídicos fundamentales.

Los estudios doctrinales presentan diversas soluciones para abordar la responsabilidad jurídica en el uso de la IA, destacando principalmente la aplicación de la responsabilidad por imprudencia y la implementación de modelos de cumplimiento normativo —*compliance*— como enfoques más sólidos y viables. Es de resaltar que, este trabajo no pretende agotar todas las cuestiones abordadas ni aquellas que aún están por plantearse, pero sí comenzar la discusión a nivel universitario y científico, como es este Congreso de estudiantes de Derecho de las Universidades ecuatorianas. Es ineludible dar los primeros pasos para hacerlo, ya que resulta evidente que la IA ha sido incorporada con relativo éxito en procesos de toma de decisiones. Además, su presencia en estos ámbitos no parece disminuir en el futuro, sino que, por el contrario, continuará en expansión.

Conflicto de interés

Los autores no tienen conflictos de interés

Financiación

Este proyecto no contó con ninguna fuente de financiación

Responsabilidades Éticas

El proyecto fue aprobado por el comité de ética de la institución.

REFERENCIAS

- Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador*. Registro oficial No. 449, de 20 de octubre de 2008.
- Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180 de 10-feb-2014.
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459 de 26-may.-2021.
- Asamblea Nacional del Ecuador. (2023). *Ley Orgánica para la Transformación Digital y Audiovisual*. Registro Oficial Tercer Suplemento No. 245, de fecha 7 de febrero de 2023.
- Becerril, A. (2021). Retos para la regulación jurídica de la inteligencia artificial en el ámbito de la ciberseguridad. En *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, 15(48), 9-34. <https://doi.org/10.35487/rius.v15i48.2021.705>
- Bravo Zapata, J. (2024). Afectaciones de las nuevas tecnologías al derecho de propiedad intelectual en Ecuador en el año 2023. Repositorio Digital UNIANDES. <https://dspace.uniandes.edu.ec/handle/123456789/18769>
- Comisión Europea. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas.
- Ferrajoli, L. (2007). *Garantismo Penal*. Universidad Nacional Autónoma de México.
- García Falconí, R.; Barona Pazmiño, K. (2024). Inteligencia artificial y proceso penal. En *Revista San Gregorio*, 1(58), 101-110. <http://dx.doi.org/10.36097/rsan.v1i58.2808?subject=>
- Gómez, G. (2024). De la investigación sociojurídica a la investigación interdisciplinaria en derecho: una mirada crítica sobre las transformaciones en las últimas décadas en Colombia. *Revista CS*, 44, a04. <https://doi.org/10.18046/recs.i44.04>
- Jakobs, G. (1996). *La imputación objetiva en el Derecho Penal*. Ad-Hoc, SRL.
- Laguna. I. (2021). *Inteligencia Artificial y atribución de la responsabilidad penal*. Universidad del País Vasco.

- Laín Moyano, G. (2021). Responsabilidad en inteligencia artificial: Señorita, mi cliente robot se declara inocente. En *Ars Iuris Salmanticensis*, Vol. 9, junio 2021, 197-232. <https://revistas.usal.es/cuatro/index.php/ais/article/view/AIS202191197232>
- León Párraga, V. (2024). *Responsabilidad penal de la IA: ausencia de producción normativa en Ecuador*. Universidad Laica “Eloy Alfaro” de Manabí. <https://repositorio.uleam.edu.ec/bitstream/123456789/6424/1/ULEAM-DER-0117.pdf>
- Loaiza Moreno, J.; Soto Soto, F.; Hoyos Escaleras, A. (2024). Revolucionando la justicia: el impacto de la inteligencia artificial en el Derecho Penal. En *Estudios y Perspectivas Revista Científica y Académica*, Vol. 4, Núm. 3, julio-septiembre 2024, Pilar, Paraguay. <https://doi.org/10.61384/r.c.a.v4i3.537>
- Matthias, A. (2004). The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata”. En *Ethics and Information Technology*, vol. 6, núm. 75. <https://philpapers.org/rec/MATTRG>
- Miró Llinares, F. (2018). Inteligencia Artificial y Justicia Penal: Más allá de los resultados lesivos causados por robots. En *Revista de Derecho Penal y Criminología*, 3.^a Época, No. 20, 87-130. <https://revistas.uned.es/index.php/RDPC/article/view/26446>
- NIST, Inteligencia Artificial (2025). Mandatos, órdenes ejecutivas y acciones del Congreso sobre IA. Sitio web oficial del Gobierno de EE.UU. <https://www.nist.gov/artificial-intelligence/ai-congressional-mandates-executive-orders-and-actions>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO . (2021). Recomendación sobre la ética de la Inteligencia Artificial. <https://bit.ly/3ITlvSf>
- Organización de las Naciones Unidas. (2022-2025). *Programa de las Naciones Unidas para el Desarrollo (PNUD) en su Estrategia Digital 2022-2025*.
- Parlamento Europeo y Consejo. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo*, de 13 de junio de 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

- Prigiani, F. (2023). Beneficios y problemas de la IA en el Derecho. En *Revista Pensamiento Penal*, No. 460, marzo 2023, 1-3.
https://www.pensamientopenal.com.ar/system/files/Documento_Editado1027.pdf
- Rouhiainen, L. (2018). *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*.
https://proassetspdlcom.cdnstatics2.com/usuaris/libros_contenido/arxius/40/39307_Inteligencia_artificial.pdf
- Roxin, C. (2010). Problemas de la imputación objetiva. En *Revista de Derecho Penal* 2010-2. Imputación, causalidad y ciencia-II, Edic. Rubinzal-Culzoni, Santa Fe, 13-35. <https://www.rubinzalonline.com.ar/catalogo/tomoRevista.php?id=3910>
- Sáenz, M.; Terán, A. (2024). Regulación de la inteligencia artificial en Ecuador. *HEKA*.
https://es.linkedin.com/pulse/regulaci%C3%B3n-de-la-inteligenciaartificial-en-ecuador-evitar-sobrerregulaci%C3%B3n-ufpje?trk=public_post
- Steiner, A. (2025). *Prefacio a la Estrategia Digital 2022-2025*. Programa de las Naciones Unidas para el Desarrollo. <https://digitalstrategy.undp.org/>
- Vall Prieto, J. (2022). Sobre la responsabilidad penal por la utilización de sistemas inteligentes. En *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 24-27. <https://dialnet.unirioja.es/servlet/articulo?codigo=8587635>
- Villalta León, J. (2024). Desafíos y adaptaciones legales ante la inteligencia artificial: privacidad y protección de datos en el marco del Código Orgánico Integral Penal. En *Revista Sinergia Académica*, Vol. 7, No. Especial 6, año 2024, 524-540.
<https://sinergiaacademica.com/index.php/sa/article/view/323/650>