J-40402082-9

Fundación Aula Virtual

Aula Virtual

Generando Conocimiento

http://www.aulavirtual.web.ve

ISSN: 2665-0398

Deposito Legal: LA2020000026

Vol. 7 Nº 15 Año 2026

Periodicidad Continua

AulaVirtual
Generando Conocimiento

ISSN: 2665-0398

REVISTA CIENTÍFICA AULA VIRTUAL

Director Editor:

- Dra. Leidy Hernández PhD.
- Dr. Fernando Bárbara

Consejo Asesor:

- MSc. Manuel Mujica
- MSc. Wilman Briceño
- Dra. Harizmar Izquierdo
- Dr. José Gregorio Sánchez

Revista Científica Arbitrada de Fundación Aula Virtual

Email: revista@aulavirtual.web.ve
URL: http://aulavirtual.web.ve/revista

ISSN: 2665-0398
Depósito Legal: LA2020000026
País: Venezuela
Año de Inicio: 2020
Periodicidad: Continua
Sistema de Arbitraje: Revisión por pares. "Doble Ciego"
Licencia: **Creative Commons** CC BY NC ND
Volumen: 7
Número: 15
Año: 2026
Período: Julio 2026 – Diciembre 2026 (continua)
Dirección Fiscal: Av. Libertador, Arca del Norte, Nro. 52D, Barquisimeto estado Lara, Venezuela, C.P. 3001

La Revista seriada Científica Arbitrada e Indexada **Aula Virtual**, es de acceso abierto y en formato electrónico; la misma está orientada a la divulgación de las producciones científicas creadas por investigadores en diversas áreas del conocimiento. Su cobertura temática abarca Tecnología, Ciencias de la Salud, Ciencias Administrativas, Ciencias Sociales, Ciencias Jurídicas y Políticas, Ciencias Exactas y otras áreas afines. Su publicación es **CONTINUA**, indexada y arbitrada por especialistas en el área, bajo la modalidad de doble ciego. Se reciben las producciones tipo: *Artículo Científico* en las diferentes modalidades cualitativas y cuantitativas, *Avances Investigativos*, *Ensayos, Reseñas Bibliográficas, Ponencias o publicaciones derivada de eventos*, y cualquier otro tipo de investigación orientada al tratamiento y profundización de la información de los campos de estudios de las diferentes ciencias. La Revista **Aula Virtual,** busca fomentar la divulgación del conocimiento científico y el pensamiento crítico reflexivo en el ámbito investigativo.

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD PENAL: NUEVAS FRONTERAS EN LA IMPUTACIÓN DE DELITOS

ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY: NEW FRONTIERS IN THE ATTRIBUTION OF CRIMES

Tipo de Publicación: Artículo Científico
Área del Conocimiento: Ciencias Sociales y Aplicadas
Recibido: 18/09/2026
Aceptado: 20/10/2026
Publicado: 29/20/2026
Código Único AV: e890
Páginas: 1(2031-2056)
DOI: https://doi.org/10.5281/zenodo.23765431

Autor:
Juan Pablo Rodas Izquierdo
Juez multicompetente
Maestría en Derecho, mención Estudios Judiciales
https://orcid.org/0009-0008-2839-8029
E-mail: rodasiz@hotmail.com
Afiliación: Universidad Bolivariana del Ecuador
País: Ecuador

Resumen

La rápida expansión de la inteligencia artificial genera un vacío normativo de gran relevancia en la teoría del delito contemporánea, especialmente frente al impacto tecnológico inminente en el ordenamiento penal ecuatoriano. Este estudio científico tuvo como objetivo evaluar de manera dogmática y comparada la suficiencia de los criterios de imputación del Código Orgánico Integral Penal ante conductas lesivas de sistemas autónomos, proponiendo un modelo normativo basado en el control humano significativo. Para ello, se adoptó un riguroso enfoque cualitativo y documental, aplicando la triangulación hermenéutica entre la dogmática nacional, el derecho comparado internacional y los presupuestos técnicos del aprendizaje profundo y la opacidad algorítmica de la caja negra. Los resultados revelan que las categorías antropocéntricas tradicionales colapsan por completo ante la autonomía algorítmica, evidenciando la inviabilidad jurídica de adscribir dolo o culpa clásica y la notoria insuficiencia del régimen restrictivo de las personas jurídicas. Asimismo, se demuestra que la teoría de la imputación objetiva funcionalista permite reconducir adecuadamente el riesgo mediante esferas de competencia organizativa sin recurrir a la errónea ficción de sancionar a la máquina. En conclusión, se valida plenamente la necesidad imperativa de una reforma legal específica para superar la impunidad tecnológica y garantizar la seguridad jurídica.

Palabras Clave Ecuador, funcionalismo penal, imputación objetiva, inteligencia artificial, responsabilidad penal

Abstract

The rapid expansion of artificial intelligence generates a significant normative gap within contemporary criminal theory, particularly regarding its imminent technological impact on Ecuador's criminal justice system. This scientific study aimed to dogmatically and comparatively evaluate the sufficiency of the imputation criteria set forth in the Comprehensive Organic Criminal Code when dealing with harmful conduct perpetrated by autonomous systems, ultimately proposing a normative model based on significant human control. To achieve this, a rigorous qualitative and documentary approach was adopted, applying hermeneutic triangulation between national dogmatics, international comparative law, and the technical assumptions of deep learning and the algorithmic opacity of the black box. The results reveal that traditional anthropocentric categories collapse completely before algorithmic autonomy, evidencing the legal infeasibility of ascribing classical intent or negligence, as well as the notorious insufficiency of the restrictive regime for legal entities. As a fundamental discussion, it is demonstrated that functionalist objective imputation theory allows for appropriately redirecting risk through spheres of organizational competence without resorting to the erroneous fiction of sanctioning the machine. In conclusion, the imperative need for a specific legal reform is fully validated to overcome technological impunity and guarantee legal certainty.

Keywords Artificial intelligence, criminal liability, ecuador, objective imputation, penal functionalism

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

Introducción

La cuarta revolución industrial ha desplazado de forma definitiva el rol de la tecnología desde un plano meramente instrumental hacia un estatus de agente activo dotado de capacidad para la toma de decisiones autónomas y adaptativas. La Inteligencia Artificial (IA) contemporánea ya no se limita a ejecutar líneas rígidas de código preprogramado; por el contrario, los sistemas actuales interactúan de forma dinámica con su entorno, modificando sus propios parámetros funcionales y de decisión en tiempo real a través de modelos probabilísticos y de aprendizaje continuo (Salardi, 2020).

Este salto cualitativo representa un hito sin precedentes para la sociedad global y redefine sustancialmente las bases epistemológicas de las ciencias sociales, imponiendo un desafío de primer orden para la ciencia del Derecho, la cual se enfrenta a la urgente necesidad de adaptar sus conceptos tradicionales a realidades operativas caracterizadas por la imprevisibilidad y la autonomía técnica.

La justificación de investigar la relación entre la Inteligencia Artificial y la responsabilidad penal descansa sobre la rápida e irreversible penetración de estas tecnologías en sectores de alto impacto para la seguridad colectiva y el orden público social. Entornos de alto riesgo como la medicina de precisión, la conducción de vehículos autónomos, las transacciones financieras de alta frecuencia y los sistemas automáticos de control industrial delegan día a día funciones críticas en modelos algorítmicos.

Sin embargo, el dinamismo vertiginoso con el que la IA asume roles tradicionalmente reservados al juicio humano no ha sido correspondido por una evolución regulatoria análoga en el plano penal, lo que genera un vacío de protección jurídica ante daños emergentes (Bashayreh, 2021). Por lo tanto, analizar la imputación de delitos cometidos mediante o con asistencia de IA no constituye un mero ejercicio académico de prospectiva jurídica, sino una necesidad imperativa para garantizar la paz social y la protección eficaz de los bienes jurídicos fundamentales.

El problema dogmático central radica en que la teoría del delito tradicional ha sido construida sobre cimientos estrictamente antropocéntricos que dificultan su aplicación directa a sistemas autónomos. Categorías fundamentales como la conducta —constreñida doctrinalmente a la acción u omisión voluntaria y consciente del ser humano— y la culpabilidad —enlazada con los elementos cognitivos y volitivos del dolo o la culpa de una persona física— pierden operatividad frente a los actos lesivos decididos y ejecutados de forma autónoma por un algoritmo (Momblanc, 2024). Cuando un sistema de aprendizaje profundo toma una decisión imprevisible para sus desarrolladores o usuarios que desencadena un daño típico, como la lesión de un paciente por un error de diagnóstico

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

autónomo, se produce una severa fragmentación del nexo causal y de los criterios de imputación penal vigentes.

Frente a este escenario de incertidumbre, el ordenamiento jurídico se enfrenta a una asimetría técnico-jurídica de complejas consecuencias sociales e institucionales. Por un lado, existe el riesgo de recurrir a la peligrosa ficción de atribuir responsabilidad o capacidad sancionatoria a la máquina, lo cual contraviene el principio de culpabilidad y la función motivadora de la pena. Por otro lado, la imposibilidad de adscribir la conducta a un individuo físico puede conducir a una preocupante impunidad donde los daños reales sufridos por las víctimas no encuentren respuesta en el sistema de justicia criminal. La pregunta central que orienta este trabajo no consiste en determinar si una máquina puede ser declarada culpable, sino en precisar bajo qué condiciones normativas una decisión automatizada permite atribuir a una persona natural o jurídica una conducta penalmente relevante.

Esta distinción adquiere un relieve ético y práctico fundamental en el plano de la justicia distributiva y la protección de derechos garantizados. Cuando un sistema utilizado en áreas estratégicas como la salud, el transporte o los servicios públicos ocasiona un daño grave, las víctimas tienen derecho a una investigación efectiva y a la reparación integral de los perjuicios. No obstante, los profesionales e ingenieros involucrados en el ciclo de vida de la tecnología también tienen el derecho fundamental a no ser condenados por el solo hecho de haber participado en una cadena tecnológica compleja. Por consiguiente, la dogmática penal contemporánea exige una formulación teórica capaz de conciliar de forma armónica la protección de bienes jurídicos tutelados, el fomento de la innovación tecnológica responsable y el respeto irrestricto a las garantías penales.

En el contexto específico del Ecuador, esta problemática adquiere una gravedad institucional particular debido a la brecha existente entre la adopción tecnológica y el marco normativo. Aunque la incorporación de herramientas de automatización e IA ha experimentado un incremento constante en el sector productivo y corporativo nacional (Instituto Nacional de Estadística y Censos [INEC], 2024), la legislación penal sustantiva se mantiene inalterada desde la promulgación del Código Orgánico Integral Penal (COIP) en el año 2014. El COIP carece por completo de definiciones técnicas, principios de gestión del riesgo y herramientas conceptuales aptas para juzgar la criminalidad de base algorítmica, lo que sitúa al país en una condición de vulnerabilidad normativa ante eventuales siniestros tecnológicos.

La ausencia de un marco legal actualizado fuerza a los operadores de justicia ecuatorianos a

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

enfrentar un dilema constitucionalmente inaceptable ante eventos lesivos derivados de la IA. Por una parte, existe la tentación de realizar interpretaciones analógicas in malam partem de los tipos penales tradicionales para forzar la culpabilidad del usuario o desarrollador, lo cual vulnera de manera directa el principio de estricta legalidad y el debido proceso garantizados por la Constitución de la República del Ecuador (2008). Por otra parte, la falta de herramientas tipificadoras y de criterios normativos para atribuir el deber objetivo de cuidado sobre sistemas opacos conduce frecuentemente al archivo de las causas y a la impunidad fáctica de infracciones causadas por imprudencia en el diseño o supervisión algorítmica.

Para superar este estancamiento doctrinal y legislativo, resulta indispensable analizar las soluciones formuladas por el derecho comparado y la dogmática penal moderna. La tendencia internacional demuestra que la evaluación de los siniestros inteligentes no debe basarse en esquemas causalistas naturalistas, sino en criterios de imputación objetiva y en el examen de la infracción de deberes de cuidado derivados del riesgo permitido.

En este sentido, instrumentos como el Reglamento (UE) 2024/1689 de la Unión Europea ofrecen un marco de referencia relevante al clasificar los sistemas de IA según su nivel de riesgo y fijar estándares técnicos de supervisión humana que pueden servir de insumo normativo extrapenal para delimitar la responsabilidad de los actores involucrados (Reglamento UE 2024/1689, 2024).

En atención a las consideraciones expuestas, el objetivo general de este estudio consiste en evaluar de manera dogmática y comparada la suficiencia de los criterios de imputación de la teoría del delito en el Código Orgánico Integral Penal ecuatoriano frente a las conductas lesivas ejecutadas por sistemas autónomos de Inteligencia Artificial, con la finalidad de formular una propuesta normativo-funcional basada en el control humano significativo y la gestión del riesgo algorítmico que garantice la seguridad jurídica y prevenga escenarios de impunidad tecnológica. Con ello, la investigación busca contribuir a la actualización del debate jurídico penal nacional, ofreciendo pautas teóricas y legislativas coherentes con el Estado constitucional de derechos y justicia.

Para cumplir con este propósito, la investigación articula una metodología cualitativa fundamentada en la triangulación dogmática, el análisis de derecho comparado y la revisión de la normativa técnica aplicable a las tecnologías disruptivas. A través de este enfoque, se examinan las categorías clásicas de la conducta, la tipicidad, la antijuridicidad y la culpabilidad a la luz del fenómeno de la opacidad algorítmica o "caja negra", proponiendo esferas de competencia claramente delimitadas para desarrolladores, implementadores

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

y usuarios. De este modo, el estudio pretende sentar las bases teóricas para una reforma legal prudente y garantista que responda de manera eficaz a los desafíos planteados por la consolidación de la era digital en la administración de justicia.

Metodología

Para abordar de manera rigurosa y sistemática los vacíos de imputación penal derivados de la proliferación de sistemas de Inteligencia Artificial (IA) en el ordenamiento jurídico ecuatoriano, la presente investigación adopta un diseño cualitativo de alcance descriptivo-explicativo, fundamentado en la investigación dogmático-jurídica, la hermenéutica normativa y el análisis de derecho comparado (Aguilar Campos & Alé Martínez, 2025; Roxin, 1997). El estudio se aparta de la contrastación cuantitativa de variables empíricas físicas o sociodemográficas directas, enfocándose en la relectura epistemológica y sistemática de las categorías fundamentales de la teoría del delito (conducta, tipicidad, antijuridicidad, culpabilidad e imputación objetiva) a la luz del progreso tecnológico de los algoritmos de aprendizaje profundo (Momblanc, 2024; Salvadori, 2024).

El enfoque cualitativo-documental permite evaluar la coherencia lógica interna, la validez axiológica y la adecuación práctica de las soluciones normativas vigentes frente al fenómeno técnico de la opacidad algorítmica o efecto de "caja negra" (Russell & Norvig, 2022; Salardi, 2020). De este modo, la investigación procesa la información jurídica y tecnológica no como meros enunciados teóricos abstractos, sino como unidades de análisis interconectadas que requieren una interpretación integrada para resolver problemas concretos de atribución de responsabilidad penal en la sociedad digital contemporánea (Barona Vilar, 2019; Silva Sánchez, 2020).

Como hipótesis central de trabajo se postula que la teoría de la imputación objetiva de base funcionalista —combinada con el examen individualizado de la infracción del deber objetivo de cuidado y el análisis de la posición de garante en las esferas de competencia organizativa— ofrece un marco dogmático técnicamente sólido y jurídicamente defendible para procesar penalmente los daños ocasionados por sistemas autónomos de IA en el Ecuador, sin necesidad de recurrir a la ficción inconstitucional de dotar de personalidad penal a la máquina ni generar escenarios de impunidad fáctica (Jakobs, 1997; Pullas Tituaña, 2026; Roxin, 2014).

Para verificar y contrastar la hipótesis planteada dentro de un esquema analítico riguroso, el proceso de investigación se estructuró en torno a tres preguntas de verificación normativa y técnico-probatoria orientadas a determinar quién ostentaba la posición de garante y la capacidad fáctica para controlar el riesgo (Morte Ferrer, 2021; Rodas Izquierdo, 2026), cuál fue el deber objetivo de

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

cuidado o estándar de seguridad concretamente incumplido durante el ciclo de vida del algoritmo (Concha Flores, 2024; Reglamento UE 2024/1689, 2024), y si el daño típico materializado corresponde precisamente a la realización del peligro no permitido generado por la conducta negligente (Momblanc, 2024; Silva Sánchez, 2020).

Para garantizar la validez interna y la transferibilidad del estudio, el método de investigación se sustenta en la triangulación analítica cualitativa articulando tres dimensiones metodológicas interdependientes. La primera es la dimensión dogmática y constitucional nacional, que comprende el estudio exegético y hermenéutico del Código Orgánico Integral Penal del Ecuador (COIP, 2014), analizando la estructura de la infracción penal (Art. 18), la conducta relevante (Art. 22), el dolo (Art. 26), la culpa (Art. 27), la omisión impropia (Art. 28) y la responsabilidad penal de personas jurídicas (Art. 49) frente a las garantías constitucionales del debido proceso y el principio de estricta legalidad consagrados en el artículo 76 de la Constitución de la República del Ecuador (2008).

La segunda es la dimensión de derecho comparado y normativa internacional, la cual involucra el análisis cualitativo-comparativo de las tendencias regulatorias de vanguardia, tomando como referente el Reglamento (UE) 2024/1689 de Inteligencia Artificial (AI Act), la doctrina de responsabilidad por productos defectuosos en los Estados Unidos (Bashayreh et al., 2021), los modelos de certificación técnica previa en Japón y Corea del Sur (Bashayreh et al., 2021), y los avances normativos y jurisprudenciales incipientes en América Latina (CEPAL, 2025; Souto Etchamendi, 2025).

La tercera es la dimensión técnica e informática de la IA, que analiza los presupuestos empíricos de la informática moderna y la ciencia de datos (Russell & Norvig, 2022), examinando los niveles de autonomía algorítmica y el funcionamiento estocástico de las redes neuronales profundas para determinar el alcance científico de conceptos penales como la previsibilidad y la transparencia algorítmica (Salvadori, 2024).

La recolección de información se realizó mediante un muestreo documental cualitativo no probabilístico por conveniencia teórica. La búsqueda bibliográfica y documental se ejecutó de forma sistemática en bases de datos científicas indexadas de alto impacto (Scopus, Web of Science, SciELO, Redalyc) y repositorios normativos oficiales, empleando operadores booleanos (AND, OR) con cadenas de búsqueda especializadas como: "inteligencia artificial" AND "responsabilidad penal", "machine learning" AND "imputación objetiva", "opacidad algorítmica" OR "caja negra" AND "derecho penal", y "AI Act" AND "dogmática jurídica". El período de revisión abarcó la producción científica y legislativa publicada entre

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

los años 2014 y 2026. Los criterios de inclusión comprendieron artículos de investigación dogmática en revistas arbitradas, monografías jurídicas, tesis doctorales, reglamentos internacionales y manuales técnicos de ciencias de la computación sobre gobernanza algorítmica y teoría del delito. Se excluyeron publicaciones no arbitradas, notas de prensa y ensayos especulativos sin rigor técnico o jurídico. Tras la depuración correspondiente, el corpus bibliográfico definitivo quedó integrado por 31 fuentes documentales clave.

Para transformar el análisis documental en hallazgos utilizables y sistemáticos, la investigación operacionalizó las variables cualitativas y categorías teóricas de la informática y el derecho sustantivo mediante la matriz conceptual sintetizada en la Tabla 1, la cual vincula los niveles de la IA y la opacidad algorítmica con sus respectivos indicadores de compatibilidad dogmática en el COIP y sus mecanismos de imputación propuestos:

Categoría Teórica / Nivel de IA	**Fenómeno Técnico-Informático**	**Implicación en la Teoría del Delito (COIP)**	**Mecanismo de Imputación Propuesto**
IA Débil o Estrecha *(Deep Learning)*	Opacidad algorítmica / Efecto de "Caja Negra" (*Black Box*)	Quiebra del principio de acción voluntaria; imposibilidad de adscribir dolo o culpa tradicional.	Imputación Objetiva Funcionalista / Infracción del deber objetivo de cuidado.
Esferas de Competencia *(Desarrollador / Diseñador)*	Generación de riesgos de origen en el diseño algorítmico y entrenamiento con datos sesgados.	Infracción de deberes de seguridad de origen ("seguridad por diseño").	Posición de garante del desarrollador / Artículo C (Entrenamiento negligente).
Esferas de Competencia *(Implementador / Usuario)*	Puesta en marcha operativa de sistemas de alto riesgo sin supervisión activa.	Omisión de controles y delegación ciego-tecnológica en entornos críticos.	Posición de garante institucional / Artículo B (Omisión de supervisión obligatoria).
Estándares Internacionales *(AI Act / UE)*	Clasificación de riesgos ex ante y ex post en sectores sensibles (salud, justicia).	Inexistencia de tipos penales automáticos; utilidad como norma técnica extrapenal de cuidado.	Criterio normativo de diligencia debida / Artículo A (Puesta en circulación sin certificación).

Tabla 1. Matriz Conceptual de Operacionalización Categorial entre la Informática y la Dogmática Penal
Nota: Elaboración Previa

Desde el punto de vista del método taxonómico utilizado, la articulación de una respuesta penalmente rigurosa exige descartar definiciones equívocas del término inteligencia artificial y recurrir a categorías teóricas consolidadas en las ciencias computacionales y el derecho de las nuevas tecnologías (Aguilar Campos & Alé Martínez, 2025; Russell & Norvig, 2022). En este sentido, la investigación adopta y sistematiza tres categorías fundamentales: a) la Inteligencia Artificial Débil o Estrecha, que representa el estado del arte de la tecnología disponible en el mercado para resolver tareas específicas y delimitadas sin autoconciencia, siendo reconducible al derecho

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

penal bajo la teoría del instrumento o la autoría directa o mediata (Morán Espinosa, 2021; Muñoz Vela, 2022); b) la Inteligencia Artificial Fuerte o General, entendida como una hipótesis teórica de sistemas con capacidades cognitivas multifuncionales equivalentes al razonamiento humano que actualmente carece de existencia material y cuya regulación penal directa pertenece al ámbito de la prospectiva doctrinal (Momblanc, 2024; Roxin, 2014); y c) la Inteligencia Artificial Superinteligente o Machina Sapiens, que hace referencia a entidades sintéticas teóricas que superarían exponencialmente el intelecto humano y cuya discusión sobre una supuesta personalidad electrónica es rechazada por la dogmática penal de corte garantista por desviar la atención de los problemas reales de negligencia y gestión del riesgo humano (Aguilar Campos & Alé Martínez, 2025; Silva Sánchez, 2020).

El procedimiento investigativo se ejecutó a través de tres fases sucesivas y complementarias que permitieron estructurar de forma integral el estudio. En la primera fase se realizó el diagnóstico y la sistematización dogmática de los vacíos normativos en el COIP (2014), identificando las brechas insalvables entre las disposiciones punitivas tradicionales y la opacidad de los algoritmos de aprendizaje profundo que rompen la previsibilidad ex ante exigida por la culpa y el dolo (Momblanc, 2024).

En la segunda fase se llevó a cabo el análisis comparado de estándares de riesgo, evaluando la aplicabilidad del enfoque preventivo del Reglamento (UE) 2024/1689 como insumo extrapenal para la determinación del deber objetivo de cuidado (Reglamento UE 2024/1689, 2024). Finalmente, en la tercera fase se formuló la propuesta normativa y el diseño de la respuesta funcional, estructurando un modelo de responsabilidad penal híbrida basado en el principio de control humano significativo, la delimitación estricta de esferas de competencia para desarrolladores, implementadores y usuarios, la tipificación de delitos específicos de negligencia tecnológica y la formulación de una hoja de ruta técnica e institucional para el Estado ecuatoriano (Pullas Tituaña, 2026; Rodas Izquierdo, 2026).

Resultados

Para articular una aproximación penalmente rigurosa a los desafíos tecnológicos actuales, la investigación evidencia la necesidad imperativa de evitar generalizaciones vagas sobre el término "inteligencia artificial" y recurrir de manera estricta a referentes teóricos consolidados tanto en las ciencias de la computación como en el derecho tecnológico (Aguilar Campos & Alé Martínez, 2025; Russell & Norvig, 2022).

De acuerdo con la doctrina especializada, los sistemas inteligentes deben clasificarse rigurosamente según sus capacidades cognitivas y

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

su nivel de autonomía, lo cual determina de forma directa la idoneidad y el alcance técnico-jurídico de las herramientas de imputación penal aplicables. Desde la teoría de sistemas computacionales y con un amplio respaldo de la dogmática jurídica (Morán Espinosa, 2021; Salardi, 2020), los resultados demuestran que se configuran tres categorías teóricas fundamentales de inteligencia artificial que condicionan el análisis normativo: la IA Débil o Estrecha, la IA Fuerte o General, y la IA Superinteligente o Machina Sapiens.

En cuanto a la primera categoría, la Inteligencia Artificial Débil o Estrecha comprende aquellos sistemas informáticos optimizados específicamente para la resolución de una tarea acotada y limitada, tales como el filtrado avanzado de correos electrónicos, el reconocimiento facial básico o los algoritmos de ajedrez computacional (Russell & Norvig, 2022). Estos sistemas operan de forma estrictamente reactiva y se desenvuelven dentro de un marco de reglas cerrado que ha sido previamente predefinido por el programador humano.

Al carecer por completo de autoconciencia, comprensión holística o voluntad propia, los resultados confirman que estos sistemas actúan como meros instrumentos o extensiones tecnológicas del ser humano, siendo perfectamente reconducibles en el ámbito penal bajo los criterios tradicionales de la autoría directa o de la autoría mediata por instrumento inanimado (Morán Espinosa, 2021).

Por otra parte, la Inteligencia Artificial Fuerte o General se configura como una hipótesis teórica de sistemas dotados de capacidades cognitivas multifuncionales que equivalen o emulan de manera integral la racionalidad humana (Morán Espinosa, 2021). Un sistema de esta naturaleza poseería autoconciencia, flexibilidad de aprendizaje autónomo y la aptitud inequívoca para comprender contextos abstractos y motivarse por directrices éticas o normativas. No obstante, al constituir un objeto recurrente de debate en la filosofía del derecho y la ética del desarrollo que actualmente carece de existencia material en el plano técnico, su regulación penal directa pertenece exclusivamente al ámbito de la prospectiva doctrinal y carece de operatividad práctica inmediata (Momblanc, 2024).

Finalmente, la Inteligencia Artificial Superinteligente o Machina Sapiens representa la categoría de entidades autónomas hipotéticas que no solo emularían la capacidad cognitiva del cerebro humano, sino que la superarían de manera exponencial en todos los órdenes imaginables del razonamiento, la creatividad y la interacción social (Morán Espinosa, 2021). Si bien diversos pensadores sugieren que el surgimiento de estas entidades justificaría en el futuro la creación de una 'personalidad electrónica' dotada de derechos y obligaciones —en una línea similar a las propuestas

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

iniciales debatidas en el Parlamento Europeo—, los hallazgos de la ciencia penal contemporánea ratifican que centrar el debate actual en la supuesta personalidad de la máquina desvía indebidamente la atención de los problemas reales de gestión del riesgo y negligencia humana (Aguilar Campos & Alé Martínez, 2025; Silva Sánchez, 2020).

Profundizando en el análisis empírico, los resultados determinan que el verdadero desafío para el Derecho Penal moderno radica en los sistemas de IA débil que operan mediante técnicas de Aprendizaje Profundo (deep learning), sustentadas en redes neuronales artificiales de múltiples capas que procesan volúmenes masivos de datos para extraer patrones complejos y adoptar decisiones autónomas (Russell & Norvig, 2022).

A diferencia de los programas secuenciales clásicos estructurados bajo la lógica condicional rígida del tipo 'si X, entonces Y', los modelos de deep learning no reciben instrucciones explícitas sobre cómo resolver un problema específico. En su lugar, el sistema ajusta internamente sus pesos y coeficientes matemáticos a través de miles de iteraciones sucesivas de entrenamiento, lo que le otorga la capacidad de encontrar soluciones y caminos de decisión originales que jamás fueron previstos ni anticipados por el programador humano (Salvadori, 2024).

Ante esta realidad técnica, el análisis exige diferenciar con precisión el concepto de opacidad respecto al de imprevisibilidad absoluta. Un modelo informático avanzado puede ser extremadamente difícil de explicar en cada una de sus operaciones matemáticas internas y, sin embargo, exhibir fallas estadísticamente conocidas, limitaciones documentadas o riesgos perfectamente identificables mediante pruebas de validación.

Para la valoración jurídica y penal, la cuestión decisiva no radica en si el programador anticipó la secuencia exacta de cálculos algorítmicos, sino en determinar si una persona situada razonablemente en su posición funcional y con la información disponible al momento del diseño o despliegue podía prever y evitar una clase relevante de daño (Momblanc, 2024). Dicha dificultad técnica inherente a las redes neuronales debe ser acreditada rigurosamente mediante peritajes especializados en el proceso judicial, y nunca presumida de forma automática por el solo uso de la tecnología.

Este proceso informático dinámico y autoajustable genera ineludiblemente el fenómeno técnico-empírico conocido como la 'caja negra' (black box) (Salvadori, 2024). La opacidad algorítmica implica que, si bien se pueden constatar con claridad los datos de entrada (inputs) y el resultado final de la decisión automatizada (outputs), resulta materialmente imposible para un observador humano —incluyendo al propio equipo de ingeniería y desarrollo que diseñó el software— reconstruir de manera íntegra el razonamiento

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

matemático interno que justificó una decisión concreta en un instante determinado (Salvadori, 2024).

Esta falta de visibilidad técnica rompe de forma radical con los estándares clásicos de la previsibilidad del resultado típico exigidos por el derecho penal, impidiendo atribuir el dolo (que demanda conocimiento y voluntad consciente del resultado) o la culpa tradicional (fundamentada en la previsibilidad objetiva del resultado lesivo) ante la ocurrencia de eventos dañosos (Muñoz Vela, 2022).

Para responder de forma coherente y armónica a la complejidad de la opacidad de la caja negra, los resultados demuestran que la ciencia del Derecho Penal debe abandonar la pretensión anacrónica de reconstruir nexos causales naturalistas y basar la atribución de responsabilidad en la dimensión normativa de la sociedad. En este sentido, la teoría de la imputación objetiva de base funcionalista se consolida como el eje indispensable y el aporte dogmático más significativo de la investigación para garantizar la tipicidad de los delitos algorítmicos sin alterar las bases de la culpabilidad individual (Roxin, 2014).

El causalismo clásico y la teoría de la equivalencia de condiciones fracasan de manera sistemática frente a la autonomía de la IA, puesto que si un algoritmo de deep learning adopta una decisión lesiva imprevista, la cadena causal física retrocedería indefectiblemente hacia el desarrollador que escribió el código años atrás o hacia el usuario que encendió el dispositivo, lo cual violaría flagrantemente el principio constitucional de culpabilidad al instaurar un régimen inaceptable de responsabilidad objetiva por el mero resultado (Roxin, 2014).

En consecuencia, los hallazgos confirman que la imputación objetiva opera como un filtro normativo adicional que exige identificar con precisión la conducta humana, el riesgo jurídicamente desaprobado y la materialización específica de dicho riesgo en el resultado lesivo (Pullas Tituaña, 2026). Siguiendo el enfoque normativo de Claus Roxin, un resultado típico solo es imputable a un sujeto si su conducta incrementó el riesgo de forma prohibida y el peligro se concretó en el daño (Roxin, 2014).

Así, la labor judicial frente a sistemas autónomos debe centrarse en verificar si el actor humano responsable actuó dentro de los márgenes de sus deberes objetivos de cuidado. Al mismo tiempo, bajo el concepto funcionalista del 'riesgo permitido' desarrollado por Günther Jakobs, el ordenamiento jurídico acepta la introducción de tecnologías peligrosas en atención a sus beneficios sociales, fijando como límite infranqueable el cumplimiento estricto de normas técnicas de seguridad y protocolos de testeo (Jakobs, 1997; Silva Sánchez, 2020).

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

Bajo este prisma analítico, la opacidad de la caja negra se transforma en una fuente normativa de riesgo especial, donde el sujeto que decide comercializar u operar una tecnología opaca asume una 'posición de garante' reforzada sobre dicha fuente de peligro (Jakobs, 1997). Si el sistema genera un daño típico debido a un entrenamiento deficiente con datos sesgados o por la omisión de supervisión activa, el garante no puede escudarse en la imprevisibilidad algorítmica, ya que al operar al margen de las directrices de seguridad ha quebrado su 'competencia por el rol' social (Pullas Tituaña, 2026).

Para estructurar operativamente este modelo, los resultados proponen delimitar las esferas de competencia organizativa en la cadena tecnológica: la competencia del desarrollador como garante de la seguridad por diseño mediante el uso de datos limpios y documentación rigurosa (Morte Ferrer, 2021); la competencia del implementador o usuario institucional como garante directo en la fase operativa, quien incurre en responsabilidad penal si delega ciegamente decisiones críticas sin supervisión humana activa (Pullas Tituaña, 2026); y la competencia del usuario final, limitada al respeto de los manuales técnicos oficiales. Este modelo funcionalista salvaguarda plenamente la seguridad jurídica y la dignidad humana en la sociedad digital (Aguilar Campos & Alé Martínez, 2025; Rodas Izquierdo, 2026).

En consonancia con lo anterior, los resultados del análisis comparado revelan una tendencia internacional clara hacia la promulgación de normativas vinculantes. La Unión Europea encabeza esta evolución con el Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial o AI Act), el cual adopta un enfoque preventivo clasificando los sistemas en niveles de riesgo inaceptable (prohibidos por atentar contra la dignidad), alto riesgo (sujetos a auditorías estrictas ex ante y ex post en sectores críticos como salud, justicia e infraestructuras) y riesgo limitado o mínimo (Reglamento UE 2024/1689, 2024).

Si bien este reglamento constituye un referente regulatorio extrapenal que define con precisión el estándar del deber objetivo de cuidado exigible a proveedores y usuarios —configurando una infracción grave si se comercializa software sin auditorías—, no crea automáticamente tipos penales en el Ecuador ni sustituye la comprobación de la culpa individual (Reglamento UE 2024/1689, 2024).

Por su parte, los Estados Unidos abordan la materia de manera fragmentada mediante la responsabilidad por productos defectuosos y la negligencia criminal en accidentes de vehículos autónomos (Bashayreh, 2021), un modelo casuístico que adolece de predictibilidad para la tradición jurídica ecuatoriana. En contraste, países asiáticos como Japón y Corea del Sur priorizan

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

certificaciones técnicas oficiales emitidas por agencias especializadas, utilizando su ausencia como baremo para presumir la culpa de los ejecutivos corporativos (Bashayreh, 2021).

En América Latina, el desarrollo es asimétrico: Brasil tramita proyectos inspirados en el AI Act, Chile incorpora neuroderechos, y Colombia cuenta con jurisprudencia vinculante de su Corte Constitucional que ratifica que la IA opera exclusivamente como herramienta de apoyo, estando vedada la sustitución del juicio ético y el razonamiento del juez, Souto Etchamendi (2025).

Finalmente, al confrontar los estándares internacionales con el ordenamiento nacional, los resultados exponen un desfase estructural profundo en el Código Orgánico Integral Penal, COIP (2014). El COIP se encuentra anclado en postulados dogmáticos estrictamente antropocéntricos que colapsan frente a la criminalidad algorítmica moderna (COIP, 2014). El artículo 18 define la infracción penal como conducta típica, antijurídica y culpable basada en la acción u omisión humana consciente, categoría que se quiebra ante la autonomía de los algoritmos de deep learning (Muñoz Vela, 2022).

Del mismo modo, el dolo y la culpa exigidos por los artículos 26 y 27 del COIP resultan de imposible concurrencia debido a la imprevisibilidad derivada de la caja negra. Adicionalmente, el COIP carece de definiciones técnicas sobre IA y restringe la responsabilidad de las personas jurídicas bajo un régimen de numerus clausus en su artículo 49, omitiendo la negligencia tecnológica (COIP, 2014).

Para superar esta obsolescencia, los resultados consolidan la propuesta de un modelo de responsabilidad penal híbrida fundamentado en el principio de control humano significativo, la tipificación de conductas negligentes específicas y la implementación obligatoria de registros de decisiones inalterables (logs de IA) respaldados por una hoja de ruta institucional en tres fases (Pullas Tituaña, 2026; Rodas Izquierdo, 2026).

Discusión

La contrastación exhaustiva de los estándares internacionales frente a la realidad legislativa ecuatoriana revela un desfase estructural profundo que no puede resolverse mediante interpretaciones analógicas simplistas. El Código Orgánico Integral Penal (COIP), promulgado en el año 2014, constituye un cuerpo normativo firmemente anclado en postulados dogmáticos pre-digitales y estrictamente antropocéntricos, lo que lo torna incapaz de responder con suficiencia a las complejas exigencias de imputación de la criminalidad algorítmica moderna (COIP, 2014). Tal como lo establecen las disposiciones generales del COIP, el artículo 18 tipifica que la infracción penal es una conducta típica, antijurídica y culpable (COIP, 2014), definiendo doctrinariamente a la conducta

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

como una acción u omisión humana voluntaria y consciente.

Sin embargo, los resultados del análisis demuestran que, cuando un sistema inteligente dotado de aprendizaje profundo adopta una decisión autónoma que desencadena un daño típico directo en los bienes jurídicos de terceros, la categoría tradicional del principio de acción se quiebra irremisiblemente. En este sentido, lo expresado por la doctrina especializada concuerda plenamente al señalar que no es posible identificar una acción humana voluntaria en el instante preciso de la consumación delictiva, toda vez que la máquina actúa de forma adaptativa y autónoma, sin una interferencia directa del programador o del usuario en el momento causal del resultado (Muñoz Vela, 2022).

Esta desconexión operativa encuentra sustento al examinar de manera integral el articulado del cuerpo punitivo nacional. Si bien el COIP cuenta con el artículo 22 referente a las conductas penalmente relevantes, y los artículos 23 y siguientes que regulan la acción, la omisión y las diversas modalidades de imputación, además de los artículos 26 y 27 que abordan respectivamente el dolo y la culpa (COIP, 2014), estas disposiciones normativas no obligan ni justifican buscar una voluntad delictiva en la estructura interna de la máquina.

Las ideas expuestas por los autores sostienen de manera concordante que la investigación penal bajo ningún concepto debe extraviarse intentando atribuir subjetividad a un algoritmo, sino que debe concentrarse con rigor en las conductas humanas anteriores o concurrentes, siempre y cuando exista un tipo penal aplicable y se satisfagan los requisitos de tipicidad. No obstante, la autonomía del software no suprime por sí misma la posible relevancia jurídica de una omisión de vigilancia, pero tampoco autoriza a presumir dicha omisión de manera objetiva (Pullas Tituaña, 2026; Rodas Izquierdo, 2026).

Profundizando en el análisis de los elementos subjetivos, la categoría de la culpabilidad en el COIP exige inexorablemente la presencia de dolo o culpa. El dolo requiere el conocimiento y la voluntad de realizar el resultado típico (Art. 26 COIP, 2014), lo cual representa una concurrencia de imposible materialización en la arquitectura inanimada y puramente matemática de un algoritmo informático. Como lo respaldan los hallazgos dogmáticos, intentar imputar dolo directamente a una Inteligencia Artificial constituye un sinsentido conceptual de proporciones graves que subvierte las bases del derecho penal de acto.

Por otra parte, la culpa (Art. 27 COIP, 2014) exige la infracción de un deber objetivo de cuidado fundamentada en la previsibilidad objetiva del resultado lesivo ex ante. Sin embargo, dado el

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

indómito carácter de caja negra característico del deep learning, el resultado de una decisión algorítmica automatizada resulta técnicamente imprevisible ex ante para el observador e incluso para su creador, lo que anula los presupuestos dogmáticos de la culpabilidad culposa clásica y genera un insalvable vacío de impunidad institucional, (Salvadori, 2024).

A esta aporía dogmática se suma el hecho de que el COIP adolece de una ausencia absoluta de definiciones legales y conceptos técnicos operativos indispensables para enmarcar jurídicamente las nuevas tecnologías. Nociones fundamentales de la informática contemporánea tales como 'sistema de inteligencia artificial', 'algoritmo autónomo', 'aprendizaje automático', 'aprendizaje profundo' o 'riesgo algorítmico' son completamente inexistentes en el texto penal sustantivo ecuatoriano. Esta carencia técnica impide que los tipos penales vigentes —como el homicidio culposo, las lesiones o los daños a la propiedad— puedan ser aplicados de manera típica e integrada a los siniestros inteligentes, dejando un peligroso margen al arbitrio discrecional del juzgador para interpretar la negligencia en el diseño, programación o entrenamiento de los sistemas (COIP, 2014; Muñoz Vela, 2022).

En el ámbito de la responsabilidad corporativa, si bien el artículo 49 del COIP introdujo la responsabilidad penal de las personas jurídicas en el ordenamiento ecuatoriano, esta figura dogmática se rige bajo el principio estricto de especialidad y numerus clausus (COIP, 2014). Esto implica que las empresas y corporaciones solo pueden ser procesadas penalmente por el listado taxativo de delitos expresamente previstos por el legislador en el texto del código. Debido a que el catálogo de delitos corporativos del COIP omite por completo figuras vinculadas con la negligencia tecnológica, las fallas graves de control por diseño, el entrenamiento de algoritmos con datos sesgados o la comercialización de software peligroso de alto riesgo, los daños sistémicos y masivos causados por IAs corporativas en sectores sensibles como el financiero, el médico o el de transporte quedan sustraídos por completo del alcance sancionatorio del derecho penal ecuatoriano (Aguilar Campos & Alé Martínez, 2025; Silva Sánchez, 2020).

No obstante, la postura doctrinal compartida ratifica que el artículo 49 del COIP contempla la responsabilidad corporativa bajo supuestos y condiciones específicas que exigen verificar una relación de beneficio y la actuación de personas vinculadas; de ahí no se sigue que cualquier falla de un producto inteligente genere automáticamente responsabilidad corporativa, ni que toda conducta empresarial riesgosa quede impune, siendo indispensable justificar con precisión qué lagunas subsisten frente a los tipos ya existentes (Roxin, 2014; Pullas Tituaña, 2026).

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

En el plano procesal y probatorio, la discusión pone de manifiesto que ni el COIP ni el Código Orgánico General de Procesos contemplan protocolos ni directrices adecuadas para la obtención, preservación y valoración de pruebas periciales de base algorítmica. El efecto de caja negra obstruye radicalmente la carga de la prueba para la Fiscalía General del Estado. En ausencia de una obligación legal que exija transparencia, trazabilidad técnica y explicabilidad en los sistemas de IA comercializados en el país, resulta de imposible ejecución pericial reconstruir ex post la cadena lógica de una decisión automatizada. Esto genera una asimetría cognitiva insalvable entre el equipo pericial del Estado y los desarrolladores corporativos de la tecnología, bloqueando la demostración fehaciente de la tipicidad objetiva en juicios penales complejos (Coronel Ojeda, 2025; Salvadori, 2024).

Las consecuencias directas de estos vacíos normativos se traducen en una profunda inseguridad jurídica que desprotege sistemáticamente los derechos y bienes jurídicos fundamentales de los ciudadanos ecuatorianos. Al suscitarse un daño a causa de un sistema inteligente autónomo en el territorio nacional, los operadores de justicia se ven enfrentados a un dilema inconstitucional ineludible: o bien aplican de forma analógica tipos penales tradicionales para forzar la culpabilidad del usuario o programador, vulnerando flagrantemente el principio de legalidad penal consagrado en el artículo 76 de la Constitución de la República del Ecuador (2008), o bien decretan la impunidad fáctica del hecho (COIP, 2014).

Esta desprotección jurídica resulta completamente inaceptable en un Estado constitucional de derechos y justicia (Art. 1, CRE, 2008), donde la máquina actúa de forma adaptativa y autónoma sin supervisión adecuada, evidenciando que las ideas de los autores convergen en la necesidad imperiosa de adecuar el ordenamiento jurídico a través de una reforma estructurada (Muñoz Vela, 2022; Rodas Izquierdo, 2026).

Por consiguiente, la pregunta decisiva en el debate dogmático no es si el sistema informático puede ser considerado autor de un delito —premisa que la investigación descarta categóricamente—, sino qué intervención humana jurídicamente relevante precedió al resultado lesivo. Un modelo automatizado puede producir una recomendación no anticipada por su operador; sin embargo, ello no elimina por sí mismo la necesidad de examinar con exhaustividad las decisiones humanas de diseño, selección de datos, validación, despliegue, mantenimiento y vigilancia. Cada una de estas etapas constituye un momento distinto de posible creación o incremento de un riesgo no permitido, que debe ser valorado estrictamente conforme al tipo penal aplicable y a los elementos de prueba

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

disponibles (Momblanc, 2024; Pullas Tituaña, 2026).

En este orden de ideas, los autores sostienen de manera concordante que la teoría de la imputación objetiva ofrece herramientas metodológicas sumamente valiosas para distinguir la causalidad naturalista de la atribución normativa mediante la creación de un riesgo jurídicamente desaprobado y su consiguiente materialización en el resultado. No obstante, el funcionalismo penal no reemplaza la tipicidad, ni exime de probar el elemento subjetivo, ni menoscaba las garantías procesales fundamentales.

Otras perspectivas dogmáticas relativas a la autoría, la participación, la imprudencia y la omisión deben contribuir de forma articulada a la solución del problema. En consecuencia, la hipótesis del estudio se sostiene en un sentido delimitado y prudente: el funcionalismo aporta criterios dogmáticos muy útiles para la delimitación del riesgo, pero no constituye una respuesta exclusiva ni habilita la creación de regímenes de responsabilidad penal objetiva (Jakobs, 1997; Roxin, 2014).

En cuanto al derecho comparado, se discute que si bien el Reglamento (UE) 2024/1689 aporta un referente internacional de incalculable valor para la gobernanza de sistemas de alto riesgo al establecer en su artículo 14 obligaciones de supervisión humana proporcionales y estándares de documentación rigurosos, Reglamento UE 2024/1689 (2024), se trata de una regulación extranjera con un régimen primordialmente administrativo. Dicha normativa europea no crea automáticamente tipos penales en el Ecuador ni determina por sí sola la culpabilidad individual o corporativa de un desarrollador. Su eventual recepción y adaptación al contexto nacional exige decisiones legislativas soberanas que guarden absoluta compatibilidad con los principios constitucionales de legalidad, proporcionalidad, lesividad y presunción de Inocencia (Bashayreh, 2021; Souto Etchamendi, 2025).

En materia probatoria, la discusión evidencia que los registros de operación (logs), las distintas versiones de los modelos algorítmicos, las pruebas de validación, los protocolos de mantenimiento y las decisiones documentadas de los operadores humanos contribuyen de manera decisiva a reconstruir la secuencia cronológica de los acontecimientos en un siniestro tecnológico.

Sin embargo, la doctrina ratifica que no corresponde calificarlos como una prueba tasada ni presumir de forma dogmática que todo sistema opaco permite una explicación íntegra de sus procesos internos. La valoración judicial debe realizarse estrictamente conforme a las reglas procesales aplicables, garantizando el derecho de contradicción, la actuación de peritos independientes y el resguardo legítimo de datos

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

personales y secretos industriales, (Barona Vilar, 2019; Salvadori, 2024).

Finalmente, la dimensión socio-jurídica de este debate adquiere una relevancia indiscutible. Cuando un error automatizado generado por la tecnología afecta derechos sensibles como la salud, la integridad o el acceso a servicios públicos, la persona perjudicada y la sociedad exigen vías efectivas de investigación judicial y reparación integral. Pero esa legítima exigencia de justicia no justifica bajo ningún concepto debilitar las garantías sust específicas de quien es investigado.

El desafío central para el legislador ecuatoriano consiste precisamente en evitar de forma simultánea la impunidad derivada de la opacidad tecnológica y el castigo injustificado por la mera pertenencia a una cadena de desarrollo. Una política criminal verdaderamente responsable debe fundamentarse en la prevención técnica, la supervisión administrativa constante y el fortalecimiento de las capacidades forenses institucionales (Aguilar Campos & Alé Martínez, 2025; Silva Sánchez, 2020).

Propuesta Normativa para la Integración de un Modelo de Responsabilidad Penal Híbrida en el Ordenamiento Jurídico Ecuatoriano

Frente a la evidente obsolescencia dogmática y legislativa del Código Orgánico Integral Penal (COIP), la presente investigación formula una propuesta técnica y normativa orientada a estructurar un modelo de responsabilidad penal híbrida. Este modelo no pretende incurrir en la ficción jurídica de dotar de personalidad a las máquinas, sino normativizar de manera efectiva el riesgo tecnológico, redefiniendo con precisión la posición de garante tanto a nivel humano como corporativo detrás de la creación, comercialización e implementación del código algorítmico (Pullas Tituaña, 2026; Rodas Izquierdo, 2026).

Como primer componente de la propuesta, se plantea reformar el COIP mediante la adición de una Disposición General que incorpore definiciones técnicas penales operativas, alineadas de manera armónica con los estándares internacionales del Reglamento (UE) 2024/1689 (2024). En este sentido, se define como Sistema de Inteligencia Artificial a aquellos sistemas computacionales basados en hardware o software que, a través del análisis automatizado de datos masivos y técnicas de aprendizaje autónomo, generan outputs tales como predicciones, decisiones, recomendaciones o contenidos con capacidad para influir de manera directa o indirecta en entornos físicos o virtuales, operando con diferentes niveles de autonomía.

Asimismo, dentro de esta misma disposición se conceptualiza el Riesgo Algorítmico Penalmente Relevante como la creación o el incremento desaprobado de un peligro no tolerable para los bienes jurídicos tutelados, originado directamente por la omisión de estándares técnicos de seguridad,

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

la introducción de sesgos graves de diseño o la falta de control efectivo durante las fases de diseño, entrenamiento, prueba o despliegue de un algoritmo autónomo.

Como segundo componente, se propone la incorporación formal al Título IV del COIP de la doctrina del 'Control Humano Significativo' como el principio rector y delimitador por excelencia de la imputación objetiva en delitos asistidos por tecnología autónoma. Este principio establece normativamente que la responsabilidad penal de base tecnológica siempre se anclará en un sujeto humano que, ocupando una posición de garante sobre la fuente de riesgo, posea la capacidad fáctica y técnica de ejercer una supervisión activa para monitorear el comportamiento operacional del algoritmo y verificar que se mantenga dentro de los límites del riesgo permitido; una intervención oportuna para modificar o corregir en tiempo real las decisiones del sistema inteligente ante fallas perceptibles; y una desconexión inmediata para activar paradas de emergencia o cortafuegos lógicos ante desviaciones imprevistas que amenacen con causar un daño típico (Morte Ferrer, 2021; Pullas Tituaña, 2026).

Como tercer componente, y sometiendo las propuestas estrictamente a los principios constitucionales de legalidad, lesividad, necesidad, proporcionalidad y última ratio —reconociendo que no toda omisión administrativa de auditoría merece una pena privativa de libertad y que la sanción a personas jurídicas no debe confundirse con la privación de libertad de personas naturales—, se plantea la tipificación penal de tres conductas delictivas específicas para su integración en el COIP.

En primer lugar, se formula el Artículo A, relativo a la puesta en circulación de sistemas autónomos de alto riesgo sin certificación de seguridad, el cual sanciona con pena privativa de libertad de uno a tres años a la persona natural o jurídica que comercialice, despliegue o ponga en circulación sistemas inteligentes autónomos catalogados de alto riesgo para la vida o la salud de las personas, omitiendo las auditorías algorítmicas previas y las certificaciones técnicas obligatorias exigidas por la autoridad estatal competente (Reglamento UE 2024/1689, 2024).

Asimismo, se propone el Artículo B concerniente a la omisión de supervisión algorítmica obligatoria, el cual sanciona con pena privativa de libertad de uno a tres años al operador o implementador institucional de un sistema autónomo de alto riesgo que, por negligencia grave, abandono inexcusable de funciones o impericia, omita supervisar el sistema de manera activa o ignore deliberadamente las alertas técnicas de seguridad, causando un resultado típico lesivo que hubiere podido ser evitado mediante el ejercicio

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

efectivo del control humano significativo (Pullas Tituaña, 2026).

Finalmente, se integra el Artículo C enfocado en el entrenamiento algorítmico negligente, el cual sanciona con pena privativa de libertad de dos a cinco años al desarrollador o empresa que, actuando con dolo o con negligencia grave, utilice conjuntos de datos con sesgos severos, datos alterados o incompletos para el entrenamiento de sistemas autónomos destinados a la toma de decisiones en ámbitos críticos como la salud, la justicia o la seguridad pública, derivando en discriminación sistémica o siniestros masivos, Salvadori (2024).

Como cuarto componente para superar procesalmente el obstáculo técnico de la opacidad de la caja negra, la propuesta de reforma penal introduce la obligación legal imperativa para todo implementador institucional y corporativo de sistemas autónomos de alto riesgo en el Ecuador de mantener un registro de decisiones inalterable e incorruptible (logs de decisiones de IA). Estos registros técnicos de control deberán registrar de forma automática y sistemática la totalidad de las decisiones operativas de la máquina y las interacciones de los operadores humanos, debiendo custodiarse bajo estrictas normas de cadena de custodia digital para actuar como un elemento de prueba tasada o pericial de referencia en la reconstrucción procesal de un siniestro inteligente (Coronel Ojeda , 2025; Salvadori, 2024).

Finalmente, ante la complejidad técnica de la materia y las evidentes limitaciones institucionales del Estado ecuatoriano, se propone una hoja de ruta estratégica estructurada en tres fases sucesivas de implementación progresiva. En primer lugar, se establece la Fase 1 a corto plazo e inmediata, la cual consiste en la ejecución de reformas dogmáticas específicas al COIP orientadas a definir legislativamente el control humano significativo, delimitar la posición de garante sobre tecnologías autónomas y ampliar la responsabilidad penal de las personas jurídicas al ámbito de la negligencia tecnológica y de gestión de bases de datos.

Posteriormente, se contempla la Fase 2 a mediano plazo en un horizonte de 24 meses, la cual comprende la creación formal de la Agencia de Regulación y Control Algorítmico (ARCA), concebida como una entidad de naturaleza técnica y administrativa encargada de emitir los estándares oficiales de riesgo permitido, auditar los sistemas de IA de alto riesgo, realizar peritajes forenses algorítmicos oficiales y certificar obligatoriamente los softwares de deep learning que pretendan ingresar al mercado nacional.

Finalmente, se proyecta la Fase 3 a largo plazo en un período de 48 meses, la cual se enfoca en la consolidación definitiva de un marco nacional integral de gobernanza algorítmica y ética del desarrollo tecnológico, plenamente armonizado con las directrices internacionales de la OCDE, el

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

Reglamento (UE) 2024/1689 y los convenios internacionales vigentes en materia de ciberseguridad y protección de datos personales.

Conclusiones

A partir del análisis dogmático y comparado desarrollado en esta investigación, es posible formular conclusiones de alto nivel de abstracción jurídica que responden de manera precisa, unívoca y concreta al objetivo central definido en el estudio, respaldando la hipótesis planteada en un sentido delimitado. De este modo, la imputación objetiva permite ordenar con eficacia el examen del riesgo creado por personas y organizaciones, aunque no resuelve por sí sola las dificultades de prueba ni sustituye los demás presupuestos ineludibles del delito, aportando un método de análisis individualizado que parte de los deberes concretos de cada actor y de la relación entre su incumplimiento y el resultado, lo cual ofrece una respuesta respetuosa del principio de culpabilidad frente a la inviabilidad de atribuir responsabilidad penal a la máquina o imponer sanciones automáticas a sus creadores.

En consonancia con lo anterior, se concluye que el dogma antropocéntrico que rige el principio de acción en el Código Orgánico Integral Penal (COIP) ecuatoriano es ontológicamente incapaz de procesar por sí solo el fenómeno de la autonomía algorítmica de aprendizaje profundo, generando un estado crónico de desprotección legal y vulnerabilidad para los bienes jurídicos fundamentales. Por consiguiente, la superación del causalismo naturalista mediante la adopción de la imputación objetiva funcionalista se configura como la única vía metodológicamente coherente para reconducir penalmente los siniestros causados por inteligencia artificial, logrando redefinir la culpabilidad sobre la base del quebrantamiento de deberes normativos humanos y no sobre una supuesta voluntad de la máquina.

Asimismo, se determina que la opacidad de la caja negra tecnológica no constituye una barrera técnica insalvable para el derecho penal contemporáneo, sino que debe ser normativizada adecuadamente como una fuente especial de riesgo, lo que impone una posición de garante reforzada a quien introduce dicha tecnología en el mercado, obligándolo a garantizar trazabilidad y explicabilidad bajo la sanción de incurrir en un riesgo jurídicamente desaprobado.

Para gestionar esta complejidad, la asignación de responsabilidad penal en la cadena tecnológica exige un modelo híbrido basado en esferas de competencia organizativa bien delimitadas, donde el desarrollador, el implementador y el usuario responden exclusivamente en la medida en que vulneren su rol normativo específico y su correspondiente deber de cuidado.

Adicionalmente, se establece que el criterio de control humano significativo actúa como el

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

principio limitador y de anclaje indispensable de la imputación penal, asegurando que la responsabilidad se mantenga siempre dentro del ámbito del control humano racional y respetando el principio de dignidad que impide sancionar penalmente a entidades carentes de consciencia.

Por último, se concluye que la tipicidad penal en la era digital resulta inviable sin una reforma estructural al COIP que incorpore definiciones técnicas operativas y tipifique delitos específicos de negligencia por diseño y omisión de supervisión, superando la ineficacia de la responsabilidad corporativa bajo el régimen restrictivo de numerus clausus, al tiempo que el debido proceso y la verdad procesal exigen una reforma instrumental del sistema de pruebas penales en el Ecuador que imponga la obligatoriedad de auditorías algorítmicas y la custodia de registros de decisión (logs), complementada con la formación técnico-jurídica urgente de los operadores de justicia para revertir la asimetría cognitiva frente a los desarrolladores de tecnología.

Referencias

Aguilar Campos, P., & Alé Martínez, V. (2025). Responsabilidad penal en la era de la inteligencia artificial: De la agencia humana a la autonomía de la machina sapiens. *Revista de Estudios de la Justicia*, (42), 153–183. Documento en línea. Disponible https://doi.org/10.5354/0718-4735.2025.77061

Bashayreh, M. H., Sibai, F., & Tabbara, A. (2021). Artificial intelligence and legal liability: towards an international approach of proportional liability based on risk sharing. Information & Communications Technology Law, 30, 169-192. Documento en línea. Disponible DOI: 10.1080/13600834.2020.1856025

Barona Vilar, S. (2019). Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: Revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia. *Revista Jurídica Digital UANDES*, 3(1), 1-25. Documento en línea. Disponible https://doi.org/10.24822/rjduandes.0301.1

CEPAL (2025) Estudio Económico de América Latina y el Caribe, 2024. Resumen ejecutivo. Versión accesible. CEPAL. Documento en línea. Disponible https://www.cepal.org/es/publicaciones/81301-estudio-economico-america-latina-caribe-2024-resumen-ejecutivo-version-accesible

Concha Flores, L. F. (2024). Inteligencia Artificial, enfoque de riesgos y responsabilidad civil. Aspectos centrales para una razonabilidad práctica. Sapientia Iuris, 1, 140–169. Documento en línea. Disponible https://doi.org/10.5281/zenodo.14735552

Constitución de la República del Ecuador. (2008). Registro Oficial No. 449, 20 de octubre de 2008. Documento en línea. Disponible https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Coronel Ojeda, E. I. (2025). La arquitectura de la justicia penal digital en Ecuador. En Justicia penal iberoamericana: Procesos y digitalización (pp. 95-120). Dykinson. Documento en línea. Disponible https://international.vlex.com/vid/capitulo-5-arquitectura-justicia-1102897305

Código Orgánico Integral Penal [COIP]. (2014). Registro Oficial Suplemento No. 180, 10 de febrero de 2014. Documento en línea. Disponible https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_con_judi_c%C3%B3d_org_int_pen.pdf

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

Instituto Nacional de Estadística y Censos (INEC). (2024). Rendición de cuentas 2024: Estadísticas Ecuador en cifras. Dirección de Difusión y Comunicación, INEC. Documento en línea. Disponible https://www.ecuadorencifras.gob.ec/institucional/rendicion-de-cuentas-2024-fase-2/

Jakobs, G. (1997). Derecho Penal: Parte General. Fundamentos y Teoría de la Imputación (2ª ed.). Marcial Pons. Documento en línea. Disponible https://proyectozero24.com/wp-content/uploads/2021/09/Jakobs-1997-Derecho-Penal.-Parte-General.pdf

Momblanc, L. C. (2024). Inteligencia Artificial y Derecho Penal. ¿Será necesario un Nuevo Concepto de Delito? Lex, 22(34), 185–209. Documento en línea. Disponible http://dx.doi.org/10.21503/lex.v22i34.2789

Morte Ferrer, R. (2021). Valoraciones éticas para una inteligencia artificial adecuada a la privacidad. Arbor, 197(802), a625. Documento en línea. Disponible https://doi.org/10.3989/arbor.2021.802006

Morán Espinosa, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 15(48), 123-145. Documento en línea. Disponible https://doi.org/10.35487/rius.v15i48.2021.706

Muñoz Vela, J. M. (2022). Inteligencia artificial y responsabilidad penal. Derecho Digital e Innovación: Digital Law and Innovation Review, (11), 75-92. Documento en línea. Disponible https://www.aranzadilaley.es/tienda/derecho-digital-e-innovacion-digital-law-and-innovation-review?srsltid=AU7gw4UyHfbH0nesrgcjDR9NRQp5TD25Vilfq33YxpBEiJRmboxQK2v8

Pullas Tituaña, O. A. (2026). Imputación objetiva en delitos cometidos mediante inteligencia artificial en Ecuador (Trabajo de integración curricular). Universidad Tecnológica Indoamérica. Documento en línea. Disponible https://repositorio.uti.edu.ec/items/7ac34855-0d65-439d-9fd0-c763b3959cde

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial. (2024). Diario Oficial de la Unión Europea, L 2024/1689, 12 de julio de 2024. Documento en línea. Disponible http://data.europa.eu/eli/reg/2024/1689/oj

Rodas Izquierdo, J. P. (2026). Inteligencia Artificial y Responsabilidad Penal. Nuevas Fronteras en la Imputación de Delitos (Tesis de doctorado). Secretaría de Educación del Estado de Zacatecas / UNICAP. Documento en línea. Disponible http://repositorio.unicap.edu.mx/id/eprint/312

Roxin, C. (1997). Derecho Penal: Parte General. Tomo I: Fundamentos. La Estructura de la Teoría del Delito (D. Luzón Peña, M. Díaz y García Conlledo, & J. de Vicente Remesal, Trads.). Civitas. Documento en línea. Disponible http://www.editorialcivitas.es/libros/9788447008704/

Roxin, C. (2014). Derecho Procesal Penal (J. Maier, Trad.; 25ª ed.). Editores del Puerto. (Obra original publicada en 1997). Documento en línea. Disponible https://catalogo.uexternado.edu.co/bib/248524

Russell, S., & Norvig, P. (2022). Inteligencia Artificial: Un Enfoque Moderno (4ª ed.). Pearson. Documento en línea. Disponible https://luismejias21.wordpress.com/wp-content/uploads/2017/09/inteligencia-artificial-un-enfoque-moderno-stuart-j-russell.pdf

Salvadori, I. (2024). Cibercrimen y uso ilícito de la inteligencia artificial: Retos y desafíos del derecho penal. En Cibercrimen: Tendencias y desafíos actuales. Proyectos de Generación de Conocimiento. Documento en línea. Disponible https://boe.es/biblioteca_juridica/pdf/PUB-DP-2025-361.pdf

Salardi, S. (2020). Robótica e inteligencia artificial: retos para el derecho. *Derechos y Libertades: Revista de Filosofía del Derecho y Derechos Humanos*, (42), 203–232. Documento en línea. Disponible https://doi.org/10.14679/1158

Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional

ISSN: 2665-0398

Silva Sánchez, J. M. (2020). La expansión del Derecho Penal: Aspectos de la política criminal en las sociedades postindustriales (3ª ed.). B de F. Documento en línea. Disponible https://www.editorialbdef.com.ar/productos/silva-sanchez-jesus-maria-la-expansion-del-derecho-penal-aspectos-de-la-politica-criminal-en-las-sociedades-postindustriales/

Souto Etchamendi, M. (2025). La tecnología y su adaptación a la función judicial desde la perspectiva de Uruguay. En Justicia penal iberoamericana: Procesos y digitalización (pp. 121-146). Dykinson. Documento en línea. Disponible https://international.vlex.com/vid/capitulo-8-tecnologia-adaptacion-1102897353

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 15, Año: 2026 (Julio 2026 - Diciembre 2026)
Esta obra está bajo una Licencia Creative Commons Atribución No Comercial-Sin Derivar 4.0 Internacional