UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

El uso malicioso de inteligencia artificial como propuesta de tipo penal

AUTOR:

Choez Peñafiel Ronald Felipe

Trabajo de titulación previo a la obtención del grado de

ABOGADO

TUTOR:

Ab. Carrión Carrión Pablo

GUAYAQUIL, ECUADOR

2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por, **Choez Peñafiel, Ronald Felipe**, como requerimiento para la obtención del Título de Abogado.

TUTOR

f. _____

Ab. Pablo Carrión Carrión

DIRECTORA DE LA CARRERA

_____

Dra. Nuria Pérez Puig-Mir, PhD

Guayaquil, a los 19 días de agosto de 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS.

CARRERA DE DERECHO.

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Choez Peñafiel, Ronald Felipe**

DECLARO QUE:

El Trabajo de Titulación **EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL,** previo a la obtención del Título de Abogado, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil,

EL AUTOR

f. _____

Choez Peñafiel, Ronald Felipe

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

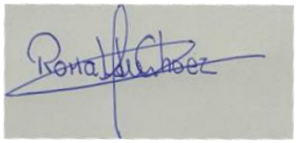
AUTORIZACIÓN

Yo, **Choez Peñafiel, Ronald Felipe**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación **EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 19 días de agosto de 2025

EL AUTOR



f. _____

Choez Peñafiel, Ronald Felipe

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
REPORTE COMPILATIO

CERTIFICADO DE ANÁLISIS
magister

EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL II

3% Textos sospechosos

6% Similitudes (ignorado)
1% similitudes entre comillas
0% entre las fuentes mencionadas
1% Idiomas no reconocidos
2% Textos potencialmente generados por la IA

Nombre del documento: EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL II.docx
ID del documento: b02bf8e6668c676b50d6e1ff19c8c4f59b8a2711
Tamaño del documento original: 397,01 kB

Depositante: Pablo Javier Carrión Carrión
Fecha de depósito: 25/8/2025
Tipo de carga: interface
fecha de fin de análisis: 25/8/2025

Número de palabras: 9124
Número de caracteres: 59.421

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	doi.org | Evolución del concepto de Inteligencia Artificial (IA) y sus consecuencias j... https://doi.org/10.5944/rduned.35.2025.45884 1 fuente similar	2%		Palabras idénticas: 2% (138 palabras)
2	dspace.unl.edu.ec | La Sanción Penal a las Personas Jurídicas establecida en el C... http://dspace.unl.edu.ec/jspui/handle/123456789/17534 14 fuentes similares	2%		Palabras idénticas: 2% (146 palabras)
3	assets.kpmg.com https://assets.kpmg.com/content/dam/kpmg/es/pdf/2024/01/claves-nuevo-reglamento-IA.pdf 1 fuente similar	1%		Palabras idénticas: 1% (123 palabras)
4	sites.google.com | IA Responsable - Principios Éticos https://sites.google.com/view/ia-responsable/página-principal/principios-éticos 6 fuentes similares	1%		Palabras idénticas: 1% (109 palabras)
5	www.dspace.uce.edu.ec | Problemática de la imputación del resultado en las de... http://www.dspace.uce.edu.ec/handle/25000/27572 14 fuentes similares	1%		Palabras idénticas: 1% (122 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales

f. _____

Choez Peñafiel, Ronald Felipe

f. _____

DEDICATORIA

A Dios, primeramente, por su infinita misericordia por jamás soltarme y ser esa guía que siempre necesite, a mi mamá por su apoyo constante sin ella no fuera posible, por su cariño y dedicación y ser un ejemplo en mi vida.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA,

CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

_____

(NOMBRES Y APELLIDOS)

Oponente

_____

Ab. Xavier Zavala Egas

Decano

_____

Abg. Ángela Paredes, Mgs.

Coordinadora de Unidad de Titulación

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia

Carrera: Derecho

Período: UTE A 2025

Fecha: 19 de Agosto de 2025

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado **EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL**, elaborado por el estudiante, certifica que durante el proceso de acompañamiento dicha estudiante ha obtenido la calificación de 9/10 lo cual la califica como ***APTA PARA LA SUSTENTACIÓN***

f. _____

Ab. Pablo Carrión Carrión

ÍNDICE

INTRODUCCIÓN. 2

CAPÍTULO I 4

LA REGULACIÓN DE LA IA EN EL ECUADOR 4

1.2. Tipos de sistemas de IA y su uso en la sociedad 5

1.3. Usos ilegales y antiéticos de la inteligencia artificial 7

2. El Reglamento de Inteligencia Artificial de la Unión Europea como pionera en regulación internacional sobre IA 8

3. El estado de la técnica de la IA y su nexo con el derecho penal 9

4. El problema jurídico 10

5. Bienes jurídicos protegidos en la Constitución de la República del Ecuador en relación al uso de IA 12

6. Principio de legalidad y taxatividad penal 13

7. Tipificación penal actual en el COIP y su aplicación a conductas con IA 14

8. Límites de aplicación de figuras penales tradicionales a nuevos escenarios tecnológicos 14

CAPÍTULO II 16

Propuesta de incorporación de un tipo penal sobre el uso malicioso de IA en el COIP 16

9. Fundamento jurídico de la necesidad de un nuevo tipo penal 16

9.1. La evolución tecnológica y la responsabilidad penal 16

9.2. El riesgo de impunidad ante lagunas legales 17

10. Elementos estructurales del tipo penal propuesto 17

10.1. Sujeto activo y pasivo 18

10.2. Conducta típica: diseño, uso y supervisión dolosa o culposa 19

10.3. Resultado y nexo de causalidad 21

11. Criterios para la determinación de la sanción penal 22

12. Consideraciones sobre la responsabilidad de personas jurídicas 23

13. Derecho Comparado 24

13.1. Perú 24

13.2. Estados Unidos 26

14. Propuesta de solución al problema jurídico 27

CONCLUSIONES 29

REFERENCIAS 30

RESUMEN

El presente trabajo de titulación analiza la urgente necesidad de adaptar el derecho penal ecuatoriano a los desafíos que plantea el uso indebido de tecnologías emergentes, particularmente la inteligencia artificial (IA). El problema jurídico central radica en que el Código Orgánico Integral Penal (En adelante, COIP) no contempla de forma específica la punibilidad de conductas maliciosas cometidas mediante IA, lo cual genera vacíos normativos que pueden dejar impunes actos que atentan contra bienes jurídicos fundamentales que reconoce el Estado ecuatoriano como la intimidad, la seguridad pública y la integridad de las personas. El trabajo propone la incorporación de un tipo penal autónomo que sancione a la persona natural o jurídica que, con dolo o culpa, en el diseño, uso o supervisión de sistemas automatizados, cause daños a personas o bienes. Se justifica esta necesidad en la naturaleza evolutiva de la IA y su capacidad de generar conductas lesivas difíciles de prever bajo los tipos penales tradicionales. Además, se realiza un análisis comparativo con legislaciones extranjeras, destacando avances significativos en Francia y Estados Unidos, donde ya se han tipificado penalmente conductas como la creación y difusión de *deepfakes* o imágenes generadas con IA sin consentimiento, sentando precedentes útiles para el contexto ecuatoriano. Se concluye recomendando reformas al COIP para cubrir las lagunas expuestas.

Palabras Clave: Inteligencia artificial, principio de legalidad, derecho penal, estado de la técnica de la IA.

ABSTRACT

This degree thesis analyzes the urgent need to adapt Ecuadorian criminal law to the challenges posed by the improper use of emerging technologies, particularly artificial intelligence (AI). The central legal issue lies in the fact that the Comprehensive Organic Criminal Code (From now on, COIP) does not specifically address the ability of sanctioning malicious acts committed through AI, resulting in legal gaps that may leave unpunished behaviors that threaten fundamental legal interests recognized by the Ecuadorian State, such as privacy, public safety, and personal integrity. The study proposes the incorporation of an autonomous criminal offense to sanction natural or legal persons who, through intent or negligence, cause harm to individuals or property during the design, use, or oversight of automated systems. This need is justified by the evolving nature of AI and its potential to generate harmful behaviors that are difficult to foresee under traditional criminal classifications. A comparative analysis is also conducted with foreign legislation, highlighting significant advances in France and the United States, where criminal provisions already address conduct such as the creation and dissemination of deepfakes or AI-generated images without consent, offering useful precedents for the Ecuadorian context. The study concludes by recommending reforms to the COIP to address the identified gaps.

Keywords: Artificial intelligence, principle of legality, criminal law, state of the art in AI.

INTRODUCCIÓN.

En la actualidad, la inteligencia artificial (IA) emerge como una tecnología estratégica del siglo XXI que promete transformar radicalmente sectores como la salud, la educación, la industria y las comunicaciones. Como observa Muñoz Vela (2021), "la IA integra un conjunto de tecnologías que promete cambiar el mundo que conocemos y aportar un enorme valor al ser humano, si bien conlleva distintos riesgos y retos". Esta revolución tecnológica genera grandes beneficios –por ejemplo, facilita diagnósticos médicos avanzados o la automatización de procesos industriales– pero simultáneamente plantea dilemas sociales y éticos inéditos.

Según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2024), el rápido auge de la IA "ha generado nuevas oportunidades a nivel global: desde facilitar los diagnósticos de salud hasta posibilitar las conexiones humanas a través de las redes sociales, así como aumentar la eficiencia laboral mediante la automatización de tareas". Sin embargo, estos avances "plantean profundos dilemas éticos". La IA, sin unas barreras normativas claras, puede reproducir prejuicios sociales y amenazar derechos humanos fundamentales. De hecho, la ONU ha subrayado la necesidad de una "brújula ética" para orientar el desarrollo de estas tecnologías y mitigar sus riesgos en derechos humanos.

Jurídicamente, el uso de la IA plantea importantes desafíos. La capacidad de crear contenidos falsos (imágenes, audios o videos), de tomar decisiones autónomas o de procesar grandes volúmenes de datos personales de forma automatizada abre múltiples preguntas legales: ¿cómo se protege la dignidad, la privacidad y la seguridad de las personas frente a sistemas inteligentes? ¿Cómo encaja la IA en el derecho penal tradicional?

La resolución del Parlamento Europeo (2021) advierte que el avance exponencial de la IA, si bien "la convierte en una de las tecnologías estratégicas del siglo XXI", también implica "enormes riesgos para los derechos fundamentales y las democracias basadas en el Estado de Derecho". Esta doble naturaleza (potencial transformador y simultáneamente riesgoso) resalta la importancia social y jurídica del tema: proteger bienes jurídicos (vida, libertad, privacidad) frente a conductas maliciosas mediadas por IA.

En el ámbito social, la IA ya está siendo aprovechada incluso por delincuentes. Reportes recientes alertan que los usos ilegales de IA están creciendo alarmantemente. Un artículo de prensa destaca que, en solo un año, los casos de fraude asociados a *deepfakes* (audios o videos falsos generados por IA) "se multiplicaron por diez", y la pornografía no consentida mediante estas técnicas "se duplica cada seis meses" (Peralta, 2023).

Las empresas de ciberseguridad advierten que la IA permite fabricar estafas sofisticadas (clonación de voces de familiares, falsos presidentes ejecutivos de empresas hablando en videos, etc.) y pornografía abusiva con rostros de víctimas sin su consentimiento. En suma, los delitos tradicionales se potencian con herramientas de IA que aumentan su alcance y eficacia.

Este contexto tecnológico y criminal evidencia la urgencia de una respuesta normativa. El Derecho penal debe considerar si los delitos cometidos mediante o con apoyo de IA quedan adecuadamente tipificados. En el caso ecuatoriano, no existe actualmente una figura penal específica para el "uso malicioso de IA", y el COIP sólo alude de forma genérica a medios informáticos o tecnológicos.

Dado el crecimiento global de la IA, legisladores y académicos coinciden en la necesidad de evaluar cómo el marco legal –local e internacional– está abordando este reto. En el plano internacional, por ejemplo, la Unión Europea ha adoptado el Reglamento (UE) 2024/1689, el primer marco jurídico global en materia de IA, con un enfoque basado en riesgos.

De modo similar, organismos multilaterales como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura en la Recomendación sobre la ética de la IA (2024) han solicitado marcos éticos y jurídicos para la IA. En Ecuador, este escenario pone de relieve tanto el potencial de la IA para el desarrollo como sus desafíos jurídicos: de aquí surge la propuesta de tipificar penalmente los usos maliciosos de IA, tema central del presente trabajo.

CAPÍTULO I

LA REGULACIÓN DE LA IA EN EL ECUADOR

1. Conceptualización de la inteligencia artificial

1.1. Definición

La inteligencia artificial es un concepto amplio que carece de una única definición consensuada, pero suele describirse como el campo tecnológico dedicado a diseñar sistemas capaces de procesar información de modo similar a un comportamiento inteligente (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2024).

La Comisión Europea (2018) la define como aquellos "sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos".

Luego, el Parlamento Europeo y el Consejo de la Unión Europea extendieron la concepción de la IA, enmarcándolo de la siguiente manera en el Reglamento UE 2024/1689 dentro de su Art. 3 numeral 1:

> […] un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales (Reglamento UE 2024/1689, 2024).

Además, a partir de la promulgación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, en el régimen de este sector de derecho comunitario se distingue entre diversos tipos o niveles de IA según su complejidad y autonomía. Por ejemplo, se habla de IA débil (estrecha) cuando un sistema realiza tareas específicas (reconocimiento de voz, recomendaciones, chatbots), frente a una hipotética IA fuerte (general) que alcanzaría capacidades intelectuales humanas en cualquier dominio (Reglamento (UE) 2024/1689, 2024). También se clasifican

sistemas de IA por su técnica: algunos utilizan lógica simbólica y reglas explícitas; otros se basan en grandes conjuntos de datos y modelos estadísticos (p. ej. algoritmos de aprendizaje supervisado o no supervisado). Desde la perspectiva funcional, existen sistemas de IA de percepción (visión por computador, reconocimiento de voz), de aprendizaje (algoritmos que mejoran con experiencia) y de agentes autónomos (robots, vehículos inteligentes) dotados de cierto grado de independencia.

Tal como plantea la UE, una característica definitoria de la IA es su capacidad de inferir "predicciones, contenidos, recomendaciones o decisiones" a partir de datos complejos (Reglamento (UE) 2024/1689, 2024). Esto implica que las respuestas de un sistema de IA no se programan explícitamente sino que el sistema las aprende de los datos de entrenamiento, lo que a su vez genera incertidumbres sobre su razonamiento interno. En resumen, la IA abarca una variedad de sistemas computacionales con distinto grado de autonomía e inteligencia aparente, cuya definición precisa varía según el contexto tecnológico o científico, pero siempre remite a la idea de procesar información de manera "inteligente" en algún sentido.

1.2. Tipos de sistemas de IA y su uso en la sociedad

Los sistemas de IA se pueden clasificar de diversos modos en base a diseño o uso. Una de las distinciones principales se produce entre los sistemas IA basados exclusivamente en el sistema que tengan en su base de datos, y por otro, de los sistemas de aprendizaje automática, donde a partir de datos de origen externo el algoritmo se retroalimenta y genera nuevo contenido. En este sentido, las redes neuronales artificiales y el aprendizaje profundo denominado deep learning han ganado protagonismo, al impulsar avances en reconocimiento de imágenes, procesamiento del lenguaje y juego estratégico. Otra categoría incluye sistemas autónomos o agentes inteligentes, que perciben su entorno, procesan esa información y actúan de modo independiente según objetivos programados.

En cuanto a su aplicación, la IA permea múltiples ámbitos sociales. En el sector salud, existen sistemas de IA que analizan imágenes médicas para apoyar diagnósticos o que realizan seguimientos predictivos de enfermedades. En la industria y manufactura, la robótica inteligente y la automatización basada en IA optimizan procesos productivos, logística y mantenimiento predictivo. En el ámbito de servicios se usan *chatbots* y asistentes virtuales para atención al cliente, -como Siri y Alexa- así

como sistemas de recomendación de contenidos en plataformas digitales. En el transporte, desde hace años se desarrollan vehículos autónomos que integran visión artificial y aprendizaje para conducir sin intervención humana. Además, la IA está presente en la gobernanza de datos de grandes empresas tecnológicas: algoritmos determinan qué noticias o anuncios se muestran a cada usuario en redes sociales, y sistemas de IA analizan el comportamiento en línea para fines de mercadeo o seguridad.

Por su parte, el sector financiero emplea IA para *trading algorítmico,* para la predicción de mercados y detección de fraudes en tiempo real. En seguridad pública, algunos gobiernos usan herramientas de análisis predictivo basadas en IA para identificar patrones de criminalidad o mapear redes delictivas. Por ende, el progreso de la IA ha venido ofreciendo beneficios que parten desde la conectividad social hasta la eficiencia en el mundo económico. Estos usos cotidianos de la IA subrayan que ningún sector escapa a su influencia: nuestro día a día ya está lleno de asistentes digitales, sensores inteligentes y servicios automatizados que aprenden y se adaptan mediante IA.

En la sociedad actual, pues, la IA existe en casi todos los campos. Ejemplos incluyen la detección de fraude electrónico mediante algoritmos que analizan transacciones bancarias, la generación de imágenes sintéticas y deepfakes basados en redes generativas adversariales, los filtros de spam y seguridad en correo electrónico impulsados por aprendizaje automático, y los prototipos de uso militar a través de drones autónomos o sistemas de identificación de blancos. Cada tipo de sistema IA interactúa con la sociedad de formas distintas: los *big data* y aprendizaje automático posibilitan el análisis de poblaciones enteras para políticas públicas, mientras que la robótica alcanza el entorno físico. En definitiva, los sistemas de IA en uso hoy tienen capacidades muy distintas, desde resolver problemas complejos sin supervisión humana hasta realizar tareas simples de forma automatizada, lo cual multiplica las oportunidades pero también los vectores de riesgo social. Esta variedad de sistemas subraya que cualquier examen legal de la IA debe considerar no una sola tecnología, sino un espectro amplio de sistemas y aplicaciones.

1.3. Usos ilegales y antiéticos de la inteligencia artificial

Junto a sus aplicaciones legítimas, la IA facilita nuevos modos delictivos y ha abierto escenarios éticamente cuestionables. Entre los usos ilegales que preocupan a expertos figuran los siguientes: la creación de deepfakes para estafar o difamar, la suplantación de identidad mediante clonación de voces o rostros, y la automatización de ataques cibernéticos. También pueden mencionarse la generación de campañas de desinformación automatizada, como redes de bots IA que difunden noticias falsas, y el uso de IA para violentar la privacidad mediante sistemas de reconocimiento facial masivo sin consentimiento. En el ámbito económico, delincuentes emplean IA para elaborar cartas de phishing muy creíbles o para realizar fraudes financieros complejos. En escenarios más extremos, se habla de armas autónomas (drones o robots letales con IA) que presentarían un grave dilema ético y penal.

Diversos estudios y reportes dan cuenta de este fenómeno creciente. Un artículo de El País señaló que la IA está siendo “adoptada por delincuentes” (Peralta, 2024) y la pornografía *deepfake,* manifestó el autor que se duplica cada seis meses, mientras los fraudes asociados a IA “se multiplicaron por diez” entre 2022 y 2023 . En muchos casos, la IA amplifica delitos ya conocidos: un fraude bancario tradicional se vuelve más creíble al usar una voz clonada por IA; un atentado informático puede causar mayor daño si es orquestado por un algoritmo que aprende de los fallos de seguridad. Por otro lado, también surgen usos antiéticos que, aunque no sean directamente punibles, plantean dilemas de derechos: por ejemplo, emplear IA para crear perfiles psicológicos secretos de personas basándose en sus hábitos en redes sociales (violando su privacidad), o usar algoritmos sesgados que discriminen a poblaciones minoritarias en toma de decisiones que violen el derecho a la igualdad real, formal y no discriminación.

La ha generado nuevas oportunidades a nivel global: desde facilitar los diagnósticos de salud hasta posibilitar las conexiones humanas a través de las redes sociales, así como aumentar la eficiencia laboral mediante la automatización de tareas Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2024) enfatiza estos riesgos éticos de la IA: advierte que:

> La tecnología de inteligencia artificial aporta grandes beneficios en muchos ámbitos, pero sin unas barreras éticas corre el riesgo de reproducir los prejuicios y la discriminación del mundo real, alimentar las divisiones y amenazar los derechos humanos y las libertades fundamentales.

En consecuencia, la frontera entre uso ético e ilegítimo de la IA puede volverse difusa si no existe un control normativo. Casos recientes ponen en relieve estas tensiones: por ejemplo, ataques de *deepfake* pornográfico han acabado en extorsión y explotación de víctimas, siendo la IA la herramienta "devastadora para ataques personales" (Peralta, 2024). En resumen, los usos criminales y antiéticos de la IA –desde el fraude sofisticado hasta la violación de la dignidad humana mediante pornografía no consentida– han crecido de forma alarmante, lo que subraya la relevancia de analizar cómo el derecho penal puede y debe responder a ellos.

2. El Reglamento de Inteligencia Artificial de la Unión Europea como pionera en regulación internacional sobre IA

El Reglamento (UE) 2024/1689, también llamado Ley de Inteligencia Artificial de la UE, constituye la primera regulación integral de la IA a nivel global. Aprobado en junio de 2024, introduce un marco común para el desarrollo y uso de sistemas de IA en la Unión Europea. La Comisión Europea (2024) enfatiza que se trata del "primer marco jurídico global en materia de IA en todo el mundo" , lo que subraya su carácter pionero. Este reglamento adopta un enfoque basado en riesgos, estableciendo niveles diferenciados: desde usos "de riesgo inaceptable" (totalmente prohibidos) hasta usos de riesgo bajo. En particular, prohíbe expresamente aplicaciones consideradas contrarias a la ética y la seguridad: por ejemplo, se prohíbe la IA para identificación biométrica remota sin consentimiento, reconocimiento de emociones o categorización por características personales.

El texto del reglamento exige que los sistemas de IA de alto riesgo (aquellos que impactan directamente la salud, la seguridad o los derechos fundamentales) cumplan exigencias estrictas antes de su comercialización: deben someterse a evaluación y mitigación de riesgos, transparencia sobre su funcionamiento, supervisión humana y sistemas de vigilancia del post-comercialización. Asimismo, establece responsabilidades legales y multas severas por incumplimiento. En palabras

de la Comisión, el objetivo es "garantizar un nivel elevado y coherente de protección de los intereses públicos" (Reglamento (UE) 2024/1689, 2024) en relación con la salud, seguridad y derechos . Además, impone transparencia en aplicaciones de IA de uso cotidiano: por ejemplo, un *chatbot* debe advertir al usuario que no es humano, de modo que este pueda tomar decisiones informadas. En suma, el reglamento UE 2024/1689 sienta un modelo regulatorio global: es vinculante para todos los Estados miembros desde 2025, y establece referencias internacionales en cuanto a principios de transparencia, rendición de cuentas y privacidad, que influyen en el debate mundial. Su relevancia radica en haber tipificado formalmente prácticas de IA inaceptables y en insistir en la tutela de derechos fundamentales, lo que alimenta la discusión en otros ordenamientos –incluido el ecuatoriano– sobre la necesidad de normas específicas para la IA.

3. El estado de la técnica de la IA y su nexo con el derecho penal

El estado actual de la técnica en IA muestra sistemas cada vez más autónomos y sofisticados, lo que interactúa directamente con la función del derecho penal. Por ejemplo, la IA es utilizada por autoridades policiales y judiciales en tareas de investigación: desde el uso de software de reconocimiento facial para identificar sospechosos en bases de datos, hasta análisis automáticos de grandes volúmenes de información para predecir delitos o detectar fraudes. En efecto, La Resolución (2020/2016(INI) del Parlamento Europeo (2021) enumera múltiples aplicaciones de IA en la investigación forense:

> (…) reconocimiento facial, reconocimiento automático de matrículas, identificación por voz, tecnologías de lectura de labios, vigilancia auditiva (detección de disparos), análisis de bases de datos, predicción de delitos y zonas críticas, autopsia virtual, detección de fraudes financieros, vigilancia de redes sociales.

Estas herramientas incrementan la eficacia policial, pero –según el mismo documento– tienen *"*implicaciones significativas para la protección de los derechos fundamentales*"* (Resolución (2020/2016(INI) del Parlamento Europeo, 2021**)**.: su fiabilidad puede variar y su uso masivo podría vulnerar la presunción de inocencia, la privacidad y la igualdad ante la ley.

Desde el punto de vista tecnológico, los sistemas de IA modernos integran aprendizaje estadístico y capacidad de procesamiento en la nube. Esto permite que, por ejemplo, una red neuronal profunda mejore con cada nuevo caso procesado. Sin embargo, esta opacidad del razonamiento interno genera problemas de imputación penal: si un algoritmo discrimina o falla, ¿cómo se determina responsabilidad? La comunidad jurídica debate si los algoritmos predictivos y las máquinas autónomas deben considerarse meros instrumentos o si se requiriesen figuras especiales en el código penal.

El derecho penal enfrenta, por lo tanto, retos nuevos. Históricamente, las leyes penales se han aplicado a actos humanos directos; ahora se plantean situaciones donde la acción puede venir mediada por IA, o la conducta prohibida puede ejecutarse en parte por una máquina autónoma. En este sentido, ya hay discusiones sobre la responsabilidad en el uso de sistemas IA: por ejemplo, en Chile y otros países se debate si los fiscales o jueces que usan IA para análisis predictivo actúan dentro del Estado de Derecho, dado que la automatización "cuestiona profundamente" el enfoque tradicional del derecho penal como reacción posterior al delito (Resolución (2020/2016(INI) del Parlamento Europeo, 2021**)** . En síntesis, el nexo actual entre IA y derecho penal es complejo: la tecnología permite nuevas formas de comisión de delitos, pero también ofrece herramientas para combatirlos. Este panorama exige un constante análisis técnico-jurídico para definir si las normas penales existentes cubren estos escenarios o si es preciso actualizar el ordenamiento.

4. El problema jurídico

El legislador ecuatoriano no incorpora un tipo penal específico sobre el uso malicioso de la inteligencia artificial lo que genera una alta posibilidad de impunidad por parte de victimarios ante la creciente utilización de estas tecnologías para cometer actos que vulneran la seguridad pública, la intimidad y otros bienes jurídicos protegidos, dado a que no toda conducta donde se emplea inteligencia artificial que pueda causar un perjuicio relevante a un bien jurídico pueden ser punibles en base a los tipos penales actuales previstos en el COIP (2014).

Es importante recordar que si bien habría ciertas conductas donde el uso de inteligencia artificial puede ser considerado para sancionar delitos ya existentes, como aquellos delitos que mencionan la ejecución de un verbo rector a través de "cualquier medio" , estos tipos penales no podrían cubrir todos los delitos existentes en el COIP debido a cómo han sido tipificados algunos.

En términos jurídicos, los tipos penales existentes del COIP se centran en la acción ilícita o en el resultado como el daño patrimonial, el acceso no autorizado, y la revelación de secretos, independientemente del medio. Por ejemplo, el COIP (2014) castiga el ataque a sistemas informáticos y el acceso no consentido a sistemas , así como la transferencia electrónica ilícita de fondos . Sin embargo, ninguno de esos tipos excluye ni incluye expresamente la posibilidad de que un programa de IA actúe como sujeto material del delito. De modo similar, delitos penales clásicos (estafa, extorsión, fraude) podrían aplicarse si la IA es simplemente un instrumento pasivo al servicio del autor humano, pero dejan sin tipificar escenarios donde la IA tenga un papel más autónomo.

Por tanto, se verifica un problema de tipicidad penal: el legislador ecuatoriano necesita incorporar un tipo penal específico sobre el uso malicioso de la inteligencia artificial, precisamente porque el COIP no contempla la peculiaridad de estos delitos emergentes. Esta carencia puede llevar a que actos delictivos cometidos con IA queden impunes. De este modo, la evolución tecnológica supera la letra fría de la ley, y que el concepto de autoría mediata a través de imputar el resultado de un algoritmo al programador, podría no ser suficiente ni claro para sancionar todas las conductas relacionadas con IA maliciosa. En resumen, los tipos penales existentes no cubren adecuadamente los delitos cometidos mediante IA, lo que justifica el estudio de una eventual tipificación nueva.

Adicionalmente, debido a la naturaleza de la inteligencia artificial y por estar en constante evolución es conveniente contar un tipo penal que pueda prever la punibilidad de conductas perjudiciales, -que no se pueden imaginar en su totalidad en la actualidad-, a bienes jurídicos protegidos por la Constitución y la normativa penal. De este modo, se llega a proteger el pacto social y los bienes jurídicos que tutela nuestro ordenamiento.

5. Bienes jurídicos protegidos en la Constitución de la República del Ecuador en relación al uso de IA

La Constitución ecuatoriana protege diversos bienes jurídicos que resultan afectados por el uso indebido de la IA. En primer lugar, destacan los derechos vinculados a la privacidad y los datos personales. El Artículo 66 literales 19 y 20 reconoce expresamente "el derecho a la protección de datos de carácter personal" y "el derecho a la intimidad personal y familiar" (Constitución de la República del Ecuador, 2008). Asimismo, el Art. 66 numeral 21 tutela la inviolabilidad de las comunicaciones, y el literal 22 la inviolabilidad del domicilio (Constitución de la República del Ecuador, 2008); ambos bienes pueden verse comprometidos cuando la IA es usada para interceptar comunicaciones (por ejemplo, mediante software de escucha) o para espiar sin orden legal.

Otros derechos constitucionales también son relevantes. La protección de la vida e integridad personal reconocida en el Art. 66, numeral 1 de la Constitución de la República del Ecuador (2008) se vulnera si se usan sistemas IA con fines violentos; la libertad de expresión del Art. 66, numeral 13 de la norma suprema mencionada entra en tensión con la difusión de información falsa generada por IA. El derecho al desarrollo científico y tecnológico exige que la innovación sea responsable, lo que implica regular la IA para proteger a la sociedad. Además, la Constitución de la República del Ecuador (2008) en su Artículo 66 numeral 27 prevé la protección del medio ambiente, que puede afectarse indirectamente por la huella ambiental de la infraestructura de IA (centros de datos) o su impacto en actividades relacionadas con el medio. Finalmente, otros bienes colectivos como la seguridad nacional y el orden público tutelados en el Art. 43 de la carta magna pueden verse amenazados si la IA es empleada en delitos contra la seguridad del Estado o para atentar contra la paz social.

Los usos maliciosos de IA involucran bienes jurídicos fundamentales consagrados constitucionalmente en Ecuador, lo que justifica su atención penal y constitucional

6. Principio de legalidad y taxatividad penal

El principio de legalidad penal se encuentra consagrado en la Constitución de la República del Ecuador (2008) en su Art. 76 numeral 3 en los siguientes términos:

> En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas:
>
> 3. 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, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento.

El COIP (2014), mediante su Art. 5 numeral 1 recoge este principio de la siguiente forma:

> **Art. 5**.- Principios procesales.- El derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, se regirá por los siguientes principios:
>
> 1. Legalidad: no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla.

De este modo, se reconoce que solamente la ley penal escrita puede definir delitos y penas (*nullum crimen, nulla poena sine lege*). Esto implica que toda punible en materia penal debe estar prevista de forma expresa en el COIP (2014), con normas claras que delimiten el tipo penal.

En el campo de la IA, estos principios implican que no es suficiente señalar de manera indiscriminada que la IA puede llegar a ser peligrosa, sino que debe existir un tipo penal que de forma específica y clara defina la conducta maliciosa, con todos sus

elementos. De lo contrario, se violaría la legalidad penal al castigar actos no previamente descritos.

Cualquier proyecto de tipo penal para la IA debe formularse con precisión técnica y expresamente; la analogía interpretativa queda prohibida, por lo que la propia ley penal debe aludir claramente a los nuevos escenarios tecnológicos para garantizar seguridad jurídica.

7. Tipificación penal actual en el COIP y su aplicación a conductas con IA

Dentro del COIP (2014), algunas disposiciones amplían su alcance a tecnologías modernas con fórmulas genéricas. Por ejemplo, el acoso académico constatado en el Art. 154.3, literal 1 se configura si la conducta ocurre “por cualquier medio incluyendo a través de las tecnologías de la información y comunicación” (COIP, 2014) . De modo análogo, el artículo 170 (violencia sexual agravada) incrementa la pena si el abuso “fuese grabado o transmitido en vivo... por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación” (COIP, 2014) . Estas expresiones señalan que la ley penal busca abarcar casos donde la violencia o el acoso se difunden a través de Internet o dispositivos electrónicos, sin fijar la tecnología precisa.

En síntesis, las referencias de la frase “por cualquier medio” en el COIP (2014) buscan garantizar que los tipos clásicos cobijen comportamientos con tecnología. Sin embargo, en el ámbito de la IA este mecanismo resulta insuficiente para señalar conductas específicas de IA. Se limita a tratar a la IA como medio electrónico, pero no como figura jurídica propia. Esto implica que, ante nuevos escenarios tecnológicos, la aplicación del COIP actual a delitos con IA puede dar lugar a vacíos o inseguridad jurídica: el juez deberá calificar el hecho con las categorías existentes (acoso, daño informático, fraude, etc.), aunque la conducta delictiva implique particularidades de la IA que la ley no contempla expresamente.

8. Límites de aplicación de figuras penales tradicionales a nuevos escenarios tecnológicos

Los delitos tradicionales del COIP fueron concebidos para conductas humanas concretas, y presentan límites al aplicarse a escenarios tecnológicos disruptivos. En primer lugar, el derecho penal clásico asume siempre un autor humano con dolo o

culpa, capaz de entender su acción. Cuando la IA actúa de modo parcialmente autónomo, surge la dificultad de imputar responsabilidad. La teoría jurídica de la autoría mediata podría asignar la acción al programador o al usuario de la IA, pero esto no resuelve todos los casos. Por ejemplo, si la IA aprende de forma imprevista y causa daño por sí sola–. Este es un vacío legal: la IA no tiene personalidad jurídica ni puede ser sancionada como sujeto penal, pero tampoco hay norma que tipifique la autoría mediata con IA como instrumento especial.

A su vez, es ineludible reconocer la existencia de un límite en el grado de especificación que la ley pudiere ser capaz de anticipar. Las tecnologías de IA evolucionan rápidamente; por ello, las figuras penales que pretenden ser amplias mediante la denominación de por cualquier medio pueden quedarse obsoletas. Sin duda, se reconoce la necesidad de actualizar el ordenamiento penal. Pero esa actualización debe hacerse con criterios ponderados: respetando los principios de legalidad y proporcionalidad, y evitando criminalizar genéricamente a la tecnología. En suma, las figuras penales tradicionales resultan insuficientes para abordar integralmente los delitos de IA maliciosa, pues no contemplan ni la autonomía ni la complejidad de los sistemas tecnológicos emergentes. Esto evidencia que los límites actuales del COIP exigen, al menos, claridad legislativa sobre cómo encarar las conductas con IA en el ámbito penal.

CAPÍTULO II

Propuesta de incorporación de un tipo penal sobre el uso malicioso de IA en el COIP

9. Fundamento jurídico de la necesidad de un nuevo tipo penal

La rápida evolución de la inteligencia artificial (IA) en la sociedad plantea desafíos inéditos para el Derecho Penal. Las leyes penales tradicionales suelen quedarse atrás frente a tecnologías emergentes capaces de producir daños de nuevas formas. En este contexto, se vuelve imprescindible fundamentar jurídicamente la creación de un nuevo tipo penal específico que sancione el uso malicioso de la IA. Solo así se puede garantizar que el sistema penal ecuatoriano esté a la altura de los riesgos modernos y proteja eficazmente los bienes jurídicos fundamentales potencialmente vulnerados por conductas mediadas por IA.

9.1. La evolución tecnológica y la responsabilidad penal

El avance tecnológico ha introducido herramientas de IA con autonomía y complejidad crecientes, lo cual tensiona los principios clásicos de responsabilidad penal. La IA puede generar resultados dañinos difíciles de prever o encuadrar en las figuras penales vigentes. Por ello, se reconoce a nivel comparado la necesidad de actualizar los códigos penales para adaptarlos a estas innovaciones. Así lo destaca la doctrina europea al referir que el nuevo Reglamento de IA de la Unión Europea “apela a la necesidad de actualización de los códigos penales europeos para graduar la respuesta sancionadora frente a los perjuicios derivados” (De la Cuesta Aguado, 2025) de prácticas riesgosas, forzando incluso “la reforma penal... para cerrar las lagunas que no pueden ser satisfechas con los actuales tipos penales” (De la Cuesta Aguado, 2025).

En base a la naturaleza de la IA de ser capaz de tomar decisiones semiautónomas, existe un quiebre respecto a las nociones tradicionales de autoría y culpabilidad. Surge el debate de si responsabilizar al programador, al operador, a la empresa propietaria o incluso al sistema autónomo mismo. La postura mayoritaria rechaza dotar de personalidad penal a la máquina y enfatiza mantener la imputación en sujetos humanos. Como se ha observado en entornos tecnológicos peligrosos de armas y maquinarias, el consenso es que los agentes artificiales automáticos bajo control humano generan responsabilidad en personas físicas, mientras que los sistemas

autónomos o semiautónomos crean “un cierto vacío de responsabilidad (*responsibility gap*), sí– complicado tratamiento jurídico (y penal)” (De La Mata Barranco, 2023) de la misma. Es decir, a mayor autonomía de la IA, más difícil resulta atribuir la responsabilidad penal dentro del marco legal vigente. Esta evolución tecnológica exige, por tanto, reajustar nuestras normas para no dejar sin respuesta penal los daños ocasionados con IA y para clarificar qué sujetos deben rendir cuentas en cada supuesto.

9.2. El riesgo de impunidad ante lagunas legales

La falta de tipos penales específicos para conductas cometidas con ayuda de IA acarrea el riesgo real de impunidad. La aplicación de las teorías penales clásicas a la realidad de la IA presenta problemas dado a que dejan a “la determinación de la responsabilidad penal en zonas grises que diluya la responsabilidad” (Valls, 2022). Dichas zonas grises implican que ciertos comportamientos dañinos podrían no encajar con claridad en ningún delito existente, posibilitando que queden sin castigo.

Se ha advertido que la enorme complejidad y opacidad de estos sistemas “impone severas dificultades a la identificación precisa del nexo de causalidad entre una determinada conducta y el daño o peligro de daño” (Túlio Felippe, 2023) que se produce. En otras palabras, la cadena de eventos que lleva del actuar humano inicial (diseño, programación o decisión de desplegar la IA) al daño final puede ser tan difusa que las responsabilidades individuales se diluyen.

El fundamento jurídico del nuevo tipo penal, entonces, es cerrar esas lagunas legales para asegurar que ninguna conducta gravemente lesiva realizada mediante IA quede sin respuesta penal. La tipificación específica brinda certeza jurídica y cumple una función preventiva, dejando claro a la sociedad que valerse dolosamente o con imprudencia grave de la IA para hacer daño constituye delito y acarreará sanciones.

10. Elementos estructurales del tipo penal propuesto

Definir un nuevo tipo penal requiere establecer con precisión sus elementos estructurales: quién puede cometer el delito y contra quién, cuál es la conducta típica (qué acciones u omisiones abarca, con qué forma de culpabilidad) y qué resultado debe producirse, así como el nexo causal entre la acción y el resultado. A continuación se

detallan estos aspectos para el delito de uso malicioso de IA que se propone incorporar en el COIP.

10.1. Sujeto activo y pasivo

Sujeto activo: Se concibe que el delito pueda ser cometido por cualquier persona, sea natural o jurídica. Es decir, tanto individuos humanos como empresas u otras entidades colectivas podrían ser sujetos activos del ilícito. Esto es coherente con la tendencia moderna del derecho penal de admitir la responsabilidad penal de las personas jurídicas en determinados delitos tecnológicos o económicos. En el contexto de la IA, las compañías desarrolladoras o usuarias de sistemas inteligentes potencialmente peligrosos deben rendir cuentas si mediante ellos causan delitos, igual que los individuos. Por lo tanto, el tipo penal propuesto tendría sujetos activos plurales: cualquier persona física o entidad corporativa que, en el diseño, desarrollo, implementación, uso o supervisión de un sistema de IA, incurra en la conducta ilícita descrita.

Sujeto pasivo: Del mismo modo, es amplio el universo de posibles víctimas u ofendidos por este delito. Dependiendo de la modalidad concreta, el sujeto pasivo podría ser una persona individual o incluso la colectividad en su conjunto. El bien jurídico protegido variará según el resultado: podría ser la vida e integridad si la IA maliciosa causa lesiones o muerte, o el patrimonio, la intimidad y honor en situaciones de difamaciones o divulgación de datos sensibles mediante IA. La formulación del tipo penal debe prever expresamente qué bienes tutela; no obstante, al ser un delito de resultado lesivo, en cada caso habrá un sujeto pasivo identificado cuya esfera de derechos es vulnerada por el actuar malicioso de o a través de la IA.

Un aspecto que recalcar es que la IA en sí misma no puede ser sujeto activo ni pasivo de delito, dado que carece de personalidad jurídica. El agente artificial es, jurídicamente, una herramienta o medio a través del cual actúa una persona. La inteligencia artificial no es un sujeto de derecho ni se le reconoce personalidad jurídica, por lo que no puede cometer delitos ni ser sancionada penalmente por sí misma, actualmente ningún ordenamiento atribuye responsabilidad penal directa a máquinas. (De La Mata Barranco, 2023) Consecuentemente, siempre habrá detrás un ser humano (o ente colectivo) al que imputar la conducta delictiva: ya sea por acción directa, por

instruir al sistema a realizarla, o por omisión culpable en su supervisión. Esta aclaración es vital para asentar la estructura del tipo propuesto: el delito protege bienes jurídicos humanos y solo seres dotados de voluntad legalmente imputable (personas naturales o jurídicas) pueden ser responsables de su comisión.

10.2. Conducta típica: diseño, uso y supervisión dolosa o culposa

La conducta típica abarcaría una variedad de comportamientos relacionados con sistemas de IA cuando se realizan de forma maliciosa. En términos generales, se propone tipificar a quien, en cualquier etapa del ciclo de vida de un sistema de inteligencia artificial –ya sea durante su diseño o programación, durante su implementación, puesta en marcha o uso operativo, o durante su deber de supervisión o control, actúe de tal modo que el sistema cometa o facilite la comisión de un delito que cause un resultado lesivo a personas o bienes. Esta formulación amplia pretende cubrir tanto acciones comisivas. Verbigracia, programar intencionalmente una IA para realizar ciberataques, o emplearla deliberadamente para difundir deepfakes difamatorios como omisiones relevantes cuando no se implementan las debidas salvaguardas o controles en un sistema de IA de alto riesgo, permitiendo que produzca un daño evitable).

Es importante precisar las formas de dolo y culpa contempladas. En cuanto al dolo, se debe sancionar a quien con intención de producir un daño o aceptando su producción mediante la IA. En cuanto a la culpa, debe ser penalmente castigada quien actuare con imprudencia grave o negligencia en el manejo de la IA, generando un resultado dañoso que era previsible y debía evitar. Estas modalidades de responsabilidad penal se erigen como válidas dado a que los sistemas de IA pueden causar lesiones a bienes jurídicos protegidos por usos maliciosos y por situaciones donde el sujeto activo recae en negligencia en el desarrollo o supervisión de dicho sistema, situación que no se encuentra fuera de su control. La inclusión de la culpa permite penalizar, por ejemplo, al desarrollador que, por descuido grave en las medidas de seguridad, lanza al mercado una IA que lesiona a consumidores; o al operador que ignora flagrantes alertas de mal funcionamiento hasta que ocurre una catástrofe.

La conducta típica dolosa comprendería: configurar o emplear la IA con la intención de cometer un delito o sabiendo que con ello se cometerá. Por ejemplo, usar

un algoritmo para estafar, difamar, sabotear infraestructura y violar datos personales. También cubriría al que ordena a la IA realizar actos ilegales (como un administrador de un sistema autónomo que le "encarga" hacer algo ilícito). Por su parte, la conducta típica culposa abarcaría: desarrollar o desplegar sistemas de IA sin las debidas precauciones, ignorando estándares técnicos o legales, de forma tal que por esa imprudencia el sistema causa un daño.

En cualquier caso, para configurar el delito será necesario que la conducta del sujeto activo guarde una relación directa con el sistema de IA en cuestión. Ejemplos concretos de la conducta típica serían: programar o entrenar un modelo de IA con datos maliciosamente sesgados para que tome decisiones perjudiciales; diseñar virus o malware de IA para atacar sistemas informáticos; utilizar una IA de síntesis de voz o video para suplantar la identidad de alguien y cometer fraude; emplear deepfakes para difamar o extorsionar; manipular un vehículo autónomo para causar un accidente; o no intervenir en un sistema de IA bajo nuestro control sabiendo que está fuera de control y causará daños. Todos estos supuestos ilustran acciones u omisiones en el diseño, uso o supervisión de IA que, de forma dolosa o gravemente imprudente, derivan en un acto lesivo.

Es fundamental que la redacción del tipo penal sea clara pero también suficientemente flexible para abarcar las múltiples formas en que la IA puede ser mal utilizada. La experiencia comparada muestra que ya existen conductas típicas emergentes relacionadas con IA, como la fabricación de *deepfakes* no consentidos para dañar la reputación o la manipulación de voces e imágenes con fines de estafa. En Perú, por ejemplo, una reciente reforma penal "tipifica penalmente el uso de IA destinado a crear *deepfakes* o contenido multimedia vinculado a la pornografía infantil y la difamación, entre otros" (Tellez Tejada, 2025), considerándolo circunstancia agravante de delitos tradicionales. Esto evidencia la diversidad de escenarios que deben cubrirse. Por ello, el tipo penal ecuatoriano deberá describir la conducta de manera amplia (referenciando el diseño, desarrollo, implementación, utilización o control de sistemas de IA) pero acotada por la exigencia de dolo o culpa grave y por la producción de un resultado ilícito específico.

10.3. Resultado y nexo de causalidad

El delito propuesto sería de resultado, lo que implica que para su configuración se requiere la efectiva producción de un daño o puesta en peligro concreto de un bien jurídico, causado por o a través del sistema de IA. En otras palabras, no se castigaría meramente la conducta de gestionar una IA de forma peligrosa, sino que dicha conducta debe desencadenar un resultado lesivo típico (por ejemplo, lesiones, muerte, fraude consumado, revelación de secretos, daño patrimonial, etc., dependiendo del caso). El tipo penal podría definirse de forma genérica, por ejemplo, mencionando aquel que "cause daños a personas o bienes mediante sistemas de IA", con el resultado lesivo como elemento esencial. Así se respetaría el principio de lesividad, evitando penalizar conductas preparatorias o de riesgo abstracto que no culminen en afectación alguna.

Ahora bien, uno de los puntos más delicados es establecer el nexo causal entre la conducta del sujeto activo y el resultado producido, dada la intervención de la IA como elemento intermedio. En delitos comunes, el nexo de causalidad exige que la acción u omisión del autor sea condición sine qua non del resultado y que, además, dicho resultado le sea objetivamente imputable, es decir, realizado dentro del ámbito de riesgo que su conducta creó. En los casos con IA, a veces la cadena causal es larga y compleja: desde la decisión humana inicial, pasando por procesos internos automáticos de la máquina, hasta el evento dañoso final. La causalidad física puede no ser lineal ni evidente.

Sin embargo, desde la perspectiva jurídico-penal, se deberá probar que el comportamiento del acusado, sea una acción u omisión respecto de la IA, fue la causa del resultado. Esto requerirá frecuentemente peritajes técnicos para explicar cómo la configuración o uso del sistema derivó en el daño. Un desafío adicional es la imprevisibilidad inherente a algunos sistemas de machine learning. Si el resultado lesivo ocurrió de forma totalmente imprevisible para un operador razonable, podría romperse la imputación objetiva (nadie puede responder por consecuencias absolutamente insospechadas). De hecho, se ha planteado que la imprevisibilidad de los outputs de ciertos algoritmos impone enormes dificultades para imputar penalmente a una persona, ya que programadores, fabricantes y usuarios "no siempre podrán prever el desempeño de la IA". Dado que el juicio de previsibilidad es clave en

la tipicidad de conductas imprudentes ya que “debe rechazarse cuando el resultado ilícito de la IA es totalmente impredecible” (Túlio, 2023). Esto significa que, si realmente nadie podía anticipar el daño causado por la IA, no habría responsabilidad penal individual (en el ámbito de la culpa, al menos).

Una cláusula importante en la tipificación será precisar que el resultado dañoso debe haber sido ocasionado mediante el sistema de IA. Es decir, establecer una relación mediata: la persona actúa sobre la IA (o deja de actuar cuando debe), y a través de esa IA se produce el daño. Esto delimita el campo del delito, diferenciándolo de los delitos comunes: aquí la herramienta o medio del crimen es un sistema de inteligencia artificial. Si el daño ocurre sin mediación de IA, se tratará de delitos tradicionales como homicidios simples y estafas, pero si el daño ocurre por la intervención de una IA maliciosamente empleada o negligentemente controlada, encajará en el nuevo tipo penal, siempre que se pruebe adecuadamente ese nexo.

En cuanto al grado de resultado, el tipo podría ser formulado de manera básica y prever luego agravantes según la gravedad del daño. Por ejemplo, un resultado de muerte o gran catástrofe podría agravar la pena en comparación con un resultado de lesión leve o perjuicio patrimonial menor. Lo importante es que la ley describa con claridad qué consecuencias entran en el tipo base y cómo se vincula la conducta con dichas consecuencias.

11. Criterios para la determinación de la sanción penal

Una vez definido el nuevo tipo penal, es necesario establecer criterios claros para graduar la sanción aplicable, atendiendo a la diversa gravedad que pueden tener las conductas y resultados involucrados. Asimismo, debe considerarse el régimen de responsabilidad de las personas jurídicas, dada su inclusión como posibles sujetos activos. A continuación, se abordan estos criterios de penalidad.

El delito de uso malicioso de IA podría ocasionar desde daños menores hasta catástrofes de gran magnitud, dependiendo del contexto (por ejemplo, no es lo mismo generar fake news difamatorias que causar un accidente masivo con un coche autónomo). Por ello, la ley debe prever una pena graduable en función de la entidad del daño causado y del riesgo concretamente creado.

Una alternativa puntual es establecer un marco penal base relativamente amplio, por ejemplo, prisión de X a Y años para el tipo básico, complementado con subtipos agravados vinculados a resultados especialmente graves. Podrían preverse agravantes específicas análogas a las existentes en delitos tradicionales, pero adaptadas al medio de la IA. Por ejemplo, si la conducta mediante IA causa la muerte de una persona, podría equipararse a un homicidio doloso o imprudente según el caso y sancionarse con penas altas. Si causa lesiones de cierta gravedad, aplicarse una pena intermedia. Si produce daños patrimoniales o fraudes millonarios, igualmente cabría una agravación. Por lo tanto, la conducta punible deberá contener una sanción basada en una proporcionalidad entre el resultado lesivo y el grado de autoría, al igual que la valoración de criterios agravantes.

12. Consideraciones sobre la responsabilidad de personas jurídicas

Al incluir a las personas jurídicas como posibles sujetos activos, surge la cuestión de cómo sancionarlas penalmente en caso de ser halladas culpables. En el régimen ecuatoriano actual, ya existe regulación para la responsabilidad penal de personas jurídicas en ciertos delitos, normalmente mediante penas de multa, comiso, suspensión de actividades, disolución, etc., en lugar de penas privativas de libertad que son inaplicables a entes colectivos. Habría que prever explícitamente la aplicación de dichas sanciones corporativas al nuevo delito.

Así, si una empresa es condenada por uso malicioso de IA, por ejemplo, una compañía que desarrolló un software de forma dolosa para espiar ilegalmente a usuarios, o que por políticas negligentes permitió un desastre medioambiental con sistemas automatizados, podrían imponérsele multas proporcionales a su capacidad económica y al daño causado, la prohibición de contratar con el Estado, la clausura temporal de locales, la publicación de la sentencia condenatoria, e incluso la disolución de la persona jurídica en casos gravísimos de reincidencia o falta de control corporativo.

La relevancia de la responsabilidad corporativa en este ámbito es subrayada por la doctrina. Se ha argumentado que, ante la complejidad de estos casos con IA, en que a veces no es posible identificar fácilmente a un autor humano individual, la vía eficaz para no dejar sin sanción el hecho es acudir a la responsabilidad de la persona

jurídica involucrada (Túlio Felippe, 2023). De hecho, en escenarios donde una IA autónoma provoca un daño y no hay una acción humana directa en ese momento, la empresa dueña o beneficiaria del sistema podría considerarse como autor del hecho típico por sí misma, en tanto la actuación de la IA es, en última instancia, consecuencia de decisiones corporativas previas.

Por lo tanto, el tipo penal propuesto debe prever que, si el delito es cometido en el seno de una persona jurídica, se aplicarán a ésta las sanciones penales correspondientes conforme a las reglas generales del COIP (2014). Asimismo, promover la adopción de programas de cumplimiento (compliance) en materia de IA sería deseable: la existencia de protocolos éticos y técnicos en la empresa para prevenir usos indebidos de IA podría valorarse como atenuante o eximente de responsabilidad corporativa, según el modelo de "debida diligencia" corporativa.

13. Derecho Comparado

Para enriquecer la propuesta ecuatoriana, resulta útil examinar cómo otras jurisdicciones están afrontando penalmente el tema del uso malicioso de la inteligencia artificial. A continuación, se presenta una comparación sucinta con dos referentes: el Derecho Penal peruano, en la región latinoamericana, y el sistema de los Estados Unidos, pionero en regular ciertos aspectos tecnológicos. Se analizan particularmente las figuras jurídicas o reformas que abordan conductas delictivas vinculadas al empleo de IA con fines ilícitos.

13.1. Perú

Perú ha dado un paso relevante al reformar su legislación penal para contemplar expresamente el uso de IA en la comisión de delitos. En abril de 2025 se promulgó la Ley Nº 32314, la cual modifica el Código Penal peruano y su Ley de Delitos Informáticos. Esta reforma introduce el uso de IA como circunstancia agravante general en diversos delitos. Con ello:

> Con esta reforma, delitos como la **difamación**, **estafa**, **pornografía infantil**, **plagio**, y las infracciones contra los derechos de autor y la propiedad intelectual, podrán ser sancionados con penas más severas cuando se cometan

mediante herramientas basadas en IA, incluyendo el uso de **deepfakes** o tecnologías de manipulación de voz e imagen (Maldonado, 2025).

En concreto, la legislación peruana ahora prevé aumentar hasta en una tercera parte la pena de cualquier delito si en su comisión se utilizó inteligencia artificial o medios análogos . Además, se incorporaron descripciones específicas: por ejemplo, se tipificó la difusión de deepfakes con contenido sexual no consentido como forma agravada de difamación, se agravó la estafa cuando se realiza manipulando con IA la voz o imagen de terceros, y se incluyó el uso de IA en delitos de pornografía infantil (Tellez Tejada, 2025) .

La normativa peruana reciente si bien no creó un delito autónomo, trató de adaptar los existentes, reflejando así un compromiso con evitar la impunidad de delitos cometidos con IA, lo cual se puede analizar en base a sus ventajas y desventajas. Por un lado, puede verse como positivo para la legislación extranjera el ánimo de mantener casi intacto el código penal reconociendo únicamente a la IA como un agravante de tipos penales. La desventaja es que puede dispersar el tratamiento del fenómeno en múltiples tipos dejando la probabilidad de no considerar una conducta que no pudiere ser adecuada en la aplicación de análisis de punibilidad en delitos tradicionales. No obstante, Perú identifica explícitamente los escenarios más preocupantes: deepfakes, suplantación de identidad, ataques a la propiedad intelectual mediante IA, como crear software para burlar medidas de protección anticopia (Maldonado, 2025). En suma, el derecho peruano penaliza el uso indebido de IA enfatizando la protección de la honra (rente a difamación con deepfakes, el patrimonio en las estafas con IA, y, la indemnidad sexual de menores en la pornografía montada con IA.

Para Ecuador, la experiencia peruana sugiere la importancia de abordar deepfakes y fraudes con IA. Si bien nuestra propuesta plantea un tipo autónomo general, podría complementarse con agravantes similares a las peruanas en delitos específicos, o al menos tomar en cuenta esas categorías de conductas al interpretar el nuevo tipo penal. También muestra la utilidad de prever sanciones a desarrolladores de IA ilícita: la ley peruana sanciona a quienes desarrollen o brinden servicios tecnológicos destinados a eludir medidas de seguridad, por ejemplo, el empleo de IA para hackear protección de derechos de autor. Esa previsión podría incorporarse en

Ecuador, penalizando no solo el uso final de la IA para delinquir, sino también la creación dolosa de herramientas de IA orientadas al delito.

13.2. Estados Unidos

En el sistema estadounidense (federal y estatal), no existe aún un código penal unificado que recoja un delito general de uso malicioso de IA. Sin embargo, recientemente se han promulgado leyes puntuales relacionadas con IA y delitos informáticos, especialmente enfocadas en la problemática de los deepfakes y la pornografía no consentida.

En 2023 se aprobó la ley federal *Take It Down Act* en respuesta a los deepfakes de carácter íntimo. Dicha ley, "penaliza la distribución no consentida de imágenes sexualmente explícitas, reales o generadas por inteligencia artificial" (Martínez, 2025), declarándola delito federal. En concreto, compartir intencionalmente contenido íntimo falso creado con IA, sin consentimiento de la persona afectada, puede conllevar penas de hasta 3 años de prisión a nivel federal en EE.UU. . Adicionalmente, la norma impone obligaciones a las plataformas digitales para retirar dicho contenido en plazos breves, bajo apercibimiento de sanciones administrativas por parte de la FTC (*Federal Trade Commission*) (Martínez, 2025).

A nivel estatal, varios estados han legislado en materia de deepfakes: por ejemplo, Virginia y California penalizaron la divulgación de pornografía ficticia hecha con IA sin consentimiento, y Texas prohibió los deepfakes maliciosos en contexto electoral. Estas iniciativas muestran una clara tendencia en EE.UU. de legislar aspectos específicos donde la IA afecta derechos fundamentales como la privacidad, el honor y la libertad sexual. También en el ámbito financiero y de ciberseguridad, las leyes existentes contra fraude electrónico y hacking se han ido aplicando a casos con IA, aunque sin disposiciones especiales sobre IA todavía.

La enseñanza para Ecuador del modelo estadounidense es doble. Por un lado, confirma la necesidad de cubrir legalmente fenómenos como los deepfakes no consentidos, pues representan una amenaza real a víctimas, especialmente mujeres, que en EE.UU. han sido las principales afectadas por pornovenganza con IA . Por otro lado, demuestra que muchas conductas con IA pueden ser perseguidas mediante tipos penales clásicos, siempre que haya voluntad interpretativa. No obstante, el riesgo es

que algunas situaciones queden fuera o sea difícil probar la intención específica relacionada con la IA. Estados Unidos está avanzando fragmentariamente (ley de deepfakes aquí, norma sobre vehículos autónomos allá, etc.), mientras que la propuesta ecuatoriana busca una figura unificadora.

14. Propuesta de solución al problema jurídico

Reformar el COIP, a través de la Asamblea Nacional del Ecuador incluyendo un nuevo tipo penal con suficiente detalle en sus elementos de la siguiente forma:

> **Artículo X. Uso malicioso de sistemas de inteligencia artificial.-** La persona que, dolosa o culposamente, diseñe, programe, use, opere o supervise un sistema de inteligencia artificial, que resulte en un daño a la vida, integridad personal, libertad, seguridad, patrimonio, derechos digitales, o cualquier otro bien jurídico protegido por este Código, será sancionada con pena privativa de libertad de tres a siete años.
>
> La pena será de doce a catorce años cuando:
>
> a) El hecho produzca la muerte de una persona.
>
> b) El hecho afecte servicios públicos esenciales, infraestructuras críticas o sistemas de salud.
>
> c) El hecho se cometa contra personas en situación de vulnerabilidad, menores de edad o personas con discapacidad.
>
> Para efectos de este código, se entiende por "sistema de inteligencia artificial" todo sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida,

como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

CONCLUSIONES

1. En mérito del avance del estado de la técnica de la IA, se han creado nuevos escenarios en los que el COIP vigente puede promover la impunidad cuando existiere la comisión de delitos con sistemas de IA debido a la falta de tipificación expresa de un tipo penal que tenga en consideración esta novedosa herramienta tecnológica.

2. En base a la experiencia proveniente del derecho comparado de Perú y Estados Unidos. Lo más idóneo sería crear un tipo penal que tenga en consideración los principios reconocidos en la Constitución de la República del Ecuador y el COIP que respete la estructura general en la que se tipifican los delitos en la segunda norma mencionada, con el objeto de no generar confusiones y evitar incongruencias con los tipos penales que se encuentran vigentes.

REFERENCIAS

Asamblea Constituyente de Ecuador. (2008). *Constitución de la República del Ecuador.* Quito: Última Reforma: Registro Oficial Suplemento 554 de 9 de mayo del 2024.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal, COIP*. Quito: Ultima Reforma: Registro Oficial Suplemento 68 de 26 de junio del 2025.

Congreso de la República del Perú. (2025). *Ley Nº 32314: Ley que modifica el Código Penal y la Ley de Delitos Informáticos para incluir el uso de la inteligencia artificial en la comisión de delitos*. Diario Oficial El Peruano.

De la Cuesta Aguado, P. M. (2025). *El Derecho penal frente al Reglamento de Inteligencia Artificial*. Revista Ius Criminale, (1), 1-23.

De La Mata Barranco, N. J. (2023). *Inteligencia artificial autónoma y responsabilidad penal de las personas jurídicas*. Almacén de Derecho. Recuperado de https://almacendederecho.org/inteligencia-artificial-autonoma-y-responsabilidad-penal-de-las-personas-juridicas

García Martínez, I. (2022). *Responsabilidad penal y sistemas inteligentes: una aproximación desde el derecho penal de acto*. Revista Electrónica de Ciencia Penal y Criminología, 24, 1-34.

Maldonado, V. (2025). Ley 32314: modifican el Código Penal y otro para sancionar el uso de la inteligencia artificial en la comisión de delitos. Pasión por el Derecho. Obtenido de: https://lpderecho.pe/ley-32314-modifican-codigo-penal-sancionar-uso-inteligencia-artificial-delitos/#:~:text=Con%20esta%20reforma%2C%20delitos%20como,manipulación%20de%20voz%20e%20imagen

Martínez, A. (2025). *Take It Down Act, la ley que criminaliza los deepfakes y la 'pornovenganza'*. El País (España). Recuperado de https://elpais.com/us/2025-05-20/take-it-down-act-la-ley-que-criminaliza-los-deepfakes-y-la-pornovenganza.html

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2024, 26 de septiembre). *Recomendación sobre la ética de la inteligencia artificial*. UNESCO. Recuperado de https://www.unesco.org/es/artificial-intelligence/recommendation-ethics

Parlamento Europeo. (2021). *Resolución de 6 de octubre de 2021 sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales* (2020/2016(INI)). Diario Oficial de la Unión Europea C 132, 23.4.2022, p. 2-15.

Parlamento y Consejo Europeo. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de marzo 2024, 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*. Diario Oficial de la Unión Europea.

Téllez Tejada, N. (2025). *Perú tipificó al uso de la inteligencia artificial como agravante de un delito*. TeleSemana. Recuperado de https://www.telesemana.com/blog/2025/04/30/peru-tipifico-al-uso-de-la-inteligencia-artificial-como-agravante-de-un-delito/

Túlio Felippe, X. J. (2023). *Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales.* Universidad de Santiago de Compostela. Estudios Penales y Criminológico. Obtenido de: https://revistas.usc.gal/index.php/epc/article/view/8902/13236#:~:text=La%20imputación%20de%20responsabilidades%20penales,o%20peligro%20de%20daño%2032

Valls Prieto, J. (2022). *Sobre la responsabilidad penal por la utilización de sistemas inteligentes*. Revista Electrónica de Ciencia Penal y Criminología, 24, 1-35.

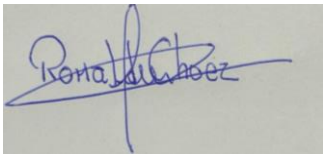
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Ronald Felipe Choez Peñafiel**, con C.I: #0991034381 autor del trabajo de titulación: **EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL,** previo a la obtención del título de Abogado en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 18 de agosto de 2025



f. _____

Ronald Felipe Choez Peñafiel

C.I: 0991034381

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	**EL USO MALICIOSO DE INTELIGENCIA ARTIFICIAL COMO PROPUESTA DE TIPO PENAL**		
AUTOR(ES)	**CHOEZ PEÑAFIEL RONALD FELIPE**		
REVISOR(ES)/TUTOR(ES)	**Ab. Pablo Carrión Carrión**		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	**Facultad de Jurisprudencia, Ciencias Sociales y Políticas**		
CARRERA:	**Carrera de Derecho**		
TITULO OBTENIDO:	Abogado		
FECHA DE PUBLICACIÓN:	18 de agosto de 2025	**No. DE PÁGINAS:**	31
ÁREAS TEMÁTICAS:	Derecho penal informático, Inteligencia Artificial, Delitos Informáticos		
PALABRAS CLAVES/ KEYWORDS:	Inteligencia artificial, principio de legalidad, derecho penal, estado de la técnica de la IA.		

RESUMEN/ABSTRACT: El presente trabajo de titulación analiza la urgente necesidad de adaptar el derecho penal ecuatoriano a los desafíos que plantea el uso indebido de tecnologías emergentes, particularmente la inteligencia artificial (IA). El problema jurídico central radica en que el COIP(COIP) no contempla de forma específica la punibilidad de conductas maliciosas cometidas mediante IA, lo cual genera vacíos normativos que pueden dejar impunes actos que atentan contra bienes jurídicos fundamentales que reconoce el Estado ecuatoriano como la intimidad, la seguridad pública y la integridad de las personas. El trabajo propone la incorporación de un tipo penal autónomo que sancione a la persona natural o jurídica que, con dolo o culpa, en el diseño, uso o supervisión de sistemas automatizados, cause daños a personas o bienes. Se justifica esta necesidad en la naturaleza evolutiva de la IA y su capacidad de generar conductas lesivas difíciles de prever bajo los tipos penales tradicionales. Además, se realiza un análisis comparativo con legislaciones extranjeras, destacando avances significativos en Francia y Estados Unidos, donde ya se han tipificado penalmente conductas como la creación y difusión de deepfakes o imágenes generadas con IA sin consentimiento, sentando precedentes útiles para el contexto ecuatoriano. Se concluye recomendando reformas al COIP para cubrir las lagunas expuestas.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593 964021017	**E-mail:** ronald.choez@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Maritza Reynoso Gaute**	
	Teléfono: +593-4-3804600	
	E-mail: angela.paredes01@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	