UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DERECHO

Los delitos a partir del uso de IA y su tipificación en la Legislación Penal Ecuatoriana

Trabajo de Titulación para optar al título de Abogado de los Tribunales y Juzgados de la República del Ecuador

Autor:

Ojeda Yanez, Robinsson Joel

Tutor:

Dr. Nelson Francisco Freire Sánchez

Riobamba, Ecuador. 2025

DECLARATORIA DE AUTORÍA

Yo, Robinsson Joel Ojeda Yanez, con cédula de ciudadanía 060571845-1, autor (a) (s) del trabajo de investigación titulado: **"LOS DELITOS A PARTIR DEL USO DE IA Y SU TIPIFICACIÓN EN LA LEGISLACIÓN PENAL ECUATORIANA"**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 18 de noviembre del 2025.

Robinsson Joel Ojeda Yanez

C.I:0605718451

AUTOR

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Dr. Dr. Nelson Francisco Freire Sánchez catedrático adscrito a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: "Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana" bajo la autoría de, Robinsson Joel Ojeda Yanez; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 18 días del mes de noviembre de 2025

Dr. Nelson Francisco Freire Sánchez

Tutor

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana, presentado por Robinsson Joel Ojeda Yanez, con cédula de identidad número 060571845-1, bajo la tutoría del Dr. Nelson Francisco Freire Sánchez; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba, a los 18 días del mes de noviembre del 2025.

Dr. Becquer Carvajal Flor
PRESIDENTE DEL TRIBUNAL DE GRADO

Dra. Gabriela Medina Gárces
MIEMBRO DEL TRIBUNAL DE GRADO

Dr. Juan Montero Chávez
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **OJEDA YANEZ ROBINSSON JOEL** con CC: **0605718451**, estudiante de la Carrera **DERECHO**, Facultad de **CIENCIAS POLÍTICAS Y ADMINISTRATIVAS**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana"**, cumple con el 6% plagio y el 8% de IA, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 07 de noviembre de 2025.

Dr. Nelson Francisco Freire Sánchez
TUTOR

DEDICATORIA

A mi madre por ser mi guía, mi respaldo de apoyo, el viento detrás de mis velas y la fuerza impulsora que me empuja más lejos por este camino. El amor, sacrificio y lecciones que me ha enseñado han moldeado la base de mis sueños.

A mi padre (+), a quien no pudo acompañarme en este momento tan importante, sus enseñanzas siempre han sido guía en mi vida, su recuerdo es fuente de fortaleza e inspiración, para encontrarme en es tu momento de mi vida.

A mi hermano mayor, mi compañero de vida, gracias por tu apoyo y por siempre estar con mi en todo momento, eres un ejemplo de esfuerzo y perseverancia.

Y a todas las personas que de una forma u otra me ayudaron en este camino, gracias con todo mi corazón. Esta tesis marca la culminación de los esfuerzos, amor y dedicación que he recibido a lo largo de la vida.

AGRADECIMIENTO

Agradezco a la Universidad Nacional de Chimborazo, en especial a la Carrera de Derecho, por brindarme el espacio para crecer tanto en el ámbito académico como personal, este trabajo es gracias al compromiso y dedicación de mis docentes, quienes compartieron sus conocimientos como experiencias, motivándome a ser mejor cada día.

A mi madre y hermano, quienes con su esfuerzo incansable, amor incondicional y consejos sabios me han enseñado el valor del esfuerzo y la honestidad, siendo su apoyo mi mayor fortaleza, que ha permitido lograr alcanzar este logro.

Finalmente, a cada persona que de alguna manera me ha ayudado a la culminación de este trabajo, expreso mi más sincero agradecimiento. Este logro no solo es solo mío, sino de todos aquellos que han creído en mí.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación analiza los delitos derivados del uso de la inteligencia artificial en Ecuador y su impacto en el ámbito penal, evidenciando cómo el avance acelerado de esta tecnología ha generado nuevas modalidades delictivas que desafiaban los marcos normativos tradicionales y crean vacíos legales que obstaculizan su persecución efectiva, se estudia los delitos más frecuentes asociados a la IA, como el fraude automatizado, la manipulación de datos y la generación de contenido falso, explorando sus características principales y aplicaciones en sectores como el derecho y la ciberseguridad, mientras se analiza cómo la responsabilidad penal se ve afectada cuando intervienen sistemas autónomos o algoritmos avanzados. Se incluye un análisis comparativo de diversas legislaciones internacionales, Estados Unidos, España y China, junto con sus casos, como fraudes financieros, ciberataques a infraestructuras críticas entre otros, lo que permite identificar estrategias normativas aplicables al contexto ecuatoriano. En Ecuador existe vacíos en el Código Orgánico Integral Penal, para enfrentar estos retos tecnológicos, nace la necesidad de reformas legislativas que tipifiquen los delitos asociados a la IA, para poder determinar la responsabilidad penal entre desarrolladores, operadores y usuarios. Se concluye que la cooperación interinstitucional es muy importante, para prevenir y sancionar el uso indebido de la IA, fortaleciendo la cooperación internacional y promoviendo programas de alfabetización digital, contribuyendo así a la construcción de un marco jurídico moderno que garantice la protección de los derechos y promueva el desarrollo tecnológico responsable en Ecuador.

Palabras clave: inteligencia artificial, vacíos legales, responsabilidad penal, regulación tecnológica.

.

ABSTRACT

This research analyzes crimes arising from the use of artificial intelligence in Ecuador and their impact on the criminal justice system, highlighting how advances in this technology are giving rise to new types of crime that challenge traditional regulatory frameworks and create legal loopholes that hinder effective prosecution. It studies the most frequent crimes associated with AI, such as automated fraud, data manipulation, and the generation of false content, exploring their main characteristics and applications in the field of law. Criminal liability is affected when autonomous systems are involved. It includes a comparative analysis of various international legislations, the United States, Spain, and China, along with their cases, which allows for the identification of regulatory strategies applicable to the Ecuadorian context. In Ecuador, there are gaps in the Comprehensive Organic Criminal Code to address these technological challenges, creating a need for legislative reforms to determine criminal liability among developers, operators, and users. It is concluded that inter-institutional cooperation is important to prevent and punish the misuse of AI, promote digital literacy programs, and thus contribute to the construction of a legal framework that guarantees the protection of rights and promotes responsible technological development in Ecuador.

Keywords: artificial intelligence, legal gaps, criminal liability, technological regulation.

Reviewed by:
Marco Antonio Aquino
ENGLISH PROFESSOR
C.C. 1753456134

CAPÍTULO I.

1.1. Introducción

El presente trabajo de investigación tuvo como fin analizar los delitos a partir del uso de inteligencia artificial (IA) y su tipificación en la legislación penal ecuatoriana, se examinará a partir del progreso de la tecnología en paralelo, al mal uso de esta debido a que han aparecido una serie de nuevos delitos, siendo estos los retos que enfrenta la justicia. Según González Quintanilla, el Delito "es un comportamiento típico, antijurídico y culpable", esto marca un punto de referencia para poder entender la definición de los ciberdelitos o delitos informáticos, según el autor Almenar Pineda en el año 2017, "son vulneraciones que sufren los internautas por parte de delincuentes que roban información personal para usarla en beneficios de ellos"(Tixi-Janeta et al., 2023). En Ecuador, el Código Orgánico Integral Penal (COIP) carece de una legislación específica que regule los delitos a partir del uso de IA, lo que conlleva que ciertas conductas ilícitas queden impunes en el ámbito judicial

La problemática refleja en un vacío importante en el sistema legal, (Segovia Segovia & Flores Quishpi, 2025) debaten que la inteligencia artificial en Ecuador aún carece de regulación específica, lo que dificulta su integración al Código Orgánico Integral Penal (COIP) y la capacidad del sistema para responder adecuadamente a los delitos cometidos utilizando herramientas basadas en IA, lo que genera un impacto significativo en el sistema judicial, ya que permite procesar grandes cantidades de información y apoyar en la toma de decisiones legales, sin embargo, a pesar de estas ventajas, también existen riesgos importantes que deben considerarse. Según (Mariscal et al., 2024), los algoritmos que utilizan la IA pueden contener sesgos que afecten negativamente el debido proceso, especialmente para grupos vulnerables

A nivel de la responsabilidad penal, algunos expertos, como Gutiérrez, sostienen que la falta de transparencia y la dificultad de entender cómo funcionan los algoritmos complejos en IA limitan la capacidad de imputar responsabilidades, lo cual es crítico en un sistema que aún no incorpora plenamente estas tecnologías ni los riesgos asociados en sus normas legales (Gutiérrez, 2022). Además, (Rodríguez Barroso & Martínez Cisneros, 2024) señalan que actualmente hay una falta de regulación clara sobre quién debe asumir la responsabilidad cuando una decisión judicial automatizada resulta errónea o injusta. Por lo tanto, es fundamental que se desarrollen marcos normativos adecuados que permitan aprovechar los beneficios de la IA, pero también que protejan los derechos y garanticen la justicia para todos.

El interés de la presente investigación nace, por el aumento del uso de la inteligencia artificial en la vida diaria, transformando sectores como la economía, educación y la seguridad, ofreciendo oportunidades para mejorar la productividad, eficiencia y la prestación de servicios (Programa de las Naciones Unidas (PNUD), 2025). En Ecuador, ha nacido la necesidad de modernizar su sistema legal, para la protección de los derechos y la seguridad de las personas frente a los retos relacionados a la tecnología (Comisión Económica para América Latina y el Caribe (CEPAL), 2025). El país se prepara para enfrentar retos que trae

consigo el desarrollo de la tecnología, para poder garantizar la seguridad y protección de los derechos, es importante la actualización del marco legal en beneficio de la sociedad.

La presente investigación adopta un enfoque cualitativo y emplea el análisis documental junto con entrevistas, para revisar la situación legal actual en Ecuador y las posibles directrices para la tipificación de delitos relacionados con IA, se revisarán las leyes ecuatorianas e internacionales vigentes, sobre delitos tecnológicos, que sirvan de guía en la regulación de delitos asociados con la IA.

Se entrevistará a profesionales en derecho penal y tecnología, así como a legisladores que puedan proporcionar una visión práctica sobre la necesidad y las implicaciones de una legislación que regule los delitos derivados de la IA, ofreciendo una visión general de los desafíos y oportunidades que presenta la creación de una normativa penal específica, se realizará un análisis comparativo de los países que ya han implementado leyes o normativas específicas en relación a la IA y los delitos tecnológicos, para evaluar la aplicabilidad y eficacia de tales medidas en el contexto ecuatoriano.

Como objetivo se revisará los delitos, que nacen a partir del uso de la inteligencia artificial en Ecuador, en el ámbito penal, explorando cómo el marco legal actual aborda estos delitos emergentes, destacando la necesidad de adaptar la legislación penal ecuatoriana, para cubrir los vacíos legales presentes.

Se identificará en qué aspectos la legislación penal ecuatoriana carece de regulación específica sobre actividades delictivas que involucren IA, apuntando a áreas concretas que precisan una actualización normativa. para así lograr realizar un análisis de derecho comparado sobre la tipificación de delitos derivados de la IA en otros países, evaluando la viabilidad de aplicar enfoques legislativos extranjeros en el contexto ecuatoriano

1.2.Planteamiento del problema

La rápida evolución y adopción de la inteligencia artificial (IA) en diversas áreas ha generado problemas inherentes en el ámbito de la justicia penal, a nivel mundial se ha señalado que el uso de IA no solo ofrece herramientas avanzadas para la investigación de delitos, sino que también plantea un riesgo de su uso en conductas ilícitas, como manipulación de información, fraude y ataques cibernéticos (Chesterman, 2021).

Según el estudio de Chesterman en el 2021, existe un vacío legislativo que aborda específicamente los delitos generados por IA, representa un obstáculo importante para la administración de justicia, dado que el sistema penal no contempla aún con la tipificación de los delitos impulsados por tecnologías emergentes, lo que conlleva a una desventaja en la persecución penal, sino que además expone a la ciudadanía a riesgos asociados al mal uso de estas tecnologías (Chesterman, 2021).

A nivel global, el autor (Gutiérrez, 2022) indica, el aumento del uso de la inteligencia artificial en diversos sistemas judiciales, presenta desafíos éticos y jurídicos en países como

México y Estados Unidos, que enfrentan la necesidad de regular las tecnologías que influye, directamente en la determinación de culpabilidad y la toma de decisiones judiciales.

En relación a Latinoamérica, autores como (Rodríguez Mendoza & Maldonado Ruiz, 2024) mencionan, la limitada integración de la inteligencia artificial en el derecho penal de los países de la zona, siendo esto una dificultad para los sistemas de justicia, los cuales deben abordar delitos que involucran inteligencia artificial, como el fraude digital o la creación de perfiles falsos.

En Ecuador, la situación es aún más compleja. A nivel local, el marco penal actual carece de figuras específicas para tipificar delitos que utilicen IA, como la creación de perfiles falsos, la generación de deepfakes, o la manipulación de sistemas de reconocimiento facial para evadir la justicia. Según (López & Vieira, 2023), aunque la IA es una herramienta útil para prevenir ciertos delitos, también conlleva el riesgo de sesgos y discriminación produciendo una falta de regulación específica genera un problema en la aplicación de justicia, consiguiendo que los operadores jurídicos recurran a figuras penales tradicionales que no siempre abarcan la complejidad de estos delitos tecnológicos.

1.3.Justificación

Este trabajo de investigación es importante porque aborda una problemática emergente y compleja que afecta no solo a Ecuador, sino a todo el mundo, el uso indebido de la inteligencia artificial en actividades ilícitas, al ser una tecnología en rápida evolución, introduce nuevos tipos de amenazas y delitos, tales como el fraude automatizado, la suplantación de identidad digital, la manipulación de datos, la generación y difusión de contenido falso o íntimo sin consentimiento, los ciberataques a sistemas financieros y la desinformación automatizada mediante bots, que desafían los sistemas legales tradicionales. Ecuador, como muchos otros países, carece de una regulación penal específica que permita sancionar adecuadamente estos actos, lo cual deja a sus ciudadanos y sistemas vulnerables ante las consecuencias de estos delitos.

Esta investigación propone un marco de tipificación penal, relacionado con el uso de IA en Ecuador, debido a que en la actualidad no está regulado en la legislación penal, ofreciendo una base teórica. De esta manera permite que Ecuador se adapte a la era digital, creando un sistema de justicia penal moderno y eficaz, que este dirigido a la protección de los derechos.

La problemática de la investigación radica en el uso indebido de la inteligencia artificial, y el impacto que provoca en el sistema legal ecuatoriano, permitiendo que Ecuador avance hacia un sistema penal que sea capaz de enfrentar los desafíos actuales y futuros, lo que permitirá crear un entorno digital seguro, justo y regulado en beneficio de la sociedad.

La investigación se lleva a cabo por razones fundamentales que reflejan la necesidad urgente de que el Ecuador se adapte a los acelerados avances tecnológicos,

que aportan grandes beneficios, también generan riesgos y desafíos jurídicos que requieren una respuesta normativa oportuna, en este contexto, el estudio busca impulsar la creación de un marco legal adecuado que permita gestionar las implicaciones éticas, sociales y penales derivadas del uso de la IA, asimismo, pretende proteger los derechos fundamentales de los ciudadanos y garantizar que el sistema legal y judicial ecuatoriano esté debidamente preparado para identificar, tipificar y sancionar los nuevos delitos emergentes que surgen como consecuencia del desarrollo tecnológico contemporáneo.

La pertinencia del tema de investigación gira en torno, a los delitos derivados del uso de la inteligencia artificial y su falta de tipificación en la legislación penal ecuatoriana, lo que genera la necesidad de adaptarse al avance tecnológico, en busca de soluciones jurídicas, que fortalecen la protección de los derechos, para poder garantizar un entorno seguro para los ecuatorianos.

1.4.Objetivos

1.4.1. Objetivo General

- Analizar los delitos derivados del uso de inteligencia artificial (IA) en Ecuador y su impacto en el ámbito penal, abordando de manera adecuada en el marco legal actual, destacando la importancia de adaptar la legislación penal

1.4.2. Objetivos Específicos

- Examinar los tipos de delitos que pueden derivarse del uso de IA en actividades ilícitas, tales como fraude automatizado, manipulación de datos y creación de contenidos falsos, para comprender sus implicaciones legales y sociales.
- Identificar los vacíos y limitaciones en la legislación penal ecuatoriana actual respecto a la regulación de actividades delictivas que involucren IA, con el fin de identificar áreas específicas que requieren actualización normativa.
- Realizar un análisis del derecho comparado sobre la normativa de tipificación de delitos derivados del uso de la IA para su posible aplicabilidad en el contexto ecuatoriano.

CAPÍTULO II.

2. MARCO TEÓRICO.

2.1. Estado del arte

Respecto del tema "Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana" no se han realizados trabajos investigativos iguales; sin embargo, existen algunos similares al que se pretende realizar, cuyas conclusiones más importantes son las siguientes

Simon Chesterman, en el año 2021, realizó un trabajo investigativo titulado: "We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law", señalando que:

> La creciente integración de la inteligencia artificial en diversos aspectos de la vida moderna, desde los vehículos autónomos y el comercio de alta velocidad hasta la toma de decisiones algorítmica, plantea desafíos significativos para los sistemas jurídicos a nivel global incluido el ecuatoriano, la legislación penal enfrenta importantes limitaciones para abordar de manera efectiva los delitos relacionados con la IA, debido a la falta de marcos legales específicos que respondan a las particularidades de estas tecnologías, ocasionando que se genere vacíos normativos que dificultan el procesamiento y la definición de nuevos tipos de delitos asociados con el uso de sistemas autónomos. La exigencia para regular la IA no es solo de Ecuador, es un desafío general por considerar, para que las leyes pueden adaptarse a las nuevas tecnologías sin frenar la innovación. El autor menciona, que existen estudios sobre la regulación de la IA a nivel mundial, resalta la importancia de los riesgos, establecer límites, proporcionando al Ecuador una ruta para una respuesta jurídica efectiva, priorizando la seguridad.

Ugo Pagallo, en el año 2013, en su libro titulado: "The Laws of Robots: Crimes, Contracts, and Torts", señalando que:

> Las implicaciones legales de la inteligencia artificial (IA) en los ámbitos de crímenes, contratos y daños, analiza cómo las leyes actuales enfrentan desafíos al intentar abordar los problemas específicos relacionados con el uso de sistemas autónomos, como la responsabilidad en casos de daños y la transparencia en los procesos algorítmicos, destacando la necesidad de marcos regulatorios adaptados que consideren tanto las capacidades únicas como las limitaciones de la IA. Al examinar el impacto de los sistemas inteligentes en el derecho, sugiriendo que las leyes tradicionales podrían no ser suficientes para gestionar estos desafíos, resaltando como ejemplos internacionales las propuestas de autorregulación de la IA como estrategias complementarias para abordar estos problemas, señala la importancia de proteger el interés público en un panorama tecnológico que evoluciona rápidamente.

Janetsy Gutiérrez Proenza, en el año 2022, en su artículo científico titulado: "La responsabilidad jurídica de la inteligencia artificial desde el derecho clásico: The legal responsibility of artificial intelligence from classical law", menciona que:

> El desarrollo de la inteligencia artificial (IA) plantea tanto oportunidades como desafíos significativos para el marco jurídico tradicional, por un lado, reconoce los beneficios que la IA aporta a la vida cotidiana, como la automatización de tareas y la mejora en la toma de decisiones, por otro lado, señala la existencia de vacíos legales y la necesidad de adaptar el derecho para abordar cuestiones específicas relacionadas con la autonomía y las decisiones tomadas por sistemas de IA, la necesidad de crear un marco normativo que regule la IA para evitar daños, evitando que resulte en actos ilícitos, planteando la posibilidad de incluir una categoría jurídica especial, como la "persona artificial", para culpar a al IA en casos específicos. La responsabilidad recae sobre el ser humano, sin importar el rol que ocupe sea fabricante, programador o usuario, en lugar de atribuir personalidad jurídica a la IA, es importante indicar que la legislación se adapte al avance tecnológico, garantizando la seguridad jurídica y protegiendo los derechos, en una sociedad cada vez más influenciada por la IA.

Rodríguez Mendoza & Maldonado Ruiz, en el año 2024, en su artículo científico titulado: “Reflexión sobre el uso de la inteligencia artificial en la investigación penal en el Ecuador-análisis de su aplicabilidad en el derecho comparado”, concluye el mismo señalando que:

> La incorporación de inteligencia artificial (IA) en la investigación penal en Ecuador es una necesidad imperativa para abordar las deficiencias del sistema judicial, caracterizadas por su ineficiencia y los crecientes índices de delitos graves como homicidios y femicidios, señala que la experiencia internacional, en países como Argentina y Estados Unidos, ha demostrado que la IA puede acelerar los procedimientos judiciales, mejorar la identificación de infractores y prevenir delitos, ofreciendo beneficios significativos en términos de eficacia y eficiencia en la administración de justicia. Destaca la importancia de adaptar el marco normativo ecuatoriano, incluyendo el Código Orgánico Integral Penal, para regular el uso de inteligencia artificial en investigaciones penales, asegurando la protección de derechos fundamentales y la privacidad ciudadana, señala la necesidad de crear un marco ético sólido que garantice el uso legítimo de datos sensibles y una supervisión adecuada.

2.2. Aspectos teóricos

2.2.1. UNIDAD 1. FUNDAMENTACIÓN TEÓRICA Y CONCEPTUAL DE LA IA EN EL ÁMBITO PENAL

En el presente capitulo se enfoca en la introducción de la inteligencia artificial en relación con el ámbito penal, partiendo del concepto general de IA detallando aspectos teóricos y conceptuales, concerniente al contexto legal

2.2.1.1. Definición y características de la inteligencia artificial (IA) y su uso en actividades tecnológicas.

Para lograr definir lo que es inteligencia artificial es necesario considerar la evolución de desde su planteamiento inicial por John McCarthy en 1956, quien la definió como "la ciencia e ingeniería de hacer máquinas inteligentes" (McCarthy, 2007) de igual manera Russell y Norvig (2021) la caracterizan como "el estudio de los agentes que reciben percepciones del entorno y realizan acciones que maximizan sus posibilidades de éxito". Las diferentes definiciones de los autores, indican las capacidades para realizar procesos humanos, como el aprendizaje, el razonamiento y la toma de decisiones.

Características de la Inteligencia Artificial

La inteligencia artificial tiene diferentes cualidades que permite que sea una herramienta poderosa para la transformación digital considerando las siguientes las más importantes:

Aprendizaje automático

Permite a los sistemas mejorar su desempeño a partir de la experiencia sin ser programados explícitamente (Goodfellow et al., 2016). Esto nos quiere decir que ha tenido un aprendizaje la inteligencia artificial, logrando alcanzar avances en áreas como la predicción de datos, la clasificación de información y la optimización de procesos.

Procesamiento del lenguaje natural

Ayuda la socialización entre humanos y máquinas mediante la interpretación y producción de texto en lenguaje natural (Jurafsky & Martin, 2009). Debido a las diferentes herramientas han mejorado la traducción automática y el estudio de textos jurídicos (Bender et al., 2021).

Automatización de tareas

Los autores Brynjolfsson y McAfee mencionan, que la automatización de tareas tanto manuales como cognitivas, revoluciona la economía y la manera en que se trabaja, refiriéndose a reducción de la intervención humana en procesos repetitivos, incrementando la eficiencia y disminuyendo errores, de igual forma en actividades que requieren juicio y análisis, como la redacción de textos o la toma de decisiones, que ahora pueden realizarse de manera más eficiente y eficaz mediante algoritmos. Se debe tomar en cuenta, que los humanos deben fortalecer habilidades difíciles de replicar por la inteligencia artificial, como la creatividad, la empatía y el juicio ético. Tomando en cuenta eso podemos decir que, aunque la automatización optimiza procesos y mejora el rendimiento, también presenta complicaciones relacionados con el empleo y la distribución equitativa de los beneficios (Brynjolfsson & McAfee, 2016).

Capacidad de análisis de grandes volúmenes de datos

La inteligencia artificial tiene la capacidad para analizar grandes volúmenes de datos y encontrar patrones complejos, que el ser humano no, en palabras de Dhar y Domingos esta habilidad, de identificar conexiones y regularidades dentro de los datos, permite desarrollar algoritmos que mejoran su desempeño, ofreciendo resultados eficientes y precisos (Dhar & Domingos, 2016). Esto resulta relevante en el campo jurídico, donde la correcta interpretación y aplicación de la norma, requiere múltiples factores, la IA abre la posibilidad de crear sistemas de apoyo que agilicen y mejoren la administración de justicia.

Adaptabilidad

Menciona (LeCun et al., 2015), la inteligencias artificial opera en torno a la manera que es operada, dependiendo de la retroalimentación tiene la capacidad de un aprendizaje dinámico y continuo, lo que permite el desarrollo de sistemas de inteligencia artificial aplicados al derecho, sobre todo en la predicción de riesgos legales y el estudio de normativas que cambian constantemente. Debido a este aprendizaje, los sistemas pueden cambiar sus modelos y mejorar a medida que reciben nueva información, lo que resulta crucial para confrontar la complejidad presente en el ámbito jurídico.

El uso de la inteligencia artificial en actividades tecnológicas

El uso de la inteligencia artificial es amplio y en constante crecimiento gracias a sus diferentes campos de aplicación entre las más relevantes:

Automatización de procesos legales

Las diferentes inteligencias artificiales tienen la capacidad de analizar documentos jurídicos, identificando información clave que facilita la predicción de resultados judiciales, esta habilidad ha transformado el ámbito legal, mejora la gestión de casos y reducir los tiempos de respuesta, lo que contribuye a una administración de justicia más eficiente y accesible, ofrecen un apoyo fundamental para abogados y jueces, permite analizar más rápido y mayor cantidad de información legal (Susskind, 2019).

Ciberseguridad

Nos indica, (Handa et al., 2019) que el aprendizaje automático es una herramienta clave en la ciberseguridad, ya que permite detectar patrones de amenazas y prevenir ataques informáticos mediante el análisis de comportamientos anómalos en redes y sistemas. Este enfoque facilita la identificación temprana de brechas de seguridad, contribuyendo a reforzar la protección de datos y la integridad de la información en entornos digitales, en el ámbito jurídico, estas capacidades son fundamentales para garantizar la confidencialidad y seguridad de la información sensible manejada en procesos judiciales electrónicos, protegiendo la integridad de expedientes, testimonios y pruebas digitales, así el aprendizaje automático no solo fortalece la infraestructura tecnológica, sino que también asegura la continuidad y confiabilidad del sistema de justicia frente a posibles ciberataques (Handa et al., 2019).

Asistentes virtuales y chatbots

La inteligencia artificial está transformando la manera en que las empresas interactúan con sus usuarios, gracias a la automatización de respuestas y a la personalización de cada interacción. Esto no solo mejora la experiencia del cliente al recibir respuestas más rápidas y adaptadas a sus necesidades, sino que también ayuda a reducir los costos operativos al disminuir la carga de trabajo manual (Martínez Sandoval et al., 2019). Señala, (Huang & Rust, 2021) que la inteligencia artificial puede crear experiencias de servicio más involucradas y satisfactorias, ya que los sistemas inteligentes son capaces de entender mejor las preferencias y emociones de los usuarios, adaptándose a ellas de forma personalizada mejorando la relación entre el cliente y el servicio, sino que también genera mayor confianza y fidelidad, aspectos fundamentales en ámbitos sensibles como el legal, donde la claridad y el respaldo son esenciales.

Aplicación en el derecho

Según (Aletras et al., 2016) menciona, la inteligencia artificial demuestra una precisión del 79% en la predicción de sentencias del Tribunal Europeo de Derechos Humanos, lo que muestra su potencial en la asistencia a jueces y abogados. Estos son utilizados para mejorar el acceso a la justicia, debido a que ayuda a la toma de decisiones judiciales y automatizar tareas administrativas en los tribunales.

2.2.1.2. Concepto y elementos constitutivos de los delitos relacionados con la inteligencia artificial (IA)

La inteligencia artificial ha revolucionado numerosos ámbitos, desde la economía, medicina hasta la seguridad, ocasionando que se genere preocupaciones legales y éticas, especialmente en lo referente a la utilización para un posible delito , a medida que la inteligencia artificial se vuelve más autónoma y sofisticada, se vuelve más complicado poder determinar la responsabilidad legal en casos donde la intervención de la tecnología haya sido utilizada para cometer actos ilícitos (Calo, 2017; Pagallo, 2013). Entendiendo así que los delitos relacionados con la inteligencia artificial presentan un gran desafío para la justicia, debido que las normas tradicionales no siempre resultan aplicables a estas nuevas formas de delitos.

Concepto de delitos relacionados con la IA

Los delitos relacionados con la inteligencia artificial (IA) pueden definirse como aquellas conductas ilícitas en las que esta tecnología es empleada como herramienta, medio o agente facilitador en la comisión de un acto delictivo, en algunos casos, la IA actúa como instrumento directo para la ejecución del delito, mientras que en otros interviene de manera indirecta, dificultando la atribución de responsabilidad penal (Hildebrandt, 2016). De este modo, la inteligencia artificial puede ser utilizada tanto para la comisión activa de delitos como para encubrir o entorpecer su sanción entre los más frecuentes se encuentran el fraude automatizado, la suplantación de identidad digital, la manipulación de datos, la difusión de contenido falso o íntimo sin consentimiento.

Elementos constitutivos de los delitos en el ámbito penal

En el derecho penal clásico, los delitos se estructuran en cuatro elementos fundamentales: conducta, tipicidad, antijuridicidad y culpabilidad.

Conducta

Según Claus Roxin menciona que, "el delito es una conducta típicamente antijurídica y culpable, realizada por una persona capaz de responsabilidad penal" (Roxin, 2017, p. 95). En entorno a la inteligencia artificial, esta definición indica que la conduta delictiva recaer, en la programación intencionada para ejecutar actos ilícitos, lo que dificulta la atribución de responsabilidad penal. Así, cuando una empresa o desarrollador crea un algoritmo con la finalidad deliberada de discriminar, manipular información o vulnerar derechos, se configura una conducta humana jurídicamente imputable, aunque el acto sea ejecutado por un sistema automatizado (Hernández Giménez, 2019). Esta relación evidencia que, los delitos relacionados con la inteligencia artificial, la responsabilidad penal no recae sobre la máquina, sino sobre las personas que diseñan, implementan o utilizan la tecnología con fines ilícitos, en consecuencia, este tipo de comportamientos constituye una manifestación contemporánea de la criminalidad tecnológica, lo que refuerza la necesidad de establecer un marco normativo en el Ecuador que regule la autoría, participación y culpabilidad en los delitos cometidos mediante inteligencia artificial.

Tipicidad

Según Eugenio Raúl Zaffaroni, "la tipicidad es la adecuación de un hecho a la descripción contenida en la norma penal" (Zaffaroni, 2013, p. 421). No obstante, el desarrollo tecnológico ha creado vacíos legales, debido a que muchos delitos ayudados por la IA no están claramente tipificados en las legislaciones penales tradicionales, provocando que diversos autores propongan la actualización de los marcos normativos para incluir delitos específicos relacionados con la IA (Mantelero, 2018). Por ejemplo, en Ecuador aún no aparece un tipo penal que considere de forma clara, el uso de inteligencia artificial para la creación de deepfake, en estos casos, las autoridades deben recurrir a tipos penales tradicionales, como la difamación o el fraude informático contemplados en el Código Orgánico Integral Penal (COIP), lo que evidencia la necesidad de actualizar la normativa penal ecuatoriana para tipificar conductas emergentes vinculadas con el uso indebido de la IA.

Antijuridicidad

Jiménez de Asúa indica que "la antijuridicidad es la contradicción del hecho con el ordenamiento jurídico en su conjunto" (Jiménez de Asúa, 1964, p. 210). En los delitos de IA, pueden aparecer dilemas referentes a la antijuridicidad de ciertas acciones, como en los casos donde un sistema autónomo comete un error que deriva en un daño legal relevante, la determinación de si la acción fue realmente ilícita depende de múltiples factores, incluyendo la probabilidad del daño ocasionado y la existencia de controles adecuados sobre la IA (Gasser & Almeida, 2017). Desde una perspectiva crítica, en Ecuador existe una marcada

insuficiencia en la interpretación y aplicación del principio de antijuridicidad frente a conductas mediadas por IA, el sistema jurídico ecuatoriano aún se encuentra anclado en paradigmas tradicionales de autoría y culpabilidad humana, lo que genera vacíos cuando la acción lesiva proviene de algoritmos autónomos o decisiones automatizadas

Culpabilidad

Según Hans Welzel, "la culpabilidad es el juicio de reproche que se dirige al autor de la infracción penal por haber accionado en contra del derecho pudiendo haberlo evitado" (Welzel, 1980, p. 175). En este contexto, la responsabilidad penal podría recaer en el programador, si diseñó la IA con fines ilícitos, en el usuario si utilizó para cometer un delito o en la empresa desarrolladora, si permitió su uso indebido. Se introduce el concepto de responsabilidad distribuida, donde múltiples actores comparten la culpa (Bryson et al., 2017). Esto significa que la culpabilidad en los delitos relacionados con la IA no puede entenderse de manera unipersonal, como ocurre en los delitos tradicionales, en lugar de atribuir la infracción a un solo individuo, el análisis debe considerar toda la cadena de decisiones humanas y técnicas que permitieron el resultado lesivo, así, la culpabilidad no solo depende de la acción directa, sino también del grado de previsibilidad, control y negligencia en el diseño, entrenamiento o uso del sistema de IA.

2.2.1.3. Tipología de actividades ilícitas basadas en IA (fraude automatizado, manipulación de datos, generación de contenidos falsos, etc.).

La inteligencia artificial (IA), ha sido causante de diversos cambios que han transformado diversos sectores, pero también ha dado lugar a nuevas formas de actividades ilícitas. Según (Guszcza et al., 2020), la capacidad de la IA para automatizar procesos y replicar comportamientos humanos la convierte en una herramienta ideal para el fraude automatizado y otras actividades ilícitas. Entre las actividades ilícitas más preocupantes facilitadas por la IA se encuentran el fraude automatizado, la manipulación de datos y la generación de contenidos falsos tal como se describe en los estudios de (Chesney, Bobby; Citron, Danielle, 2019).

Fraude Automatizado

La inteligencia artificial tiene la capacidad de replicar el comportamiento de los usuarios para ejecutar fraudes, dificultando su detección, existen estudios recientes, donde la IA analiza un gran cantidad de datos y aprende patrones, lo que ayuda ejecutar transacciones fraudulentas, que se constituye un comportamiento ilegal, ocasiona que sean difíciles, de ser detectadas por sistemas tradicionales (John et al., 2025). Gracias a la inteligencia artificial, se puede modificar detalles de las transacciones, como montos o ubicaciones, sin que el usuario legítimo se dé cuenta, complicando poder identificar el delito (Chang et al., 2022). Esto ocasiona que sea más rápido la ejecución del fraude, superando las capacidades de monitoreo y prevención.

Suplantación de identidad

Investigaciones recientes describen cómo herramientas de IA generan identidades falsas a partir de datos reales y fabricados. Estas se usan para burlar sistemas de verificación de identidad, crear cuentas fraudulentas o engañar controles KYC (Know Your Customer) (Zhang et al., 2025). Nos explica, (LeCun et al., 2015) cómo los sistemas de IA pueden simular con gran precisión los comportamientos de usuarios reales, superando los mecanismos tradicionales de autenticación, como contraseñas o sistemas biométricos.

Manipulación de Datos

En la actualidad, el uso de la inteligencia artificial en el ámbito financiero representa un avance significativo para la detección y prevención de actividades ilícitas. Los algoritmos de aprendizaje automático han demostrado una capacidad superior para analizar grandes volúmenes de datos en tiempo real, identificando patrones sospechosos y anticipando operaciones fraudulentas con mayor eficacia que los métodos tradicionales (Martínez Pazos et al., 2024). Sin embargo, esta misma tecnología presenta riesgos al ser utilizada por actores malintencionados que emplean modelos generativos para alterar detalles de transacciones como montos, fechas y destinatarios dificultando la trazabilidad de fondos ilícitos y facilitando esquemas de lavado de dinero (Tang et al., 2025). Esta dualidad tecnológica evidencia la necesidad de fortalecer los marcos normativos y las herramientas técnicas destinadas a la investigación y sanción de delitos financieros, con el fin de garantizar la integridad y seguridad del sistema financiero (Oztas et al., 2024).Por tanto, el presente estudio aborda los desafíos que plantea la IA en la tipificación y control de delitos relacionados con la manipulación de datos y el lavado de activos en el contexto ecuatoriano.

Cibercrímenes

Según (Chesney, Bobby; Citron, Danielle, 2019) menciona, los cibercriminales están utilizando IA para diseñar malware altamente sofisticado que puede infiltrar sistemas y alterar información sin ser detectado, la capacidad de la IA para aprender de las interacciones previas y adaptarse a los sistemas de defensa es lo que hace que estos ataques sean especialmente peligrosos.

Manipulación en sistemas de votación y opinión pública

Nos afirma (Tufekci, 2017), que la IA divide a los votantes, identificando sus puntos débiles y generar contenidos que favorezcan a ciertos partidos o candidatos. Además, las IA pueden generar grandes volúmenes de publicaciones automatizadas en redes sociales para influir en elecciones, un fenómeno que ya se ha observado en procesos electorales recientes en varios países.

Generación de Contenidos Falsos

Nos anuncia (Chesney, Bobby; Citron, Danielle, 2019), que los deepfakes representan una gran amenaza para la privacidad y la democracia, teniendo en cuenta pueden ser utilizados para crear noticias falsas que engañan tanto a los sistemas de verificación como al público general, la facilidad de creación y la alta calidad visual de los deepfakes permiten que se difundan rápidamente en redes sociales, afectando la imagen de individuos, empresas

y gobiernos. Alerta (Lazer et al., 2018), que los deepfakes no solo afectan a individuos específicos, sino que pueden ser utilizados para alterar eventos de importancia global, como elecciones presidenciales o protestas sociales.

Según (Tufekci, 2017) señala, la IA genera y distribuye información manipulada que influye en las decisiones de las personas, debido a que analiza grandes cantidades de datos para crear, mensajes y publicaciones que son persuasivas, lo que produce efectos como la desinformación y la manipulación de la opinión pública. Explica (Dan, 2025), que los deepfakes, son contenido visual como videos o imágenes falsas creadas con inteligencia artificial, provoca un daño muy serio al prestigio de las personas. Esto afecta la imagen pública de quienes son víctimas, influenciando en el momento de tomar decisiones importantes, como el voto en elecciones o el apoyo a protestas sociales.

Implicaciones Sociales y Éticas del Uso Indebido de la IA en Actividades Delictivas

El uso indebido de la inteligencia artificial en actividades delictivas es una cuestión de gran relevancia en la sociedad contemporánea, por lo tanto, se plantea una serie de desafíos tanto desde el punto de vista social como ético. Como señalan (Bryson et al., 2017) la capacidad de la IA para tomar decisiones autónomas y procesar grandes volúmenes de datos hace que sea susceptible a ser utilizada con fines ilícitos, lo que requiere una intervención ética y regulatoria. La ética y la responsabilidad son los principios que regirán el desarrollo y la implementación de estas tecnologías, pero en la práctica, el uso indebido causa una serie de dilemas sociales, económicos, que requiere la intervención y regulación de las autoridades competentes (Guszcza et al., 2020). Desde esta perspectiva, se considera que en el contexto ecuatoriano la falta de políticas públicas y marcos legales específicos sobre el uso ético y responsable de la inteligencia artificial representa una debilidad significativa en la prevención de delitos tecnológicos, es necesario que el Estado ecuatoriano no solo adopte normas ante los delitos cometidos con IA, incentiva estrategias basadas en la educación digital y la cooperación interinstitucional, logrando fortalecer la capacidad institucional para identificar, controlar y sancionar el uso indebido de estas tecnologías, asegurando un equilibrio entre innovación y protección de derechos fundamentales.

Violación de Derechos Humanos

Se puede identificar que uno de los temas más delicados en torno al uso de la inteligencia artificial (IA) es el riesgo que representa para los derechos fundamentales, particularmente el derecho a la privacidad, en contextos donde se utilizan tecnologías como el reconocimiento facial o los sistemas de vigilancia automatizada, existe la posibilidad de que se recolecten grandes cantidades de datos personales sin el conocimiento ni el consentimiento de las personas, genera la vulneración directamente al derecho a la privacidad reconocido tanto en instrumentos internacionales como en normativas internas (Bu, 2021).

Además (Berghoff et al., 2020), sugiere que los sistemas de inteligencia artificial pueden ser manipulaciones, a través de técnicas como el data poisoning, esto consiste en modificar los datos que alimentan los algoritmos, ocasiona que los sistemas de IA genere

errores o tomen decisiones basadas en información falsa, lo que facilita fraudes y otros delitos digitales.

Ambas fuentes coinciden en que el avance de la inteligencia artificial sin una regulación jurídica adecuada puede tener consecuencias graves sobre derechos protegidos constitucionalmente, desde esta perspectiva se hace evidente la necesidad de que los marcos legales como el ecuatoriano, desarrollen mecanismos específicos para garantizar que el uso de la IA no derive en nuevas formas de criminalidad o abusos estructurales sobre la privacidad.

Desigualdad Social y Económica

Según (Bryson et al., 2017), el uso de IA para la automatización de trabajos en sectores como el comercio o la industria ha provocado la desaparición de empleos de baja calificación, dejando a millones de personas sin acceso a trabajos dignos, si bien la IA puede generar nuevas oportunidades laborales, las personas que carecen de habilidades tecnológicas a menudo quedan marginadas. Debido a la automatización de procesos mediante IA, que antes eran realizados por seres humanos, puede dar lugar a la destrucción de empleos y la exclusión digital de ciertos grupos sociales.

Según (O'Neil, 2016), los sistemas de IA entrenados con datos sesgados pueden excluir a grupos de minorías de servicios bancarios o financieros, reforzando las desigualdades preexistentes. Además, el uso de IA en el ámbito financiero para fraudes automatizados o manipulación de mercados ha incrementado las diferencias económicas. La exclusión económica que resulta de la mala utilización de la IA puede profundizar la brecha de riqueza en sociedades ya desiguales, dejando a ciertos grupos vulnerables más expuestos al daño causado por el uso ilícito de las tecnologías (Crawford & Paglen, 2021).

Desinformación y Pérdida de Confianza Pública

Una de las consecuencias sociales más preocupantes es la perdida de la confianza pública. (Lazer et al., 2018) sostienen, que la desinformación es una de las formas más fuertes de manipulación, porque IA ha potenciado a través de la creación de noticias falsas. Crear deepfakes para manipular el contenido en redes sociales, son factores que aporta para desinformar al público, provocando graves implicaciones en el campo político, social y cultural (Tufekci, 2017).

La credibilidad de los medios de comunicación es afectada cuando la IA es utilizada para manipular el contenido de manera oculta, lo que puede tener efectos devastadores (Lazer et al., 2018). Esto crea que se pierda la credibilidad, llevando a una crisis de en los medios de comunicación tradicionales.

Responsabilidad y Toma de Decisiones Éticas

En el ámbito ético, el uso indebido de la IA genera preguntas fundamentales sobre la responsabilidad y la rendición de cuentas. Según (Bryson et al., 2017), los sistemas de IA no tienen la capacidad de tomar decisiones éticas por sí mismos, por lo tanto la

responsabilidad recae en los desarrolladores y usuarios de estas tecnologías, este punto se vuelve crucial cuando se considera el uso de IA para cometer delitos, existen algoritmos que operan de manera autónoma, lo que hace difícil asignar responsabilidades claras en caso de actividades ilícitas.

Como señalan (Guszcza et al., 2020), es fundamental que el desarrollo y uso de la inteligencia artificial esté guiado por principios éticos que pongan en el centro los valores humanos, la transparencia y la responsabilidad, estos marcos no solo ayudan a construir tecnologías más confiables, sino que también buscan evitar que la IA sea utilizada con fines delictivos. Los autores resaltan que, para lograrlo es necesario contar con mecanismos que permitan detectar y sancionar a quienes hagan un uso indebido de estas herramientas, de esta forma se puede garantizar que la inteligencia artificial aporte beneficios reales a la sociedad sin poner en riesgo la seguridad ni los derechos de las personas.

Además, (O'Neil, 2016) subraya que los algoritmos utilizados en el sistema judicial y penitenciario tienen la obligación de ser transparentes y justos. El uso de IA en el ámbito judicial, como en la evaluación de riesgos o en las decisiones de libertad condicional, se garantizara que no exista discriminación basada en criterios sesgados, la falta de transparencia en el uso de IA en decisiones críticas puede socavar la justicia y la igualdad ante la ley (Chesney, Bobby; Citron, Danielle, 2019).

2.2.2. UNIDAD 2. ANÁLISIS JURÍDICO DE LOS DELITOS DERIVADOS DE LA IA

En el presente capitulo se enfoca en el análisis jurídico en el ámbito penal, partiendo del estudio de casos nacionales e internacionales cometidos mediante IA y poder determinar la responsabilidad de dichos delitos.

2.2.2.1. Estudio de casos nacionales e internacionales sobre delitos cometidos mediante IA (fraudes financieros, deepfakes, etc.).

En este capítulo se analizará casos reales, tanto en Ecuador como a nivel internacional, donde la inteligencia artificial ha sido utilizada como herramienta para cometer fraudes, suplantaciones de identidad, deepfakes y otras conductas ilícitas. Al revisar el documento de (Chavez Tapia,Keli Emperatriz & Chirre Quiquia, 2024), plantean una idea clave: "El marco penal tradicional no contempla con precisión las nuevas formas de criminalidad digital asistida por inteligencia artificial, lo que impide una adecuada sanción y prevención". Esta afirmación refleja un problema, la brecha entre lo que la tecnología puede hacer y lo que la ley alcanza a comprender y castigar.

Casos nacionales

En Ecuador, aún no se han judicializado delitos complejos vinculados al uso de IA, pero sí existen antecedentes sobre su uso en fraudes y suplantaciones. En un estudio reciente, (Cóndor Rosas, 2024) menciona, cómo los sistemas de respuesta automatizada han sido utilizados para efectuar estafas financieras en plataformas digitales. Lo más preocupante es,

que el Código Orgánico Integral Penal (COIP) no contiene normativas claras para sancionar, cuando el autor material es un sistema algorítmico. Como estudiante, esto deja claro que existe un vacío normativo que no puede ignorarse por más tiempo.

Otro caso que me impactó fue el presentado por (Arevalo Fernandez, 2024), quien analizó cómo en Ecuador se han producido montajes audiovisuales los conocidos deepfakes, con el fin de suplantar identidades, para extorsionar a personas, su tesis demuestra que el COIP no contempla ningún artículo que aborde de forma específica este tipo de manipulación digital, lo que impide a los fiscales calificar el hecho con precisión. (Arevalo Fernandez, 2024), concluye que esta omisión legislativa vulnera derechos fundamentales y deja en estado de indefensión a las víctimas. Esta lectura me permitió entender que la inteligencia artificial no solo desafía lo tecnológico, sino también la forma en que concebimos la imputación penal.

Casos internacionales

En los diferentes países de la región, los retos no son exclusivos del Ecuador, por ejemplo (ZAMBRANO LOAIZA & SUAREZ CASTRO, 2020), estudiaron el caso de deepfakes, según los autores, esta es otra técnica, esta vez basada en inteligencia artificial, que permite superponer imágenes o videos sobre otros o imitar voces con un nivel de realismo que hace muy difícil distinguir el contenido incorrecto del contenido real. Aunque el contenido causó un fuerte impacto mediático, la legislación colombiana no consideró el uso de IA como un agravante del delito, lo que demuestra que en muchos países todavía se legisla sobre el hecho y no sobre el medio tecnológico que lo potencia.

Un caso considerado clave fue el documentado por (Chavez Tapia,Keli Emperatriz & Chirre Quiquia, 2024) en Perú, su investigación analiza cómo una red delictiva utilizó sistemas de IA generativa para clonar voces y realizar llamadas bancarias falsas, esta forma de suplantación, tan sofisticada como eficaz, permitió sustraer datos confidenciales y ejecutar fraudes financieros, lo alarmante es que tal como señalan los autores estos hechos fueron procesados bajo normas generales de estafa, sin considerar el agravante tecnológico ni la complejidad algorítmica del delito. Esta omisión no solo reduce la eficacia de la sanción, sino que también desconoce la verdadera dimensión del daño generado por la IA maliciosa.

Finalmente, la propuesta de (Chivilches Seguil, 2023) me pareció una de las más interesantes, el plantea que los delitos cometidos con sistemas inteligentes no pueden ser tratados como simples delitos informáticos, sino como una nueva categoría penal que requiere su propio marco doctrinario, su argumento se basa en que la autonomía, replicabilidad y opacidad de los algoritmos exigen una revisión profunda de los principios penales clásicos. Este planteamiento me dejó claro que no basta con adaptar leyes, es necesario repensar el derecho penal desde la lógica de la tecnología.

2.2.2.2. Análisis de la aplicación Penal en delitos relacionados con IA. Literatura mundial

La inteligencia artificial ha revolucionado diversos campos, incluido el derecho penal, generando desafíos en la determinación de la responsabilidad y en la interpretación de los marcos normativos existentes, a medida que se vuelven más sofisticados, las legislaciones nacionales e internacionales han debido adaptarse para abordar los delitos relacionados con su uso indebido (Mercader Uguina, 2022).

Enfoques Globales sobre la Aplicación del derecho penal en Delitos Relacionados con IA

Latinoamérica: Regulación en Evolución

En la región latinoamericana, la IA se ha integrado en el sistema de justicia penal tanto para la prevención como para la investigación de delitos un claro ejemplo es el país de Argentina, que implementó Prometea, una IA utilizada en tribunales para agilizar procesos judiciales, sin embargo, la aplicación de la IA en el ámbito penal plantea interrogantes sobre la responsabilidad en caso de errores o sesgos algorítmicos (Corvalán, 2018).

Colombia ha planteado debates sobre el derecho penal frente a los avances tecnológicos, (Zabala Leal & Zuluaga Ortiz, 2021) señalan que el modelo penal tradicional, se basa en la culpabilidad del autor humano, presenta limitaciones cuando esta involucrado sistemas de IA que operan con cierto grado de autonomía, esto plantea un dilema jurídico relevante, si la inteligencia artificial causa un daño sin la participación humana, quién debe asumir la responsabilidad penal.

En Ecuador, (León, 2024) realiza un análisis sobre los desafíos que enfrenta el Código Orgánico Integral Penal (COIP) ante la incorporación de tecnologías automatizadas, identifica vacíos legales en la protección de datos personales, plantea la necesidad de crear sanciones específicas para quienes utilicen la IA con fines ilícitos, debido a que el ordenamiento penal ecuatoriano no contiene leyes que regulen el uso de la IA. Se concluye que, Ecuador debe crear una regulación penal, que garantice la protección de los derechos frente al uso indebido de la inteligencia artificial.

Europa: Protección de Derechos Fundamentales

La Unión Europea se ha consolidado como pionera en la regulación de la inteligencia artificial en el ámbito penal, especialmente con la entrada en vigor de la Ley de Inteligencia Artificial en agosto de 2024. Esta normativa establece restricciones claras sobre el uso de tecnologías como la vigilancia biométrica en tiempo real y los sistemas automatizados de toma de decisiones judiciales, destaca que dicho marco legal busca proteger derechos fundamentales, como la privacidad y el debido proceso, limitando la aplicación de IA en procedimientos penales únicamente a casos autorizados expresamente por una autoridad independiente (Yazici, 2025). Asimismo, (Mökander et al., 2022) señalan que los sistemas considerados de alto riesgo deben someterse a estrictos procesos de evaluación, auditoría y supervisión humana constante. Desde esta perspectiva, la Unión Europea se posiciona como

un referente global, evidenciando que es posible integrar avances tecnológicos en el ámbito jurídico sin comprometer la protección de derechos esenciales dentro del sistema de justicia.

En España, el uso de IA en la investigación de delitos, genera preocupaciones sobre la vulneración de derechos, se ha debatido que, en algunos casos la IA, ha sido utilizada para analizar patrones de comportamiento criminal, lo que podría ocasionar discriminación, si no se implementa una protección adecuadas (Mercader Uguina, 2022).

Estados Unidos: Enfoque Pragmatista

Estados Unidos tiene un enfoque más pragmático, en la regulación de la inteligencia artificial en el derecho penal, ha generado un intenso debate, en los sistemas de predicción criminal han sido objeto de críticas, debido a su potencial para perpetuar y reforzar sesgos raciales y socioeconómicos, lo que genera preocupaciones sobre la equidad y la justicia en su implementación (Richardson et al., 2019). Esto ocasiona la necesidad de crear marco normativo que regule la utilización y garantice la protección de los derechos fundamentales en el sistema penal.

En los casos cometidos con el uso de IA, las cortes han enfrentado dificultades para determinar la responsabilidad penal, siendo el principal problema la atribución de culpabilidad, cuando una IA es utilizada para cometer delitos como fraude financiero o manipulación de información en línea (Corvalán, 2018).

2.2.2.3. Determinación de responsabilidad en delitos cometidos con IA en al ámbito penal (autores, operadores, desarrolladores).

La inteligencia artificial, involucra a desarrolladores, operadores y autores, dificulta la atribución de responsabilidad penal bajo los esquemas legales tradicionales. En su articulo (Valls Prieto, 2023) sostiene, que la autonomía de la IA, crea zonas grises en las que es difícil determinar el responsable del daño si el programador, el proveedor o el usuario final. Esto ocasiona replantear, los elementos de imputación penal tales como la intención, la previsibilidad y el control humano, para que el sistema jurídico aborde los casos en donde la IA actúa de manera autónoma, por ello, no encaja en el modelo tradicional de culpabilidad.

Los Desarrolladores

Según (Valls Prieto, 2023), el principal desafío del uso de inteligencia artificial, radica en determinar si el desarrollador es considerado responsable por el delito cometido por su herramienta, especialmente en ausencia de dolo directo, esto se enmarca en la dificultad de aplicar categorías tradicionales del derecho penal como la intención, la autoría o la participación, debido a que los sistemas actúan con autonomía. Algunos autores manifiestan que los desarrolladores podrían enfrentar responsabilidad penal, si actúan con negligencia a pesar de conocer los riesgos del sistema, omiten tomar medidas preventivas.

(Valls Prieto, 2023), refuerza esta preocupación al indicar que los sistemas de inteligencia artificial, al involucrar a distintos actores como desarrolladores, operadores y usuarios finales, generan una estructura difusa que dificulta identificar con claridad quién

debe responder penalmente cuando ocurre un uso indebido o dañoso de estas tecnologías. El autor sostiene que, en ausencia de dolo directo, la imputación de responsabilidad podría basarse en formas de culpa o negligencia, especialmente en casos donde los sistemas son diseñados sin prever los posibles usos delictivos o sin incorporar salvaguardias técnicas suficientes, esto permite comprender que los marcos legales tradicionales resultan insuficientes frente a la complejidad de los entornos digitales actuales, por lo que se hace necesaria una adaptación normativa que contemple los riesgos propios de la autonomía tecnológica.

Los Operadores

La atribución de responsabilidad penal en uso de inteligencia artificial se ha centrado cada vez más en el papel de los operadores, supervisores técnicos de los sistemas. Según el estudio de (Kirpichnikov et al., 2020), la complejidad de los algorítmicos no exime a los operadores de sus obligaciones legales, al contrario se señala que podrían ser penalmente responsables, si no actúan con la diligencia debida para prevenir daños o usos indebidos de la IA, especialmente cuando omiten implementar salvaguardas que garanticen su uso seguro.

Este enfoque es respaldado por (Vladimír Smejkal & Jindřich Kodl, 2023), quienes sostienen que la falta de controles técnicos, como registros de auditoría o mecanismos de supervisión humana, puede convertir a los operadores en responsables directos en caso de que la inteligencia artificial sea utilizada para cometer un ilícito penal.

Ambas fuentes coinciden en que los operadores no pueden ser considerados actores pasivos dentro del ecosistema de la IA, su rol implica deberes concretos de prevención, control y reacción ante comportamientos anómalos del sistema, lo cual encuadra una posible imputación penal por acción, omisión o negligencia técnica, resulta fundamental entender que debe evolucionar el derecho penal frente a tecnologías autónomas que pueden generar daños sin intervención humana directa.

La figura del operador negligente es cada vez más relevante, en vista de que muchos delitos cometidos con IA podrían haberse impedido si los operadores hubieran implementado controles más estrictos(Valls Prieto, 2023).

Los Autores

El usuario final, quien directamente emplea la IA para cometer un delito, este rol se complica cuando los sistemas actúan de manera autónoma o cuando el usuario final no tiene pleno control (Valls Prieto, 2023). No obstante (Valls Prieto, 2023), indica que la línea entre el usuario y la máquina se pierde cuando la IA actúa de manera autónoma, planteando preguntas sobre la atribución de la culpa cuando el usuario pierde el control, o cuando este actúa más allá de su programación inicial.

En muchos casos, se considera responsable al autor de un delito, cuando se demuestra una intención delictiva, como sucede en escenarios de cibercrimen o fraude algorítmico (Morán Espinosa, 2021). No obstante, surgen vacíos legales cuando el resultado de un error del sistema o de una decisión tomada de forma autónoma, sin intervención humana. En

Ecuador, (Ordóñez Córdova, 2024) analiza cómo el marco legal vigente para los delitos informáticos todavía no tiene claridad este tipo de situaciones, lo que deja sin respuesta penal a casos donde el algoritmo actúa por sí solo y causa daños.

2.2.3. UNIDAD 3. PROPUESTA DE ABORDAJE NORMATIVO Y SOCIAL EN LA REGULACIÓN DE DELITOS ASOCIADOS AL USO DE IA EN EL DERECHO PENAL ECUATORIANO

Esta unidad propone mecanismos legales y sociales para abordar estos retos, considerando la tipificación de delitos, la responsabilidad de empresas y desarrolladores, y el rol de la sociedad y el Estado en la detección y sanción de conductas ilícitas.

2.2.3.1. Mecanismos Legales para Tipificar los Delitos Asociados al Uso de IA en el Marco Penal Ecuatoriano

En el contexto ecuatoriano, persiste una preocupación creciente dentro del ámbito jurídico respecto a los vacíos normativos que rodean la inteligencia artificial y su vinculación con los delitos, a pesar de que el Código Orgánico Integral Penal contempla algunas figuras vinculadas a los delitos informáticos, no existe hasta el momento una normativa específica que aborde los desafíos propios del uso de tecnologías autónomas e inteligentes. Esta situación ha sido advertida(Pozo-Caicedo & Rodríguez-Ruiz, 2025), quienes señalan que la ausencia de un marco legal actualizado, sumada a la limitada capacitación técnica de las autoridades judiciales, dificulta la adecuada persecución penal de este tipo de conductas.

Además, investigaciones como la de (Mecias et al., 2024), indica que el uso de IA complejizan la identificación de responsables y la trazabilidad de los hechos delictivos, generando obstáculos para las instituciones encargadas de garantizar la justicia penal. Desde esta perspectiva, el ordenamiento penal ecuatoriano necesita ser reformado, para adaptarse a los nuevos escenarios tecnológicos, en especial frente a los escenarios de los delitos cometidos mediante sistemas inteligentes.

Delitos asociados a la inteligencia artificial

El creciente progreso de la inteligencia artificial ha traído consigo no solo avances positivos, sino también una serie de desafíos en el ámbito penal, especialmente en lo relacionado con los delitos, el más preocupante dentro de este contexto es el fraude automatizado, un fenómeno en el cual la IA es utilizada para suplantar identidades, manipular sistemas financieros o ejecutar estafas masivas mediante redes de bots, en el caso ecuatoriano este tipo de conducta delictiva, todavía enfrenta vacíos legales significativos como lo evidencian los análisis de quienes destacan la necesidad urgente de adaptar el marco jurídico a estos nuevos escenarios tecnológicos (Pozo-Caicedo & Rodríguez-Ruiz, 2025).

En este sentido (Okdem & Okdem, 2024), explican que la IA se está utilizando tanto para diseñar como para contrarrestar amenazas en el ciberespacio, lo que obliga al Derecho Penal, a considerar los criterios de imputación y responsabilidad. Estos hallazgos refuerzan la idea, de que la inteligencia artificial ofrece grandes beneficios, pero su uso indebido

también crea escenarios delictivos que desafían las estructuras legales tradicionales, se debe analizar cómo deben responder los sistemas jurídicos, particularmente en contextos como el ecuatoriano, donde carece de una normativa específica sobre estos temas.

La inteligencia artificial ha hecho posible que los deepfakes, sean conviertan en una amenaza para los procesos judiciales, la misma que manipula imágenes, audios y videos de manera realista, facilitando su uso en acciones ilícitas como la extorsión, difamación y desinformación. De acuerdo con (Sandoval et al., 2024), los deepfakes son un riesgo para la justicia penal, ya que pueden emplearse para fabricar pruebas falsas, poniendo en riesgo la autenticidad de la evidencia y la credibilidad del sistema judicial.

Por otro lado (Hafez et al., 2025), explican que los delincuentes emplean modelos de aprendizaje automático para identificar patrones de transacción, suplantar identidades y evadir sistemas de detección tradicionales, aunque estas tecnologías pueden ser usadas para prevenir fraudes, su uso indebido crea una paradoja, en la que las herramientas diseñadas para la protección financiera también se convierten en instrumentos de crimen.

Finalmente (Mohamed, 2025), describe como los sistemas de inteligencia artificial están transformando la defensa digital, pero también están siendo aprovechados para generar malware, coordinar ataques automatizados y evadir sistemas de detección tradicionales, esto plantea que el derecho penal debe evolucionar para incorporar figuras como la responsabilidad por omisión o por riesgo tecnológico, permitiendo sancionar a los que emplean estas herramientas, como a quienes las dejan operar sin supervisión.

Marco normativo en Ecuador

La intervención de la inteligencia artificial en los diferentes ámbitos, ha provocado cuestionamientos en materia jurídica, sobre todo en lo penal, en el caso del Ecuador, aún no existe una legislación específica que regule los delitos cometidos a través del uso de IA, esto significa que, en muchos casos, deben ser tratadas mediante una interpretación extensiva de las normas ya existentes. El Código Orgánico Integral Penal (COIP), promulgado en 2014, establece ciertas disposiciones que pueden ser aplicadas a situaciones delictivas, aunque sin referirse directamente a la inteligencia artificial.

Por ejemplo, el artículo 178 del COIP, sanciona la violación a la intimidad, podría aplicarse si una persona utiliza IA para interceptar conversaciones privadas o difundir información sin autorización. Del mismo modo, el artículo 186, que trata sobre la estafa, podría abarcar casos en los que se utiliza IA, para suplantar identidades o generar deepfakes con el objetivo de engañar y obtener beneficios, esto demuestra que el marco normativo vigente puede adaptarse parcialmente, aunque con limitaciones (Ecuador, 2014).

Algunos investigadores han advertido sobre la urgencia de reformar el derecho penal para que pueda responder con mayor eficacia ante estos nuevos desafíos, un artículo titulado “Desafíos del derecho frente a los delitos de estafa coadyuvados por la inteligencia artificial (IA)”, publicado en la revista Sinergia Académica, plantea que es necesario incorporar figuras penales específicas para delitos cometidos mediante herramientas de IA, según el

autor, la falta de claridad legal pone en riesgo principios fundamentales del derecho penal como la tipicidad y la legalidad, y deja un vacío peligroso ante prácticas como la creación de perfiles falsos automatizados o fraudes masivos por medio de bots (Espinosa et al., 2024).

Otro trabajo relevante es el que se analiza el uso de inteligencia artificial para generar pornografía infantil sintética, este estudio argumenta que, aunque no se involucren víctimas reales, el daño social y el riesgo de normalización de estas prácticas justifican una tipificación penal autónoma en palabras de los autores, "la IA no solo facilita la comisión del delito, sino que también camufla al delincuente, haciendo más difícil su identificación y sanción"(Rosero & Oñate, 2025).

Además, desde una perspectiva de género, el artículo “Violencia digital contra la mujer e inteligencia artificial. Entornos legales cubano y ecuatoriano”, resalta cómo la IA puede ser usada para acosar, difamar o amenazar a mujeres en entornos digitales, las autoras plantean que el marco normativo ecuatoriano aún no ha incorporado herramientas legales que permitan proteger adecuadamente a las víctimas de esta forma de violencia, la cual es tan real y dañina como la ejercida en espacios físicos (Fuentes-Aguila & Muñoz-Alfonso, 2025).

Todo esto evidencia que el Ecuador se encuentra en un momento clave, si bien el COIP ofrece herramientas para sancionar ciertos delitos digitales, el avance tecnológico, especialmente en IA, ha superado la capacidad de respuesta del sistema penal, es urgente entonces pensar en una actualización normativa que contemple nuevos tipos penales relacionados con el uso indebido de la inteligencia artificial.

Modelos comparados y propuestas para Ecuador

El desarrollo de la inteligencia artificial, ha impulsado la necesidad de reformas jurídicas, en especial en el derecho penal, las experiencias extranjeras pueden servir como referencia, para el diseño de futuras reformas legislativas en Ecuador, donde aún no existe una normativa penal que regule el uso e implicaciones de esta.

Uno de los modelos más desarrollados es el de la Unión Europea, cuyo Reglamento de Inteligencia Artificial aprobado en 2024 propone una clasificación de sistemas de IA por niveles de riesgo, dicho reglamento prohíbe aplicaciones que representen un riesgo inaceptable, como la manipulación del comportamiento humano, el uso de algoritmos para vigilancia masiva o la categorización social basada en perfiles automatizados, aunque se trata de una norma de carácter preventivo y administrativo, sus disposiciones abren la puerta a responsabilidades legales, incluyendo la posibilidad de sanciones penales en casos graves (Campione et al., 2024).

Además, el Consejo de Europa, manifiesta la necesidad de garantizar mecanismos de control y responsabilidad cuando las decisiones automatizadas afectan derechos fundamentales, este convenio solicita a los Estados miembros a, asegurar la trazabilidad y la transparencia de los sistemas inteligentes, así como la creación de recursos legales, frente a daños derivados de su mal uso (Consejo de Europa, 2023).

Desde la doctrina, (Hueso, 2019) sostiene que el derecho penal clásico enfrenta limitaciones, sobre los delitos cometidos mediante sistemas automatizados, según el autor, propone que se reconozca el uso de IA como una circunstancia agravante en tipos penales ya existentes, y que se contemple la creación de figuras nuevas cuando el delito haya sido posible por medio de estas tecnologías. Además, plantea que la responsabilidad penal no debe limitarse al autor material, sino extenderse a desarrolladores, operadores, que utilicen IA para fines ilícitos (Hueso, 2019).

En América Latina, no existe una legislación penal específica sobre inteligencia artificial, algunos países han comenzado a discutir reformas sobre delitos informáticos y ciberseguridad, en México, por ejemplo, se han planteado propuestas para sancionar el uso de IA en la creación de perfiles falsos, manipulación de información y generación de imágenes de carácter sexual sin consentimiento (Campione et al., 2024).

Considerando esto Ecuador, podría iniciar un proceso normativo que incluya tres elementos fundamentales. Primero, la creación de tipos penales que sancionen el uso de IA, para cometer delitos como suplantación de identidad, fraudes automatizados o producción de pornografía digital. Segundo, la inclusión del uso de IA como agravante, reconociendo que estas tecnologías, pueden incrementar el daño o dificultar la detección del delito. Por último, se propone constituir la responsabilidad penal subsidiaria, para aquellas personas naturales o jurídicas que, mediante acción u omisión, facilitan la realización de delitos por IA.

Estas reformas, garantizara que la IA se utilice dentro de un marco legal, respetando los derechos fundamentales, adaptar la legislación penal ecuatoriana no solo es una necesidad jurídica, sino también una estrategia de protección frente a nuevas formas de criminalidad digital.

2.2.3.2. Establecimiento de estándares de responsabilidad para empresas y desarrolladores de IA en la prevención de delitos.

En Ecuador, el Código Orgánico Integral Penal (COIP) contempla la responsabilidad penal de las personas jurídicas, esta regulación resulta limitada frente a los desafíos actuales que plantea la IA, en este contexto, diversos autores proponen, se incorporen modelos penales empresarial, que permitan prevenir delitos tecnológicos a través de auditorías, protocolos éticos y control interno (Romero Jarrín & Vásquez, 2025). Por su parte, (Maldonado Montenegro, 2024) sostiene que el marco legal ecuatoriano no delimita con claridad las obligaciones de quienes operan sistemas inteligentes, en consecuencia, tanto empresas como desarrolladores deberían asumir una obligación, para evitar daños derivados del uso irresponsable o negligente.

Desde una perspectiva comparada, se observa las experiencias internacionales, como la normativa de la Unión Europea sobre IA, que plantea una responsabilidad objetiva para quienes diseñan y comercializan tecnologías de alto riesgo, tal como señala (Viveros Álvarez, 2022). En el contexto nacional, estudios como el de (Espinosa et al., 2024) menciona, que existen delitos como la estafa asistida por IA, que aún no cuentan con una

tipificación específica en el COIP, generando vacíos de imputabilidad penal. A su vez, (Redroban Ortiz & Cedeño Tapia, 2022) analiza el problema en Ecuador, donde empresas contratan servicios de IA sin verificar su legalidad ni su seguridad, incurriendo en una forma de negligencia empresarial. Finalmente, (Víctor Elian León Párraga, 2024) insisten en que la falta de regulación penal, sobre la inteligencia artificial genera inseguridad jurídica para usuarios, como para desarrolladores, por lo que urgen reformas legislativas que establezcan responsabilidad, ante conductas delictivas cometidas mediante sistemas inteligentes.

Responsabilidad de empresas y desarrolladores en el uso de IA

En Ecuador, si bien el marco jurídico reconoce la responsabilidad penal de las personas jurídicas (COIP, arts. 49 y 50), aún no se han definido los límites normativos sobre el uso ético y legal de la IA por parte de empresas y desarrolladores, en este sentido, existe un riesgo creciente de que estas sean utilizadas de forma inadecuada o incluso delictiva, sin que los actores responsables enfrenten consecuencias legales claras. Así, autores como (Marina, 2024) sostienen que es urgente diseñar un régimen jurídico, para establecer estándares mínimos de responsabilidad y deberes de supervisión continua, tanto en la fase de desarrollo como en la implementación de la IA, la ausencia de esto genera vacíos que podrían ser aprovechados para evadir responsabilidades.

Desde un enfoque preventivo, (Romero Jarrín & Vásquez, 2025) proponen la incorporación de mecanismos de control interno empresarial, como parte de programas de compliance penal, que exijan la evaluación constante de los riesgos asociados al uso de IA. Esto incluiría auditorías éticas, verificaciones técnicas de transparencia algorítmica y protocolos ante fallos automatizados. Por otro lado, (Víctor Elian León Párraga, 2024) identifican un serio problema en la falta de regulación penal específica para conductas derivadas de decisiones autónomas, lo que impide sancionar adecuadamente cuando, por ejemplo, un sistema automatizado toma una decisión discriminatoria, invasiva o manipuladora. En el mismo sentido, (Espinosa et al., 2024) argumentan que los desarrolladores deben asumir una obligación jurídica de prever los posibles usos indebidos de sus productos, y establecer limitaciones técnicas para evitar su uso en actividades ilícitas.

Normativas y estándares internacionales sobre responsabilidad en IA

La creciente influencia de la inteligencia artificial en la vida cotidiana ha puesto en evidencia una necesidad urgente, establecer normas claras sobre la responsabilidad de quienes desarrollan y aplican estas tecnologías, al investigar los modelos legales que otros países y organismos internacionales han propuesto, se vuelve evidente que Ecuador aún está en un estado incipiente en esta materia, pero también que existen referentes sólidos que pueden servir como base para futuras reformas.

Uno de los marcos normativos más avanzados en este ámbito es la propuesta de Reglamento de la Unión Europea sobre Inteligencia Artificial, conocida como AI Act, esta normativa, que aún se encuentra en proceso legislativo, propone una clasificación por niveles de riesgo y obliga tanto a desarrolladores como a usuarios a cumplir con mecanismos de supervisión, transparencia y control post despliegue, lo que más me llama la atención de este

reglamento es que se establece una responsabilidad clara sobre el desarrollador cuando no se cumplen los estándares mínimos de seguridad tecnológica, algo que podría ser replicado en nuestra legislación nacional (PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL, 2021).

Por otra parte, la UNESCO, a través de su Recomendación sobre la Ética de la Inteligencia Artificial, aporta una dimensión ética y preventiva. Este documento no es vinculante, pero sí tiene un gran peso moral y político. Allí se señala que los Estados deben garantizar que las empresas tecnológicas puedan ser legalmente responsables cuando sus sistemas causen daño o violen derechos humanos (UNESCO, 2022). A mí como estudiante de Derecho me parece fundamental este principio, porque refuerza la necesidad de anticiparse al daño, no solo de reaccionar cuando este ya ha ocurrido.

El enfoque adoptado por la OCDE, que presentó sus Principios sobre la Inteligencia Artificial, entre ellos, destaca el principio de responsabilidad y la exigencia de trazabilidad técnica, lo cual implica que los sistemas deben ser entendibles y auditables, para poder asignar responsabilidad en caso de fallos (Organización para la Cooperación y el Desarrollo Económicos, s. f.). Estos principios se basan en que la IA no debe quedar al margen de los marcos jurídicos existentes, y que los desarrolladores no pueden escudarse en la autonomía de sus sistemas para eludir su responsabilidad.

En cuanto al derecho comparado, países como España han comenzado a construir marcos normativos concretos, como su Carta de Derechos Digitales (2021), que propone derechos específicos frente al uso de tecnologías automatizadas. En dicha Carta se menciona el derecho a la no discriminación algorítmica, lo cual me parece clave, ya que abre la puerta a futuras acciones legales contra algoritmos que reproduzcan sesgos o causen daños sociales (Gobierno de España, 2021).

Finalmente, desde el ámbito académico, (Morán Espinosa, 2021) reflexiona sobre un punto que considero fundamental para mi tesis: la responsabilidad penal de la IA como una frontera que el derecho penal aún no ha cruzado del todo. El autor sugiere que los Estados deben comenzar a adaptar sus normas penales para enfrentar los nuevos riesgos derivados del uso de sistemas autónomos, incluso si eso implica repensar la teoría de la imputación penal tradicional. En su análisis, destaca que la responsabilidad no puede quedar vacía solo porque la conducta fue ejecutada por una máquina.

En resumen, las normas y propuestas internacionales analizadas promueven principios, como la transparencia, la responsabilidad y el control humano, en el contexto ecuatoriano son un referente para construir una legislación, que se adapte a los avances tecnológicos y garantice la protección los derechos de las personas.

Propuestas para el establecimiento de estándares de responsabilidad

Uno de los estudios que más influye es el de (Ormazabal Sánchez, 2024), quien realiza un abordaje crítico sobre la dificultad de probar responsabilidad civil cuando un daño

es causado por un sistema de IA, sostiene que los estándares tradicionales de prueba resultan inadecuados, debido a que las víctimas no cuentan con acceso ni conocimiento técnico suficiente para demostrar el funcionamiento defectuoso del algoritmo, por ello propone introducir presunciones legales de culpa, e incluso adoptar una responsabilidad objetiva para ciertos usos de IA, especialmente aquellos de alto riesgo. Este planteamiento es muy importante para países como Ecuador, donde el sistema probatorio penal sigue exigiendo carga de la prueba a la víctima incluso en contextos de clara desventaja tecnológica.

Además, la (PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL, 2021), refuerza la idea de que no solo debe sancionarse el daño, sino también prevenirlo desde el diseño del sistema, cabe destacar que, la normativa europea establece una serie de obligaciones para desarrolladores y usuarios de IA de alto riesgo, como auditorías técnicas, controles de calidad y análisis de impacto en derechos fundamentales. Lo más valioso de esta propuesta es que considera responsable no solo al creador del software, sino también a quien lo implementa sin garantizar su correcto funcionamiento. Este enfoque se complementa con la (Organización para la Cooperación y el Desarrollo Económicos, s. f.), que insiste en la necesidad de garantizar la trazabilidad y la rendición de cuentas en todo el ciclo de vida del sistema inteligente. Como estudiante, veo que estos principios tienen un valor normativo, aunque no vinculante, porque permiten establecer criterios comunes de responsabilidad a nivel internacional.

Por otro lado, la (UNESCO, 2022), en su Recomendación sobre la ética de la inteligencia artificial, exige que los algoritmos puedan ser entendidos por los seres humanos que los regulan o fiscalizan, este principio se considera especialmente útil cuando se piensa en un sistema penal como el ecuatoriano, donde la transparencia del hecho generador del daño es esencial para imputar responsabilidad penal o civil. Finalmente, todas estas propuestas, aunque diversas en origen, convergen en un punto común, la necesidad de que existan criterios jurídicos claros para identificar al responsable humano detrás del funcionamiento de la IA. Considero que Ecuador debería inspirarse en estos marcos para construir una legislación que no solo sancione, sino también prevenga el uso indebido de sistemas inteligentes, especialmente en sectores sensibles como el financiero, sanitario y judicial.

2.2.3.3.Rol de la sociedad y los organismos estatales en la detección y sanción de actividades ilícitas con IA

El avance acelerado de la inteligencia artificial ha traído consigo beneficios incuestionables, pero también nuevos desafíos para el Derecho penal. En este contexto, no solo basta con preguntarse cómo se cometen los delitos mediante IA, sino también quiénes son los llamados a detectarlos, prevenirlos y sancionarlos. A medida que estas tecnologías se integran en más espacios de la vida cotidiana, el rol tanto del Estado como de la sociedad se vuelve clave para garantizar que no se vulneren derechos ni se consolide la impunidad digital.

La respuesta del Estado frente al uso delictivo de la IA

El Estado ecuatoriano debe fortalecer su rol institucional frente a los delitos que involucran inteligencia artificial, este tipo de conductas no solo escapan a las formas tradicionales de criminalidad, sino que también exigen nuevas herramientas jurídicas y tecnológicas para poder ser detectadas y sancionadas a tiempo. Según (Montañez Sierra, 2020), plantea que la administración de justicia debe incorporar criterios técnicos y éticos sobre el uso de IA en investigaciones penales, lo cual me parece fundamental, ya que sin una comprensión clara de cómo funcionan estas tecnologías, es muy difícil atribuir responsabilidades o proteger los derechos de las víctimas.

Además, al analizar el Código Orgánico Integral Penal (COIP), considera ciertos delitos informáticos, pero no establece una regulación específica para los delitos cometidos mediante IA. En ese sentido, estudios como el de (Guamán Terán, 2023) insiste en la necesidad de reformar el marco penal ecuatoriano, para incluir delitos tecnológicos y establecer criterios de imputación cuando la IA es utilizada como herramienta delictiva. Es relevante pensar en una futura ley, que incorpore la participación de desarrolladores, plataformas tecnológicas y entidades públicas, tal como ya se está discutiendo en otras jurisdicciones.

El papel activo de la ciudadanía en la prevención y denuncia de delitos digitales

La sociedad no puede ser vista como una simple víctima pasiva frente a los delitos tecnológicos, por el contrario, la ciudadanía tiene un rol protagónico en la prevención, la educación digital y la denuncia activa de actividades ilícitas realizadas mediante IA. Por ejemplo, en el estudio de (Sinaluisa Sagñay, 2024) se plantea que una gran parte de los delitos digitales como los deepfakes de carácter íntimo o las estafas automatizadas no se denuncian porque las víctimas desconocen cómo funcionan estas tecnologías o no saben a qué entidad acudir, esto evidencia una brecha que no es solo tecnológica, sino también jurídica y cultural, y que puede solucionarse mediante campañas de alfabetización digital con enfoque legal.

Además, resulta muy interesante el trabajo de (Andrade Arias & Yurank Tsamaraint, 2025), quienes proponen crear observatorios ciudadanos de delitos informáticos que colaboren con las autoridades en la validación de evidencia digital y en el monitoreo de redes sociales, foros y plataformas en línea. Esta propuesta me parece sumamente acertada, porque reconoce que la detección temprana de delitos tecnológicos requiere una lógica colectiva, donde el Estado y la ciudadanía trabajen de forma coordinada. También se considera muy valioso lo señalado por la (UNESCO, 2022), al indicar que la gobernanza de la inteligencia artificial debe ser participativa, ética y corresponsable. En otras palabras, ni el Estado puede actuar solo, ni la sociedad puede mantenerse al margen de este fenómeno tan complejo.

CAPÍTULO III.

3. METODOLOGIA.

Con este propósito, en el presente estudio denominado “Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana.” se emplearon varios métodos, técnicas, instrumentos y recursos que permitieron alcanzar los objetivos planteados.

3.1. Unidad de análisis

La investigación se realizará en la ciudad de Riobamba en la Unidad Judicial Penal, se centra en los riesgos sobre el uso de IA en conductas ilícitas, identificando los vacíos legales, gracias al análisis de legislaciones internacionales. Se determinará cómo la legislación penal ecuatoriana se puede adaptar para tipificar estas nuevas formas de delitos.

3.2. Métodos

Para poder estudiar el tema los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana, se emplearán los siguientes métodos.

3.2.1. Método deductivo

El método deductivo “se realiza tomando como fundamento algunos principios o conocimientos generales que son aplicables para inferir conclusiones particulares en el área” Alcívar (2023).

3.2.2. Método jurídico-analítico

Por otro lado, el método jurídico-analítico que “ayudará a comprender las normas jurídicas en el contexto político, económico y social en el que surgieron, facilitando así una interpretación más completa” (Antar, 2016).

3.2.3. Método dogmático

El método dogmático según Alcívar (2023) se basa “en la legislación y la doctrina como fuentes del derecho objetivo; y eventualmente comprendería algún precedente vinculante, en tanto, tiene similar fundamento y efectos que la legislación”.

3.3. Enfoque de la Investigación

El enfoque de investigación para abordar el tema "Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana" es principalmente cualitativo, dado que nos permite analizar en profundidad los vacíos normativos, las doctrinas jurídicas y los desafíos éticos y sociales relacionados con estos delitos.

3.4. Tipo de Investigación

Por los objetivos que se pretende alcanzar, la presente investigación es de tipo investigación dogmática y la investigación jurídica explorativa.

3.4.1. Dogmática

La investigación dogmática “ubica al Derecho desde la ciencia o técnica formal concibiendo el problema jurídico desde una perspectiva formalista excluyendo el contexto social o todo elemento de la realidad relacionado con la norma jurídica, estructura legal o institución, tomando en consideración solo a las fuentes formales del Derecho concretamente la legislación y la doctrina, encargada solo de evaluar la estructura del Derecho” (Alcívar, 2023).

3.4.2. Jurídica explorativa

La investigación jurídica explorativa, según Tantaleán Odar (2015) “se utiliza cuando el tema a tratar es relativamente nuevo o desconocido para el investigador, es decir, cuando la literatura es escasa” (Tantaleán Odar, 2015). Este enfoque abre nuevos horizontes y genera conocimientos, sobre áreas nuevas en el campo del Derecho, contribuyendo a la investigación y expansión del conocimiento existente. Además, este tipo de investigación aborta el problema jurídico desde distintas perspectivas, generando una comprensión más profunda y completa del fenómeno estudiado.

3.5. Diseño de Investigación

El diseño de investigación es el plan que orienta el proceso de recolección, análisis e interpretación de datos, y establece cómo se estructurará el estudio. Para el tema "Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana", se ha optado por un diseño no experimental, ya que no se pretende manipular las variables, sino observar y analizar los fenómenos tal como se presentan en su entorno real. Este enfoque permite comprender de manera integral los aspectos legales, éticos, sociales y tecnológicos vinculados con el uso de la inteligencia artificial, así como su influencia en la configuración y aplicación del derecho penal ecuatoriano.

3.6. Población y muestra

La población es el número total de los elementos que se encuentran involucrados en el trabajo investigativo; en cambio la muestra es una parte representativa y significativa de la población. La población involucrada en la presente investigación está constituida por juez de la unidad judicial penal, fiscal y un abogado especializado en derecho penal en libre ejercicio.

3.7. Técnicas e instrumentos de investigación

Para la recopilación de la información se aplicaron las siguientes técnicas e instrumentos:

3.7.1. Técnica

La técnica de investigación en el presente trabajo es la entrevista sobre determinar las distintas aplicaciones que se están generando de la inteligencia artificial en la administración de justicia, específicamente en la toma de decisiones legales en procesos civiles.

3.7.2. Instrumento de investigación

El instrumento de investigación es la guía de entrevista, que serán utilizados para poder recabar información sobre la problemática presentada

3.8. Técnicas para el tratamiento de información

La técnica empleada para el tratamiento de la información se basó en el análisis siguiendo la secuencia de las preguntas abiertas de la encuesta aplicada a la población. La interpretación de los datos se realizó a través de la herramienta ATLAS.ti, mediante el análisis y síntesis, codificación de datos que fueron de interés para los objetivos de la investigación, considerando de la información obtenida**.**

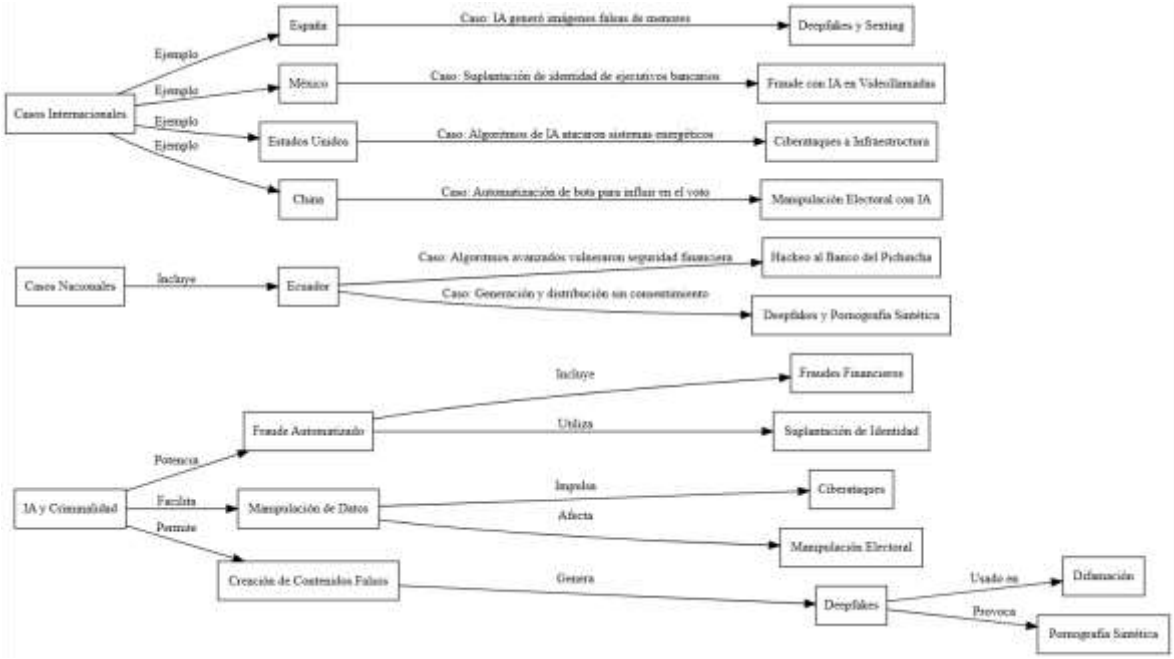
CAPÍTULO IV.

4. RESULTADOS Y DISCUSIÓN

4.1. Resultados

4.1.1. Los tipos de delitos que pueden derivarse del uso de IA en actividades ilícitas, para comprender sus implicaciones legales y sociales.

Figura 1. Mapa conceptual de tipos de delitos derivados del uso de IA



Fuente: Propia

La inteligencia artificial ha transformado vidas en muchos aspectos, pero, como toda tecnología poderosa, también ha caído en manos equivocadas, en los últimos años, se ha visto cómo se utiliza para cometer delitos de maneras que antes parecían sacadas de una película de ciencia ficción, desde fraudes automatizados hasta la manipulación de datos y la creación de contenidos falsos, estas nuevas amenazas plantean serios desafíos tanto legales como sociales.

El fraude siempre ha existido, pero con la IA ha alcanzado un nivel completamente nuevo, los delincuentes han desarrollado programas impulsados por inteligencia artificial que pueden automatizar ataques contra bancos y plataformas financieras, robando dinero e información en cuestión de segundos, lo más preocupante es que estos ataques son cada vez más elegidos, lo que hace que detectarlos sea un reto enorme.

La información es poder, y los ciberdelincuentes lo saben, lo que ha permitido gracias a la IA, alterar datos de formas casi imperceptibles, con consecuencias enormes, desde ataques a sistemas financieros y energéticos hasta la creación de noticias falsas para

manipular la opinión pública, la manipulación de datos se ha convertido en un arma peligrosa. El problema central es que vivimos en un mundo donde la información fluye a una velocidad impresionante, basta con que un dato falso se haga viral para que las consecuencias sean difíciles de revertir. Cuando se trata de información crítica, como la estabilidad de una economía o la seguridad de una nación, los efectos pueden ser devastadores.

Con la aparición de los deepfakes, es cada vez más difícil confiar en los vídeos, audios o imágenes que circulan en internet, debido a que estas herramientas pueden manipular los contenidos audiovisuales, generando desconfianza en instituciones. El uso preocupante de los deepfakes es la creación de pornografía falsa, sin el consentimiento de las personas involucradas, atentando contra la dignidad y reputación de las víctimas, constituyendo una forma grave de violencia digital.

El uso de la IA como herramienta para realizar actividades ilícitas ha crecido más rápido, que las propias leyes, es necesario actualizar la legislación para sancionar estos delitos de manera efectiva y proteger a las víctimas. Sin embargo, no basta con leyes, es necesario contar con educación digital y herramientas tecnológicas, que nos ayuden a detectar estos delitos antes de que se conviertan en problemas mayores.

No se trata de desacreditar a la inteligencia artificial, al contrario, es una herramienta poderosa que puede traer enormes beneficios si se usa de manera responsable. Sin embargo, se advierte que, si no toman medidas para frenar su uso indebido, corremos el riesgo de vivir en un mundo donde ya no podemos confiar en lo que vemos, leemos o escuchamos. La clave está en encontrar un equilibrio, impulsar el desarrollo tecnológico sin perder de vista la seguridad y la ética, porque la IA no es buena ni mala por sí misma, todo depende de cómo decidimos usarla.

Tabla 1. Tabla de las fuentes de noticias donde se evidencias los delitos que se muestran en la imagen.

Origen	**Caso**	**Delito configurado**	**Sanción en la legislación nacional**
España	IA generó imágenes falsas de menores.	Elaboración y difusión de imágenes sexuales falsas (deepfakes) de menores.	Sí, está tipificado, España reconoce la producción digital o simulada como parte del delito de pornografía infantil.
México	Suplantación de identidad, de ejecutivos bancarios.	Uso de IA, para la clonación de voz para cometer fraude financiero.	No está tipificado, pero se sanciona bajo delitos tradicionales aplicables.

Estados Unidos	Algoritmos de IA, se usaron para atacar sistemas energéticos.	Ciberataques automatizados, dirigidos contra infraestructura crítica.	Sí, existe cobertura legal, aunque sin mención en la IA.
China	Automatización de bots, para influir en el voto.	Manipulación electoral mediante bots de IA, generando desinformación.	No está tipificado, las sanciones son administrativas más que penales.
Ecuador	Algoritmos avanzados logran vulnerar la seguridad financiera.	Ataques informáticos dirigidos, a sistemas bancarios mediante IA.	Sí está tipificado, pero no hace referencia específica al uso de IA.
Ecuador	Generación y distribución imágenes, sin consentimiento.	Creación y difusión de imágenes íntimas. mediante IA sin consentimiento.	No está tipificado directamente, pero puede ser interpretada por el tipo penal.

Elaborado por: Robinsson Joel Ojeda Yanez

4.1.2. Vacíos y limitaciones en la legislación penal ecuatoriana actual respecto a la regulación de actividades delictivas que involucren IA, con el fin de identificar áreas específicas que requieren actualización normativa

Entrevistado 1

Menciona que la inteligencia artificial se relaciona con delitos tecnológicos, en Ecuador, no se ha avanzado mucho en la integración de la IA en el derecho penal, se han visto casos de IA involucrada en actividades delictivas, como hackeos, la legislación penal ecuatoriana está obsoleta y necesita reformas para abordar los delitos relacionados con IA de manera efectiva. Se necesitan nuevas normas, debido a que se identifican vacíos legales, especialmente en procedimientos para obtener pruebas en delitos tecnológicos. estos delitos impactan en las víctimas en términos económicos y de seguridad. Se sugieren reformas legales para incluir delitos relacionados con IA en el COIP, pero se enfrentarían desafíos al implementar estos cambios, la fiscalía general debe desempeñar un papel importante en la identificación y resolución de estos vacíos legales

Entrevistado 2

Destaca que la inteligencia artificial, es utilizada con mayor frecuencia en el área de informática, para reemplazar labores humanas, aunque no puede sustituir el razonamiento humano en derecho penal. La legislación penal ecuatoriana no aborda los delitos relacionados con IA, lo que nace la necesidad de reformas legales, guiándose en países con

experiencia, menciona que la reforma debe centrarse en los tipos penales afectados. Se debe reconocer el impacto de estos delitos, en las víctimas y en la complejidad procesal, se debe tomar en cuenta el papel importancia que juega los fiscales, jueces y abogados al momento de abordar, la necesidad de reformas para los delitos cometidos por IA.

Entrevistado 3

Señala que la inteligencia artificial, es un tema novedoso en el ámbito legal y su implementación en las leyes todavía no está regulada. En el derecho penal, la falta de normativa sobre la IA dificulta la imposición de sanciones a personas que cometan delitos relacionados, Ecuador no puede abordar adecuadamente estos delitos, en virtud que no está tipificada las conductas ni los procedimientos de sanción. Existen vacíos legales en áreas como la interceptación de comunicaciones, estafas cibernéticas y discriminación, donde la legislación no define claramente cómo actuar en casos relacionados con la IA. Los delitos con IA pueden tener un impacto significativo en las víctimas y complicar los procesos judiciales. Se sugiere reformar el COIP para regular el uso de IA en la comisión de delitos, estableciendo procedimientos y competencias claras para administradores de justicia. Los funcionarios del sistema judicial deben capacitarse sobre IA para poder identificar y resolver estos vacíos legales de manera efectiva.

4.1.2.1 Análisis por categorías

Brecha digital

En el entorno de la digitalización de la justicia, los diferentes expresan sus inquietudes y percepciones, sobre la brecha digital y el impacto en el ejercicio de sus funciones.

El abogado penalista menciona que, para los profesionales de su generación, les resulta complicado e incómodo, adaptarse al sistema procesal digital, explica que su formación y experiencia esta desarrollada en prácticas tradicionales, como la participación directa en audiencias y la presentación física de pruebas, lo que dificulta su cambio hacia las nuevas plataformas tecnológicas del ámbito judicial.

Desde el punto de vista del fiscal, se plantea una crítica a la creciente automatización del sistema judicial, considerando que las herramientas informáticas tienden a reemplazar funciones humanas, lo que genera preocupación sobre la posible pérdida del criterio humano en el proceso penal, siendo este un elemento esencial para garantizar la justicia y la valoración de caso.

Mientras que, un juez penal considera relevante la capacitación continua, en inteligencia artificial para todos los operadores de justicia, incluidos jueces, fiscales y defensores públicos. Destaca que, por el avance acelerado de la tecnología, es esencial mantenerse actualizado a través de, estudios y programas de formación, mejorando su capacidad para afrontar los retos que plantea la inteligencia artificial, tanto a corto como a largo plazo.

En conclusión, las opiniones, mencionan la necesidad de actualizar el sistema jurídico ecuatoriano, tanto en términos legislativos como en formación profesional, para lograr enfrentar los desafíos que presenta la brecha digital en el ámbito penal.

Daño a la imagen

Un experto en derecho penal aborda algunas de las preocupaciones más graves en este contexto. Menciona que, además de los riesgos asociados con la pornografía infantil y los delitos sexuales cometidos a través de plataformas digitales, existen otros tipos de delitos que afectan la moral pública, incluso aquellos que no requieren una introducción física, sino que atacan el pudor mediante medios electrónicos. Además, destaca el peligro que suponen las tecnologías, teniendo en cuenta que pueden vulnerar el secreto de información crucial, la cual puede ser obtenida de manera ilícita a través de hackeos.

Un fiscal indica, la creciente preocupación por el uso de IA en la comisión de delitos, entre uno de los casos se puede mencionar, la calumnia mediante publicaciones falsas generadas por IA, lo cual puede ocasionar afectación grave en la reputación y seguridad de las personas involucradas.

Finalmente, un juez penal explica los delitos más frecuentes que pueden ser facilitados por la tecnología, indica que las nuevas herramientas digitales pueden ser empleadas para llevar a cabo actividades ilegales como la interceptación de comunicaciones, el acceso no autorizado a información, la divulgación de secretos, fraudes a gran escala, acosos cibernéticos y discriminación.

Este panorama evidencia la creciente preocupación en el ámbito judicial, por la necesidad urgente de adaptar la legislación, a los retos impuestos por incremento del uso de la inteligencia artificial en la comisión de delitos.

Dificultades en la identificación de autores

Un abogado penalista señala que, en el Código Orgánico Integral Penal (COIP), aún no se ha abordado la obtención de pruebas en delitos cometidos mediante IA, considera que es necesario incorporar mecanismos específicos para este tipo de situaciones, dado que en la actualidad no existen directrices claras, sobre cómo manejar las pruebas relacionadas con delitos digitales.

Desde la perspectiva de un fiscal, se destaca la falta de regulación en torno a los delitos relacionados con la inteligencia artificial, señala que la legislación actual solo atribuye responsabilidad a los individuos, sin tomar en cuenta que en muchos casos es difícil determinar quién está detrás de estos actos, especialmente cuando se utiliza inteligencia artificial para cometerlos.

Un juez penal añade que, debido a la ausencia de un reconocimiento normativo en el COIP, actualmente es imposible imponer sanciones a quienes cometen infracciones

relacionadas con la inteligencia artificial. Menciona que, los administradores de justicia no pueden dictar resoluciones, en su opinión, es necesario aclarar a quién corresponde la responsabilidad en estos casos, ¿a la persona que creó el programa, a quien lo utiliza o al usuario final?

Impacto social de delitos con IA

El abogado penalista menciona que, una de las experiencias positivas derivadas de esta tecnología ha sido la incorporación de plataformas para audiencias telemáticas, implementadas por el Consejo de la Judicatura, este avance ha permitido a los abogados participar en audiencias sin importar su ubicación, lo que representa una aplicación práctica de la inteligencia artificial en el sistema judicial. No obstante, también advierte sobre los riesgos asociados a la ingeniosidad de las personas, señala que muchas veces, por la confianza en ofertas poco claras, los individuos caen en fraudes financieros, perdiendo grandes cantidades de dinero. Este tipo de imprudencias puede llevar a la comisión de delitos, pero las personas afectadas muchas veces no son conscientes de que están siendo engañadas.

Desde la perspectiva de un fiscal, se advierte que la IA tiene un poder significativo y que su mal uso puede generar consecuencias graves, dado que las actividades ilícitas pueden originarse en cualquier parte del mundo, se dificulta su control y sanción, a esto se suma la ausencia de una legislación específica sobre el tema. Los legisladores han reconocido la IA como una herramienta de apoyo académico y bibliográfico, pero no han abordado su uso indebido por parte de organizaciones criminales, esta laguna normativa permite que actores malintencionados exploten la tecnología con fines delictivos sin que existan mecanismos adecuados para sancionarlos.

Desde el punto de vista de un juez penal, advierte que el Código Orgánico Integral Penal del Ecuador no contempla disposiciones específicas para sancionar infracciones cometidas mediante IA, esta ausencia limita la actuación de los jueces para imponer sanciones, debido a que no se puede sancionar porque el delito no está tipificado. En este sentido, surge la necesidad definir con claridad de quién debe ser sancionado en estos casos, el creador del programa, el usuario que lo ejecuta o el destinatario final. Finalmente, el juez plantea una reflexión, el desarrollo pleno de la inteligencia artificial podría representar un desafío para la humanidad, en que el ser humano podría perder en contra las máquinas, esto resalta la urgencia de establecer un marco regulatorio, para evitar que la IA se convierta en una amenaza.

Propuestas legislativas en IA

Durante las entrevistas, se pudo destacar la urgente necesidad de que los asambleístas ecuatorianos, contemplen la necesidad de crear normas que tipifiquen delitos derivados del uso de la inteligencia artificial, los expertos en derecho penal mencionan que, es esencial que se actualicen las leyes y los procedimientos penales.

De acuerdo con lo mencionado, la reforma deberá incluir no solo la tipificación de los nuevos delitos, sino también establecer normas procesales específicas que aseguren que, el sistema judicial pueda abordar estos casos de manera efectiva. Mo obstante, se destaque que, en la actualidad, un fiscal de primer nivel no tendría acceso suficiente a la legislatura, para influir directamente en la elaboración de estas nuevas leyes, lo que restringe su capacidad de respuesta ante esta.

Los expertos están de acuerdo, en que se debe incorporar la IA en la legislación penal ecuatoriana, para lograrlo es necesario reformas urgentes, que aborden tanto la tipificación de los delitos como los procedimientos procesales, la cooperación internacional es esencial para reformar un sistema de justicia efectivo.

Regulación de la IA en Ecuador

Los entrevistados coinciden que Ecuador, enfrenta un vacío legal significativo sobre la regulación de los delitos cometidos mediante inteligencia artificial, para afrontar esto es necesario, realizar un análisis detallado y adaptar la legislación, para establecer procedimientos judiciales específicos y fortalecer la capacitación de los actores del sistema de justicia, sin una regulación adecuada, será difícil combatir eficazmente los delitos tecnológicos y garantizar la justicia.

Utilización de IA

En las entrevistas con los fiscales y jueces, se destacaron varios puntos cruciales sobre el impacto de la inteligencia artificial (IA) en el ámbito legal, la falta de regulación y los retos que enfrenta el sistema judicial ecuatoriano:

La IA es vista como una herramienta útil para la consulta rápida de información, lo que facilita el trabajo inicial de los fiscales y jueces, sin embargo, hay una preocupación sobre su uso malintencionado, considerando que no solo se utiliza para fines constructivos, sino también para cometer delitos. Actualmente, nuestra legislación no ha abordado este aspecto negativo de la IA, lo que deja un vacío normativo.

Los fiscales y jueces señalan que, la legislación ecuatoriana no se encuentra preparada para enfrentar los delitos cometidos con IA, el sistema penal ecuatoriano se basa en la "conducta humana", lo que crea un vacío cuando se trata de acciones en que la IA juega un papel importante, como en casos de discriminación generada IA.

Vacíos legales sobre IA

La inteligencia artificial (IA) ha dado lugar a nuevas formas de delitos que aún no cuentan con una regulación clara en el ámbito penal, lo que representa un reto para el sistema de justicia, uno de los mayores problemas es la falta de definición sobre qué entidad debe hacerse cargo de estos casos, especialmente cuando los delitos se cometen desde el extranjero, lo que provoca una incertidumbre, dificulta su investigación y judicialización.

Además, la legislación ecuatoriana ha quedado rezagada al ritmo de la tecnología, se reconoce el valor de la IA en la educación y otras áreas, no se ha tratado su uso con fines ilícitos, la firmeza de las leyes actuales no permite interpretar y sancionar delitos, que no están explícitamente contemplados, dejando vacíos legales que pueden ser aprovechados.

Desde el ámbito judicial, se señala que, sin leyes específicas, los jueces no tienen la capacidad de asignar responsabilidades, ni dar soluciones a estos casos, a pesar de que Constitución garantiza el acceso a la justicia, la falta de normativas impide una aplicación efectiva de la ley. En vista de esta situación es necesario, actualizar el marco legal ecuatoriano, fortaleciendo la cooperación internacional y capacitando a los operadores de justicia.

Análisis de ATLAS.ti

Figura 2. Diagrama de Sankey utilizando la información de entrevistas a expertos

Fuente: ATLAS ti

Elaborado por: Robinsson Joel Ojeda Yanez

El Diagrama de Sankey permite visualizar de manera clara, la compleja interconexión entre diversos factores asociados al impacto y regulación de la inteligencia artificial, abordando tanto sus implicaciones sociales como sus desafíos legales. Se observa que la brecha digital es un punto de partida fundamntal, pues la desigualdad en el acceso a la tecnología influye directamente en otros problemas derivados de la IA. Esta brecha se vincula, por ejemplo, con las dificultades al momento de identificar autores, afectando la protección de los derechos de propiedad intelectual, de igual forma se relaciona con el impacto en el derecho al honor y la imagen, una preocupación creciente donde la IA puede generar contenido falso.

Por otra parte, el diagrama destaca el impacto social de los delitos con IA, demostrando cómo la tecnología no solo facilita nuevas formas de criminalidad, sino que tambien genrera importantes dilemas éticos y jurídicos sobre la responsabilidad de sus acciones. De manera paralela, la presencia de la IA desarrolla un rol fundamental en la toma

de decisiones automatizadas, generando preocupaciones sobre la existencia de sesgos, en ámbito laboral al momento de la selección del personal y la administración de justicia.

A medida que estos factores se interconectan, el diagrama refleja cómo convergen en la necesidad de regular la IA en Ecuador, esto relacion evidencia la necesidad de desarrollar normativas que garanticen el uso responsable de la IA, garantizando la proteccion de los derechos sin frenar la innovación. Finalmente, el diagrama no solo indica los desafios actuales, sino que resalta la urgencia de establecer una administración tecnológica efectiva que equilibre el avance tecnológico con la justicia y la equidad social..

Tabla 2. Vacíos legales: Inaplicabilidad Penal de la IA en el Derecho Penal Ecuatoriano

Articulo	**Inaplicable en el caso de la IA**	**Analisis**
Art. 26.- Dolo	Aplicable solo entre humanos	Una IA no tiene conciencia ni intención, por lo tanto, no puede cometer delitos de forma voluntaria.
Art. 27.- Culpa	Aplicable solo entre humanos	La IA actúa con la intención de cometer el delito, pero quien la usa o programa sí puede incurrir en culpa.
Art. 42.- Autores	Aplicable solo entre humanos	La IA no es persona, no es sujeto de derecho penal, por lo tanto, no puede ser responsable.
Art. 43.- Cómplices	Aplicable solo entre humanos	La complicidad supone contribuir con conocimiento al delito, la IA puede ejecutar actos materiales, pero no con conocimiento o intención.
Art. 154.- Intimidación	Aplicable solo entre humanos	La IA puede ser canal para amenazas, pero la voluntad delictiva es siempre humana
Art. 154.1.- Instigación al suicidio	Aplicable solo entre humanos	La IA puede reproducir mensajes suicidas, pero no instiga por sí sola. Se acusa al humano detrás de la acción.
Art. 154.2.- Hostigamiento	Aplicable solo entre humanos	La IA puede operar como herramienta de acoso, si está programada, pero no tiene autonomía.
Art. 154.3.- Contravenciones de	Aplicable solo entre humanos	La IA puede ser utilizada para ejecutar actos como ridiculización, coacción o aislamiento, pero no

acoso escolar y académico		decide por sí mismo, la conducta infractora es atribuible a quien la controla docente, estudiante, autoridad.
Art. 186.- Estafa	Aplicable solo entre humanos	La IA no actúa con ánimo de lucro, solo el humano que comete la estafa es responsable.
Art. 231.- Transferencia electrónica de activo patrimonia	Aplicable solo entre humanos	La IA puede ejecutar las alteraciones, pero el usuario que ordena o diseña el ataque es penalmente responsable.
Art. 234.1.- Falsificación informática	Aplicable solo entre humanos	La IA puede de modificar o producir, documentos digitales falsos, pero carece de intención jurídica. La responsabilidad penal recae en el humano que maneja o dirige la IA.

Fuente: Propia

A partir del análisis detallado de varios artículos del Código Orgánico Integral Penal se ha podido constatar que, en la legislación penal ecuatoriana vigente, la inteligencia artificial no puede ser considerada como sujeto penalmente responsable, esto se debe a que los elementos esenciales de la imputación penal como la voluntad, la conciencia, el dolo o la culpa son características propias de los seres humanos, no de sistemas autónomos, por más avanzados que estos sean.

Se ha observado que la IA puede estar involucrada en la comisión de ciertos delitos, pero siempre como una herramienta o medio, nunca como el autor del hecho, aunque la IA puede generar documentos falsos, difundir amenazas o manipular datos informáticos, la responsabilidad penal recae en la persona que la programó, la dirigida o la utilizada con un fin delictivo, por sí sola carece de intencionalidad y de capacidad para comprender la ilicitud de sus actos.

Por tanto, se considera que el COIP, si bien contempla estas conductas, no está aún preparado para abordar con claridad los desafíos que plantea la inteligencia artificial en contextos más autónomos o complejos, esto permite concluir que es urgente promover un debate jurídico y legislativo más profundo sobre cómo debe responder el Derecho Penal frente al uso creciente de tecnologías inteligentes. El sistema legal ecuatoriano, al mantenerse centrado en la imputación exclusivamente humana, corre el riesgo de dejar vacíos normativos frente a nuevas formas de criminalidad digital mediada por algoritmos.

4.1.3. Análisis de Derecho Comparado sobre la Tipificación de Delitos Derivados del Uso de la inteligencia artificial y su Aplicabilidad en el Contexto Penal Ecuatoriano

El análisis comparado de la normativa es clave para su posible aplicación en Ecuador, mientras países como Estados Unidos, Japón y la Unión Europea cuentan con marcos legales

que regulan delitos como el fraude automatizado, la manipulación de información y los ciberataques mediante IA, Ecuador aún carece de una legislación específica. Realizar un análisis del derecho comparado sobre la normativa de tipificación. A continuación, se presenta un análisis comparativo de países con sus legislaciones. Cada una de las legislaciones ha sido evaluada en términos de Dimensiones Doctrinales Jurídicas, Marco Legal, Jurisprudencia y su Aplicabilidad al Contexto Ecuatoriano.

Tabla 3. Cuadro comparativo sobres las normativas de tipificación de delitos derivados del uso de la IA de diferentes países

País	**Dimensiones Doctrinales Jurídicas**	**Marco Legal**	**Jurisprudencia**	**Aplicabilidad Detallada al Contexto Ecuatoriano**
Estados Unidos	Enfoque centrado en la responsabilidad civil y penal, con énfasis en la imputabilidad de personas jurídicas y desarrolladores de IA.	Marco legal fragmentado: leyes federales como el Computer Fraud and Abuse Act (CFAA) y normativa estatal.	Casos relacionados con cibercrimen, privacidad y responsabilidad de desarrolladores.	Puede servir de modelo para delimitar responsabilidades individuales y corporativas en delitos cometidos con IA. La experiencia estadounidense puede orientar la tipificación penal de conductas específicas (como la manipulación algorítmica o accesos no autorizados mediante IA) y definir el rol de los desarrolladores en estos contextos
Unión Europea	Regulación específica en desarrollo (AI Act), con énfasis en el principio de precaución y estándares éticos.	Reglamento General de Protección de Datos (GDPR) y propuestas como el AI Act.	Jurisprudencia emergente del TJUE sobre responsabilidad por decisiones automatizadas.	Este modelo puede inspirar la creación de una normativa ecuatoriana centrada en los derechos fundamentales, el consentimiento informado y la trazabilidad de los algoritmos. El enfoque ético y precautorio europeo puede ser útil para prevenir abusos y proteger a usuarios frente a decisiones automatizadas.
Japón	Prioriza la ciberseguridad y la regulación ética de la	Ley de Servicios Financieros, Ley de Seguridad	Casos centrados en fraudes digitales y vulneraciones de seguridad.	Aplicable para mejorar la legislación ecuatoriana en materia de ciberseguridad y protección de infraestructuras críticas.

	IA, con atención especial a delitos tecnológicos y financieros.	Cibernética y guías regulatorias para la IA.		Japón ofrece un enfoque preventivo y técnico que puede adaptarse a la lucha contra el fraude bancario o los delitos cibernéticos ejecutados con IA.
Brasil	Enfoque emergente en la responsabilidad de plataformas digitales y regulación de algoritmos.	Marco Civil de Internet; Ley General de Protección de Datos (LGPD).	Jurisprudencia sobre responsabilidad de plataformas ante contenido ilícito o delictivo.	Es especialmente útil para Ecuador por su cercanía jurídica y lingüística. Este modelo ofrece una base para responsabilizar a plataformas tecnológicas que operen en el país, garantizando una supervisión efectiva del uso de IA, especialmente en redes sociales, comercio electrónico y servicios digitales.
Ecuador	Enfoque incipiente; el derecho penal no contempla específicamente los delitos cometidos mediante IA.	Código Orgánico Integral Penal (COIP), sin disposiciones específicas.	Escasa jurisprudencia en temas de IA o delitos tecnológicos avanzados.	Se requiere una reforma integral que incluya tipificaciones específicas, delimitación de sujetos responsables personas naturales y jurídicas , y mecanismos de control ético y técnico. La experiencia comparada puede servir como base para una legislación proactiva y orientada a la protección de derechos y la seguridad jurídica en el uso de IA.

Fuente: Propia

El análisis comparativo muestra una diversidad de enfoques, útiles para orientar el desarrollo normativo en Ecuador, en Estados Unidos predomina un modelo centrado en la responsabilidad civil y penal, con énfasis en la imputabilidad de desarrolladores y entidades jurídicas, la Unión Europea, avanza hacia una regulación basada en principios éticos, el consentimiento informado, Japón orienta sus esfuerzos en la ciberseguridad y la prevención de delitos tecnológicos y financieros, mientras que Brasil ha iniciado, regular de forma más activa las plataformas digitales, ofreciendo un referente cercano por su similitud jurídica con Ecuador.

Frente a estos avances, el marco legal ecuatoriano aún se encuentra en una etapa inicial**,** el Código Orgánico Integral Penal no contempla disposiciones específicas sobre delitos cometidos mediante IA y la jurisprudencia en la materia es escasa, esto comprueba la necesidad urgente de una reforma normativa que incluya la tipificación clara de nuevas conductas delictivas, la definición de responsabilidades para personas naturales y jurídicas, y el establecimiento de mecanismos éticos y técnicos de control, con la ayuda de la incorporación de las experiencias internacionales no solo permitirá fortalecer la seguridad jurídica, sino también anticiparse a los desafíos que plantea la creciente inclusión de tecnologías inteligentes en los distintos ámbitos de la vida social y económica.

Posibles reformas de ley para la legislación penal ecuatoriana sobre la IA.

Art. 26.- Dolo. - Actúa con dolo la persona que, conociendo los elementos objetivos del tipo penal, ejecuta voluntariamente la conducta. Responde por delito preterintencional la persona que realiza una acción u omisión de la cual se produce un resultado más grave que aquel que quiso causar, y será sancionado con dos tercios de la pena (Ecuador, 2014).

Propuesta reforma:

Art. 26.- Dolo y dolo tecnológico.

Actúa con dolo la persona que, conociendo los elementos objetivos del tipo penal, ejecuta voluntariamente la conducta. Se considerará también que existe dolo cuando la conducta se realiza mediante el uso de sistemas automatizados o de inteligencia artificial, siempre que la persona haya tenido control funcional, técnico o decisión sobre el sistema, y haya previsto, tolerado o deseado el resultado dañoso o antijurídico.

Responde por delito preterintencional la persona que realiza una acción u omisión de la cual se produce un resultado más grave que aquel que quiso causar, y será sancionada con dos tercios de la pena prevista.

Art. 27.- Culpa. - Actúa con culpa la persona que infringe el deber objetivo de cuidado, que personalmente le corresponde, produciendo un resultado dañoso. Esta conducta es punible cuando se encuentra tipificada como infracción en este código.(Ecuador, 2014)

Propuesta reforma:

Artículo 27.- Culpa. Actúa con culpa la persona que infringe el deber objetivo de cuidado, que personalmente le corresponde, produciendo un resultado dañoso. Esta conducta es punible cuando se encuentra tipificada como infracción en este Código.

En el contexto del uso, desarrollo o supervisión de sistemas tecnológicos o de inteligencia artificial, se entenderá que existe infracción al deber de cuidado cuando la persona, actuando con negligencia, imprudencia, impericia o inobservancia de reglamentos técnicos, genera un riesgo jurídicamente desaprobado que produce un resultado dañoso.

La responsabilidad por culpa podrá atribuirse también a quienes, teniendo deberes de supervisión, control o mantenimiento de sistemas automatizados, omitan medidas razonables para evitar el daño.

Art. 42.- Autores. - Responderán como autoras las personas que incurran en alguna de las siguientes modalidades:

1. Autoría directa:

a) Quienes cometan la infracción de una manera directa e inmediata.

b) Quienes no impidan o procuren impedir que se evite su ejecución teniendo el deber jurídico de hacerlo.

2. Autoría mediata:

a) Quienes instiguen o aconsejen a otra persona para que cometa una infracción, cuando se demuestre que tal acción ha determinado su comisión.

b) Quienes ordenen la comisión de la infracción valiéndose de otra u otras personas, imputables o no, mediante precio, dádiva, promesa, ofrecimiento, orden o cualquier otro medio fraudulento, directo o indirecto.

c) Quienes, por violencia física, abuso de autoridad, amenaza u otro medio coercitivo, obliguen a un tercero a cometer la infracción, aunque no pueda calificarse como irresistible la fuerza empleada con dicho fin.

d) Quienes ejerzan un poder de mando en la organización delictiva.

3. Coautoría:

Quienes coadyuven a la ejecución, de un modo principal, practicando deliberada e intencionalmente algún acto sin el cual no habría podido perpetrarse la infracción (Ecuador, 2014).

Propuesta reforma:

Artículo 42.- Autores. – Responderán como autoras las personas que incurrirán en alguna de las siguientes modalidades:

1. Autoría directa

a) Quienes cometan la infracción de manera directa, inmediata o mediante el uso de sistemas tecnológicos o inteligencia artificial, siempre que haya un control funcional del hecho.

b) Quienes no impidan o procuren impedir que se evite su ejecución teniendo el deber jurídico o técnico de hacerlo, incluyendo cuando ello implique la supervisión o control de herramientas informáticas o de sistemas automatizados.

2. Autoría mediata:

a) Quienes instiguen o aconsejen a otra persona o programa informático para que cometa una infracción, cuando se demuestre que tal acción ha determinado su comisión.
b) Quienes ordenen o configuren la comisión de la infracción valiéndose de otra u otras personas, imputables o no, o de sistemas automatizados, mediante precio, dádiva, promesa, ofrecimiento, orden o cualquier otro medio fraudulento, técnico, digital, directo o indirecto.

c) Quienes, por violencia física, abuso de autoridad, amenaza u otro medio coercitivo, obligan a un tercero a cometer la infracción, aunque no pueda calificarse como irresistible la fuerza empleada con dicho fin.

d) Quienes ejerzan un poder de mando en la organización delictiva o en la planificación de operaciones mediante el uso de inteligencia artificial.

3. Coautoría:

Quienes coadyuven a la ejecución de un delito, de un modo principal, practicando deliberada e intencionalmente algún acto sin el cual no habría podido perpetrarse la infracción, incluso cuando estos actos implican el diseño, entrenamiento, programación o implementación de tecnologías de inteligencia artificial.

Art. 43.- Cómplices. - Responderán como cómplices las personas que, en forma dolosa, faciliten o cooperen con actos secundarios, anteriores o simultáneos a la ejecución de una infracción penal, de tal forma que aun sin esos actos, la infracción se habría cometido. No cabe complicidad en las infracciones culposas. Si de las circunstancias de la infracción resulta que la persona acusada de complicidad coopera en un acto menos grave que el cometido por la autora o el autor, la pena se aplicará solamente en razón del acto que pretendió ejecutar. El cómplice será sancionado con una pena equivalente de un tercio a la mitad de aquella prevista para la o el autor (Ecuador, 2014).

Propuesta de reforma

Artículo 43.- Cómplices. - Responderán como cómplices las personas que, en forma dolosa, faciliten o cooperen con actos secundarios, anteriores o simultáneos a la ejecución de una infracción penal, aun cuando tales actos se realicen mediante sistemas informáticos, medios digitales o el uso de inteligencia artificial, siempre que, sin dichos actos, la infracción se habría cometido igualmente.

No cabe complicidad en las infracciones culpables. Si de las circunstancias de la infracción resulta que la persona acusada de complicidad cooperó en un acto menos grave que el cometido por la autora o el autor, la pena se aplicará solamente en razón del acto que pretendió ejecutar. El cómplice será sancionado con una pena equivalente de un tercio a la mitad de aquella prevista para la o el autor.

Art. 154.- Intimidación. - La persona que amenace o intimide a otra con causar un daño que constituya delito a ella, a su familia, a personas con las que esté íntimamente vinculada, siempre que, por antecedentes aparezca verosímil la consumación del hecho, será sancionada con pena privativa de libertad de uno a tres años. La pena será de tres a cinco años si la amenaza o intimidación se realiza contra una servidora o servidor público con el propósito de que actúe de manera contraria a la normativa legal vigente y los deberes que le impone el ejercicio de su función (Ecuador, 2014).

Propuesta de reforma

Artículo 154.- Intimidación. - La persona que, por sí misma, mediante terceros, o utilizando herramientas tecnológicas o sistemas de inteligencia artificial, amenace o intimide a otra con causar un daño que constituya delito a ella, a su familia, a personas con las que esté íntimamente vinculadas, será sancionada con pena privativa de libertad de uno a tres años, siempre que, por los antecedentes, el medio empleado o la naturaleza del mensaje, verosímil la consumación del hecho.

La pena será de tres a cinco años si la amenaza o intimidación se realiza contra una servidora o servidor público, con el propósito de que actúe de manera contraria a la normativa legal vigente o los deberes que le impone el ejercicio de su función, ya sea de forma directa o mediante el uso de medios informáticos, telemáticos o sistemas automatizados.

Art. 154.1.- Instigación al suicidio. - Será sancionada con pena privativa de la libertad de uno a tres años, la persona que induzca o dirija, mediante amenazas, consejos, órdenes concretas, retos, por medio de cualquier tipo de comunicación verbal, física, digital o electrónica existente, a una persona a que se provoque daño así mismo o ponga fin a su vida, siempre que resulte demostrable que dicha influencia fue determinante en el resultado dañoso (Ecuador, 2014).

Propuesta reforma:

Art. 154.1.- Instigación al suicidio. - Será sancionada con pena privativa de libertad de uno a tres años la persona que, de forma directa o a través de sistemas automatizados, inteligencia artificial, aplicaciones digitales o cualquier medio de comunicación verbal, física, digital o electrónica, induzca o dirija mediante amenazas, consejos, órdenes concretas, desafíos o cualquier forma de presión, a una persona a provocarse daño a sí misma o poner fin a su vida, siempre que resulte demostrable que dicha influencia fue determinante en el resultado dañoso.

Cuando se utilizan medios tecnológicos programados, entrenados o automatizados como herramientas de manipulación psicológica o presión emocional, la pena se aumentará hasta en un tercio.

Art. 154.2.- Hostigamiento. - La persona natural o jurídica que, por sí misma o por terceros o a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra, será sancionada con una pena privativa de la libertad de

seis meses a un año, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual.

Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de uno a tres años.

En los casos que no se configure el delito de instigación al suicidio tipificado en el artículo 154.1, se sancionará las conductas tipificadas en este artículo, con el máximo de la pena establecida cuando producto de la afectación a la salud emocional de la víctima de este delito, se deriven o hayan derivado sobre sí misma conductas autolesivas, siempre que para la o el juzgador resulte demostrable que la afectación sufrida por la víctima fue determinante en el resultado dañoso autolesivo.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aún sin ella, se aplicará los presupuestos y la pena establecida en los artículos relativos a la violencia contra la mujer y miembros del núcleo familiar (Ecuador, 2014).

Parágrafo adicional:

Cuando el hostigamiento se haya cometido a través de sistemas de inteligencia artificial programados o entrenados con el fin de acosar, perseguir o intimidar a la víctima, se considera como un agravante específico. La responsabilidad penal recaerá sobre la persona natural o jurídica que haya desarrollado, activado, utilizado o beneficiado del funcionamiento de dicho sistema con multas delictivos.

Art. 186.- Estafa. - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.

4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.

5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

6. A través de una compañía de origen ficticio, induzca a error a otra persona, con el fin de realizar un acto que perjudique su patrimonio o el de un tercero.

La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.

La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años.

La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días.

Si se determina responsabilidad penal de una persona jurídica, será sancionada con multa de cien a doscientos salarios básicos unificados del trabajador en general (Ecuador, 2014).

Propuesta de reforma parcial:

Se considerará agravante el uso de sistemas automatizados, inteligencia artificial, algoritmos o cualquier tecnología digital avanzada para la comisión de estafa, en especial cuando dichos medios permitan ampliar el número de víctimas, la magnitud del perjuicio o dificulten la identificación del responsable.

La responsabilidad penal recaerá en la persona natural o jurídica que configure, programe, active o utilice dichos sistemas con conocimiento de la ilicitud del acto.

Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Ecuador, 2014).

Propuesta de reforma parcial:

Será sancionada con pena privativa de libertad de tres a cinco años la persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programas, sistemas informáticos, telemáticos, inteligencia artificial o algoritmos, o mensajes de datos, para

procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona, en perjuicio de esta o de un tercero.

De igual manera, se sancionará a quien facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 234.1.- Falsificación informática:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.

2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena (Ecuador, 2014).

Propuesta de reforma:

Art. 234.1.- Falsificación informática:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introduzca, modifique, elimine, suprima o interfiera de cualquier forma en el tratamiento informático de datos, o produzca datos, documentos, imágenes, audios o videos no genuinos mediante el uso de tecnologías automatizadas, inteligencia artificial o sistemas generativos, será sancionada con pena privativa de libertad de tres a cinco años.

2. Quien, actuando con intención de causar perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento, imagen, audio, video o cualquier contenido producido a partir de actos referidos en el número 1, será sancionado con la misma pena.

4.2. Discusión

El trabajo de Simon Chesterman (2021) resuena profundamente con los hallazgos de esta investigación, puesto que ambos destacan la insuficiencia de los marcos jurídicos actuales para abordar los delitos relacionados con la inteligencia artificial (IA). Chesterman señala que la expansión de la IA en diversos ámbitos de la sociedad ha generado vacíos normativos, lo que dificulta la tipificación y persecución de nuevas formas de delitos cometidos mediante sistemas autónomos. Esta misma problemática se evidencia en el contexto ecuatoriano, donde la legislación penal aún no cuenta con disposiciones específicas que regulen el uso indebido de la IA en fraudes, manipulación de información y cibercrimen. En este sentido, el estudio plantea la necesidad de adaptar el Código Orgánico Integral Penal (COIP) a estas nuevas realidades, tomando en cuenta modelos regulatorios internacionales. Tal como lo menciona Chesterman, la regulación de la IA se manifiesta como una restricción al desarrollo tecnológico, sino como un mecanismo para gestionar riesgos y garantizar la

seguridad jurídica. De esta manera, Ecuador tiene la oportunidad de diseñar un marco normativo integral que no solo sancione los delitos relacionados con la IA, sino que también establezca principios éticos y salvaguardias para la protección de los derechos fundamentales en la era digital.

Las reflexiones de Ugo(Pagallo, 2022) encuentran eco en los hallazgos de este estudio, considerando que ambos evidencian las limitaciones de los marcos jurídicos tradicionales para abordar los desafíos que plantea la inteligencia artificial (IA) en el ámbito penal. Pagallo subraya la necesidad de marcos regulatorios adaptados que tomen en cuenta las capacidades y limitaciones de los sistemas autónomos, especialmente en lo que respecta a la transparencia algorítmica y la atribución de responsabilidad en casos de daño. Esta preocupación es particularmente relevante en el contexto ecuatoriano, donde la falta de normativas específicas en el Código Orgánico Integral Penal (COIP) genera incertidumbre jurídica ante delitos cometidos con IA, como fraudes automatizados y manipulación de información. En este sentido, la propuesta de Pagallo sobre la autorregulación de la IA como estrategia complementaria cobra especial importancia, por lo tanto podría servir como un mecanismo de control mientras se desarrollan marcos normativos más robustos. Sin embargo, para garantizar la protección del interés público en un entorno tecnológico en constante evolución, se requiere un equilibrio entre la regulación estatal y la responsabilidad de los desarrolladores y operadores de IA. Así, Ecuador tiene el reto de diseñar una normativa que no solo tipifique los delitos vinculados a la IA, sino que también promueva estándares de transparencia y seguridad para prevenir abusos y garantizar un uso ético de esta tecnología.

El análisis de Rodríguez Mendoza y Maldonado Ruiz (2024) complementa los hallazgos de esta investigación al resaltar la relevancia de la inteligencia artificial en la investigación penal y la necesidad de contar con una regulación adecuada en el contexto ecuatoriano, mientras el presente estudio se enfoca en los delitos a partir del uso de la IA y su tipificación en la legislación penal ecuatoriana, los autores subrayan el potencial positivo de esta tecnología para fortalecer la administración de justicia. La experiencia internacional, especialmente en países como Argentina y Estados Unidos, demuestra que la IA puede contribuir significativamente a la identificación de infractores, la agilización de los procesos judiciales y la prevención del delito, evidenciando la necesidad de implementar estas herramientas en el Ecuador, sin embargo, ambos enfoques coinciden en que dicha integración debe desarrollarse dentro de un marco normativo sólido que garantiza la protección de los derechos fundamentales y la privacidad de los ciudadanos. De manera similar a este estudio, Rodríguez Mendoza y Maldonado Ruiz destacan la urgencia de regular los dispositivos inteligentes aplicados en las investigaciones penales, asimismo, los autores señalan que la creación de un marco ético robusto constituye un elemento esencial para asegurar la transparencia y legitimidad en el uso de la IA en el ámbito judicial, evitando riesgos de discriminación algorítmica y de uso indebido de datos sensibles. En este sentido, la regulación de la IA en Ecuador no solo es necesaria enfocar en la sanción de delitos cometidos con esta tecnología, sino también en su aprovechamiento responsable para fortalecer la justicia y la seguridad ciudadana.

CAPÍTULO V.

5. CONCLUSIONES y RECOMENDACIONES

5.1. Conclusiones

Los delitos relacionados con el uso de inteligencia artificial en Ecuador, revela que la legislación penal actual muestra dificultades para afrontar los desafíos emergentes, a causa de la falta de normas específicas para tipificar delitos como el fraude automatizado, la manipulación de datos y la generación de contenido falso deja vacíos legales que pueden ser explotados por actores malintencionados.

Se identificó que la IA puede ser utilizada en la comisión de diversos delitos, como la suplantación de identidad, la desinformación y la toma de decisiones sesgadas, estos crímenes generan complicaciones, tanto jurídicas como sociales, debido a la vulneración de los derechos, como la privacidad, la seguridad de la información y la reputación de las personas.

La normativa penal ecuatoriana no cuenta con disposiciones claras que regulan el uso de IA, la falta de marcos regulatorios específicos impide un adecuado seguimiento y sanción de estas conductas, lo que permite destacar la urgencia de reformar la legislación penal ecuatoriana, para prevenir y disminuir los riesgos relacionados a estas nuevas formas de criminalidad.

El análisis comparativo de legislaciones de los diferentes países demuestra como, Estados Unidos y la Unión Europea están a un paso adelante en la creación de regulaciones, para mitigar los efectos negativos de la IA en el ámbito penal, gracias a ello Ecuador puede beneficiarse de la experiencia internacional, para poder desarrollar normativas que se alinean con estándares globales y responden a los desafíos particulares del contexto nacional.

5.2. Recomendaciones

Por medio de sus instituciones legislativas Ecuador, impulse una reforma integral del Código Orgánico Integral Penal, que incorpore disposiciones específicas sobre los delitos relacionados con el uso de la inteligencia artificial, esta reforma debe contemplar figuras como el fraude automatizado, la manipulación de datos, la suplantación digital y la generación de contenido falso, a fin de cerrar los vacíos legales existentes y garantizar una respuesta jurídica eficaz frente a las nuevas modalidades de criminalidad tecnológica.

Resulta importante que la Asamblea Nacional y las entidades competentes, promuevan espacios de diálogo y cooperación interdisciplinaria, donde se reúnan especialistas en Derecho, tecnología, ética y seguridad digital, estos espacios permitirían construir una legislación equilibrada que se ajuste a la innovación tecnológica, tomando en cuenta la protección de los derechos, garantizando así la privacidad, la seguridad de la información y la reputación de las personas en el entorno digital.

Ecuador debe tomar como referencia las experiencias normativas internacionales, especialmente aquellas de los países como Estados Unidos y los miembros de la Unión Europea, los cuales han avanzado en la creación de marcos regulatorios, que abordan los riesgos asociados al uso de la inteligencia artificial, para lograr adaptar estas buenas prácticas al contexto nacional ayudando a fortalecer el sistema penal ecuatoriano, adaptándose con los estándares globales y promoviendo un enfoque preventivo ante los delitos tecnológicos emergentes.

Las instituciones académicas y judiciales fomenten la formación continua en materia de inteligencia artificial y derecho tecnológico, capacitar a jueces, fiscales, abogados y futuros profesionales del Derecho permitirá desarrollar una comprensión integral de las implicaciones jurídicas, éticas y sociales de la IA, de esta manera, se promoverá una justicia más preparada para enfrentar los desafíos del entorno digital y se impulsarán investigaciones que contribuyan al diseño de políticas públicas y normativas adaptadas a la realidad tecnológica del país.

BIBLIOGRÁFIA

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing perspective. *PeerJ Computer Science*, *2*, e93. https://doi.org/10.7717/peerj-cs.93

Andrade Arias, W. M., & Yurank Tsamaraint, L. A. (2025). *La eficacia de una normativa especial que regule el uso de la inteligencia artificial para evitar ciber-delitos en el Ecuador*. https://dspace.ucacue.edu.ec/handle/ucacue/19816

Arevalo Fernandez, N. L. (2024). *LA OMISIÓN DEL DELITO DE DEEPFAKE EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL EN ECUADOR.*

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? 🦜. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 610-623. https://doi.org/10.1145/3442188.3445922

Berghoff, C., Neu, M., & Von Twickel, A. (2020). Vulnerabilities of Connectionist AI Applications: Evaluation and Defense. *Frontiers in Big Data*, *3*, 23. https://doi.org/10.3389/fdata.2020.00023

Brynjolfsson, E., & McAfee, A. (2016). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies* (First published as a Norton paperback). W. W. Norton & Company.

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273-291. https://doi.org/10.1007/s10506-017-9214-9

Bu, Q. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, *2*(1), 113-145. https://doi.org/10.1365/s43439-021-00022-x

Calo, R. (2017). Robots in American Law. En E. Hilgendorf & U. Seidel (Eds.), *Robotics, Autonomics, and the Law* (pp. 59-108). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845284651-59

Campione, T.-R., Presno Linera, M. Á., & Meuwese, A. (2024). *Normativa europea de inteligencia artificial: Reglamento de la Unión Europea y convenio marco del Consejo de Europa*. Servicio de Publicaciones de la Universidad de Oviedo. https://digibuo.uniovi.es/dspace/handle/10651/77111

Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*, *100*, 107734. https://doi.org/10.1016/j.compeleceng.2022.107734

Chavez Tapia,Keli Emperatriz, & Chirre Quiquia, K. M. (2024). *Implicancias legales del uso de la Inteligencia Artificial en el delito de suplantación de identidad en Lima, 2023*.

Chesney, Bobby; Citron, Danielle. (2019). *Deep Fakes: A Looming Challenge for Privacy*. https://doi.org/10.15779/Z38RV0D15J

Chesterman, S. (2021). *We, the Robots?: Regulating Artificial Intelligence and the Limits of the Law* (1.ª ed.). Cambridge University Press. https://doi.org/10.1017/9781009047081

Chivilches Seguil, F. E. (2023). *Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú*.

Comisión Económica para América Latina y el Caribe (CEPAL). (2025). Superar las trampas del desarrollo de América Latina y el Caribe en la era digital: El potencial transformador de las tecnologías digitales y la inteligencia artificial. *América Latina*.

Cóndor Rosas, J. P. (2024). *Seguridad Cibernética: Estudio Comparativo del sistema jurídico de la República del Ecuador, Colombia, Chile y Argentina*.

Consejo de Europa. (2023). *Council of Europe and Artificial Intelligence—Artificial Intelligence—Www.coe.int*. Artificial Intelligence. https://www.coe.int/en/web/artificial-intelligence

Corvalán, J. G. (2018). Inteligencia artificial: Retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. *Revista de Investigações Constitucionais*, *5*(1), 295. https://doi.org/10.5380/rinc.v5i1.55334

Crawford, K., & Paglen, T. (2021). Correction to: Excavating AI: the politics of images in machine learning training sets. *AI & SOCIETY*, *36*(4), 1399-1399. https://doi.org/10.1007/s00146-021-01301-1

Dan, V. (2025). Deepfakes as a Democratic Threat: Experimental Evidence Shows Noxious Effects That Are Reducible Through Journalistic Fact Checks. *The International Journal of Press/Politics*, 19401612251317766. https://doi.org/10.1177/19401612251317766

Dhar, V., & Domingos, P. (2016). Pedro Domingos on *The Master Algorithm*: A Conversation with Vasant Dhar. *Big Data*, *4*(1), 10-13. https://doi.org/10.1089/big.2016.29003.pdo

Ecuador. (2014). *Código Orgánico Integral Penal*.

Espinosa, K. P. G., Mendoza, M. J. B., Jaramillo, E. S. S., Lecaro, G. R. G., & Urréa, H. E. R. (2024). Desafíos del derecho frente a los delitos de estafa coadyuvados por la inteligencia artificial (IA). *Sinergia Académica*, *7*(4), Article 4. https://doi.org/10.51736/3w6j7034

Fuentes-Aguila, M., & Muñoz-Alfonso, Y. (2025). Violencia digital contra la mujer e inteligencia artificial. Entornos legales cubano y ecuatoriano. *Revista Metropolitana de Ciencias Aplicadas*, *8*(1), 54-65. https://doi.org/10.62452/6gg85d59

Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. *IEEE Internet Computing*, *21*(6), 58-62. https://doi.org/10.1109/MIC.2017.4180835

Gobierno de España. (2021). *Carta de Derechos Digitales*.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. The MIT Press.

Guamán Terán, C. E. (2023). *Estudio jurídico del artículo 190 del código orgánico integral penal sobre la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura*. https://repositorio.puce.edu.ec/handle/123456789/39901

Guszcza, J., Lee, M. A., Ammanath, B., & Kuder, D. (2020). *Human values in the loop: Design principles for ethical AI*.

Gutiérrez, J. (2022). La responsabilidad jurídica de la inteligencia artificial desde el derecho clásico: The legal responsibility of artificial intelligence from classical law. *AXIOMA*, *1*(27), 19-25. https://doi.org/10.26621/ra.v1i27.808

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1), 6. https://doi.org/10.1186/s40537-024-01048-8

Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *WIREs Data Mining and Knowledge Discovery*, *9*(4), e1306. https://doi.org/10.1002/widm.1306

Hernández Giménez, M. (2019). Inteligencia artificial y derecho penal. *Actualidad jurídica iberoamericana, Extra 10*, 792-843.

Hildebrandt, M. (2016). *Smart technologies and the end(s) of law: Novel entanglements of law and technology* (Paperback edition). Edward Elgar Publishing.

Huang, M.-H., & Rust, R. T. (2021). Engaged to a Robot? The Role of AI in Service. *Journal of Service Research*, *24*(1), 30-41. https://doi.org/10.1177/1094670520902266

Hueso, L. C. (2019). *RIESGOS E IMPACTOS DEL BIG DATA, LA INTELIGENCIA ARTIFICIAL Y LA ROBÓTICA. ENFOQUES, MODELOS Y PRINCIPIOS DE LA RESPUESTA DEL DERECHO*.

John, A., Han, I., & Jay, G. (2025). *AI-Powered Fraud Detection and Prevention in Fintech: Evaluating the Effectiveness of Advanced Algorithms*.

Jurafsky, D., & Martin, J. H. (2009). *Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition* (2nd ed). Pearson Prentice Hall.

Kirpichnikov, D., Pavlyuk, A., Grebneva, Y., & Okagbue, H. (2020). Criminal Liability of the Artificial Intelligence. *E3S Web of Conferences*, *159*, 04025. https://doi.org/10.1051/e3sconf/202015904025

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, *359*(6380), 1094-1096. https://doi.org/10.1126/science.aao2998

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436-444. https://doi.org/10.1038/nature14539

León, J. A. V. (2024). Desafíos y adaptaciones legales ante la inteligencia artificial: Privacidad y protección de datos en el marco del Código Orgánico Integral Penal. *Sinergia Académica*, *7*(Especial 6), Article Especial 6. https://doi.org/10.51736/97qs2h79

López, N. P., & Vieira, I. M. (2023). *El uso de la inteligencia artificial en derecho penal: Un estudio y prevención de la violencia de género en Ecuador y Brasil*. 57-69.

Maldonado Montenegro, C. D. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: Desafíos y perspectivas. *Revista Criminalidad*, *66*(3), 27-44. https://doi.org/10.47741/17943108.660

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(4), 754-772. https://doi.org/10.1016/j.clsr.2018.05.017

Marina, O. M. K. (2024). *ARTÍCULO CIENTÍFICO PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA*.

Mariscal, L. T. B., Rodríguez, E. G. Á., Castro, E. J. G., Romero, D. D. O., & Perero, J. L. M. (2024). La inteligencia artificial en el derecho: Desafíos del debido proceso y la equidad en la toma de decisiones algorítmicas. *Sinergia Académica*, *7*(Especial 7), Article Especial 7. https://doi.org/10.51736/txcdm234

Martínez Pazos, J. F., Gulín González, J., Batard Lorenzo, D., RobaiNa Morales, J. A., & Rodrígez Álvarez, M. M. (2024). Fraud Transaction Detection For Anti-Money Laundering Systems Based On Deep Learning. *Journal of Emerging Computer Technologies*, *3*(1), 29-34. https://doi.org/10.57020/ject.1428146

Martínez Sandoval, C. A., Sánchez Silva, S. A., & Trujillo Monterrosa, N. (2019). How to Carry Out Usability Studies with Visually Impaired Children. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-6. https://doi.org/10.1145/3290607.3299037

Mecias, C. J. B., Cabello, Y. K. J., Mueses, L. M. S., & Paredes, A. G. R. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica*, *7*(Especial 5), Article Especial 5. https://doi.org/10.51736/sjq7b043

Mercader Uguina, J. R. (with Peña, D.). (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*. Tirant lo Blanch.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*. https://doi.org/10.1007/s10115-025-02429-y

Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation. *Minds and Machines*, *32*(2), 241-268. https://doi.org/10.1007/s11023-021-09577-4

Montañez Sierra, C. F. (2020). *Decisiones judiciales asistidas: Paradigmas del juez y jueza en cuanto al uso de inteligencia artificial* [masterThesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador]. http://repositorio.uasb.edu.ec/handle/10644/7783

Morán Espinosa, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *REVISTA IUS, 15*(48). https://doi.org/10.35487/rius.v15i48.2021.706

Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences*, *14*(22), 10487. https://doi.org/10.3390/app142210487

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy* (First edition). Crown.

Ordóñez Córdova, L. A. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. *Reincisol.*, *3*(5), 1447-1469. https://doi.org/10.59282/reincisol.V3(5)1447-1469

Organización para la Cooperación y el Desarrollo Económicos. (s. f.). *Principios de la OCDE sobre la Inteligencia Artificial*. Recuperado 4 de julio de 2025, de https://www.oecd.org/en/topics/artificial-intelligence.html

Ormazabal Sánchez, G. (2024). La prueba en los procesos de responsabilidad civil por daños causados por sistemas de inteligencia artificial. *InDret*, *3*, 395-445. https://doi.org/10.31009/InDret.2024.i3.12

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems*, *159*, 161-171. https://doi.org/10.1016/j.future.2024.05.027

Pagallo, U. (2013). *The Laws of Robots: Crimes, Contracts, and Torts* (Vol. 10). Springer Netherlands. https://doi.org/10.1007/978-94-007-6564-1

Pagallo, U. (2022). *The Laws of Robots: Crimes, Contracts, and Torts* (Vol. 10). Springer Netherlands. https://doi.org/10.1007/978-94-007-6564-1

Pozo-Caicedo, L., & Rodríguez-Ruiz, M. (2025). Regulación y procesamiento de los ciberdelitos o delitos informáticos en la legislación ecuatoriana. *593 Digital Publisher CEIT*, *10*(1-1), 193-204. https://doi.org/10.33386/593dp.2025.1-1.3025

Programa de las Naciones Unidas (PNUD). (2025, junio 4). *Ecuador frente al desarrollo humano en la era de la inteligencia artificial: Un llamado a decidir con enfoque humano*. UNDP. https://www.undp.org/es/ecuador/noticias/ecuador-frente-al-desarrollo-humano-en-la-era-de-la-inteligencia-artificial-un-llamado-decidir-con-enfoque-humano

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (2021). https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52021PC0206

Redroban Ortiz, C. L., & Cedeño Tapia, S. J. (2022). COMPLIANCE EN ECUADOR, DESAFÍO TRIPARTITO ENTRE GOBIERNO, EMPRESA Y ACADEMIA: EL DIAGNÓSTICO. *REVISTA CIENTIFICA EPISTEMIA*, *6*(2), 17-34. https://doi.org/10.26495/re.v6i2.2293

Richardson, R., Schultz, J. M., & Crawford, K. (2019). *DIRTY DATA, BAD PREDICTIONS: HOW CIVIL RIGHTS VIOLATIONS IMPACT POLICE DATA, PREDICTIVE POLICING SYSTEMS, AND JUSTICE*.

Rodríguez Barroso, C., & Martínez Cisneros, L. (2024). La influencia de la inteligencia artificial en la administración de justicia: Una transformación en el sistema judicial. *Catilinaria IURIS*, *2*(2). https://doi.org/10.33210/rci.v2i2.36

Rodríguez Mendoza, S. D., & Maldonado Ruiz, L. M. (2024). Reflexión sobre el uso de la inteligencia artificial en la investigación penal en el Ecuador-análisis de su aplicabilidad en el derecho comparado. *Polo del Conocimiento*, *9*(1), 17. https://doi.org/10.23857/pc.v9i1

Romero Jarrín, F. A., & Vásquez, A. S. (2025). Compliance y gestión de riesgos judiciales en el Ecuador. *Killkana Social*, *9*(2), 87-109. https://doi.org/10.26871/killkanasocial.v9i2.1610

Rosero, L. M. R., & Oñate, P. L. G. (2025). *La inteligencia artificial, una nueva modalidad para la comisión del delito de*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR.

Sandoval, M.-P., De Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, *13*(1), 41. https://doi.org/10.1186/s40163-024-00239-1

Segovia Segovia, A. C., & Flores Quishpi, B. E. (2025). La inteligencia artificial, los derechos humanos y el sistema penal ecuatoriano: Un análisis de sus ventajas y desventajas. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(6), 8048-8059. https://doi.org/10.37811/cl_rcm.v8i6.15510

Sinaluisa Sagñay, F. G. (2024). *Deepfakes, dificultades probatorias y su incidencia en la vulneración al derecho de intimidad* [bachelorThesis, Universidad Nacional de Chimborazo, Riobamba, Ecuador]. http://dspace.unach.edu.ec/handle/51000/13841

Susskind, R. (2019). *Online Courts and the Future of Justice*. Oxford University Press. https://doi.org/10.1093/oso/9780198838364.001.0001

Tang, T., Yao, J., Wang, Y., Sha, Q., Feng, H., & Xu, Z. (2025). *Application of Deep Generative Models for Anomaly Detection in Complex Financial Transactions* (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2504.15491

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale university press.

UNESCO. (2022). *Recomendación sobre la ética de la inteligencia artificial*. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Valls Prieto, J. (2023). La inteligencia artificial frente a la colectividad. Una protección de los bienes jurídicos colectivos frente al auge de los sistemas inteligentes. *Estudios Penales y Criminológicos*, 1-26. https://doi.org/10.15304/epc.44.8880

Víctor Elian León Párraga. (2024). *Responsabilidad penal de la IA: ausencia de producción normativa en Ecuador*. UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ.

Viveros Álvarez, J. S. (2022). La inteligencia artificial y la responsabilidad internacional de los estados. *Estudios en Derecho a la Información*, 83-105. https://doi.org/10.22201/iij.25940082e.2022.14.16894

Vladimír Smejkal & Jindřich Kodl. (2023). Challenges and Solutions to Criminal Liability for the Actions of Robots and AI. *Advances in Technology Innovation*, *9*(1), 65-84. https://doi.org/10.46604/aiti.2023.12038

Yazici, T. (2025). Toward a global standard for ethical AI regulation: Addressing gaps in AI-driven biometric and high-resolution satellite imaging in the EU AI Act. *Law, Innovation and Technology*, *17*(1), 366-394. https://doi.org/10.1080/17579961.2025.2470589

Zabala Leal, T. D., & Zuluaga Ortiz, P. A. (2021). Los retos jurídicos de la inteligencia artificial en el derecho en Colombia. *JURÍDICAS CUC*, *17*(1). https://doi.org/10.17981/juridcuc.17.1.2021.17

ZAMBRANO LOAIZA, A. C., & SUAREZ CASTRO, J. C. (2020). *La seguridad de las aplicaciones bancarias y dispositivos sin contacto que permiten efectuar pagos en Colombia.*

Zhang, C. J., Gill, A. Q., Liu, B., & Anwar, M. J. (2025). *AI-based Identity Fraud Detection: A Systematic Review* (No. arXiv:2501.09239). arXiv. https://doi.org/10.48550/arXiv.2501.09239

ANEXOS

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLITICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

GUÍA DE ENTREVISTA

Tema de la investigación: Los delitos a partir del uso de IA y su tipificación en la legislación penal ecuatoriana.

Objetivo: Identificar los vacíos y limitaciones en la legislación penal ecuatoriana actual respecto a la regulación de actividades delictivas que involucren IA, con el fin de identificar áreas específicas que requieren actualización normativa.

Consentimiento Informado:

Estimado/ a

Le invitamos a participar en una entrevista cuyo objetivo Identificar los vacíos y limitaciones en la legislación penal ecuatoriana actual respecto a la regulación de actividades delictivas que involucren IA, con el fin de identificar áreas específicas que requieren actualización normativa, su participación es fundamental para nuestra investigación y es completamente voluntaria y confidencial, así como los datos recogidos se utilizaran exclusivamente con los fines de investigación y no se divulgaran a terceros.

Voluntariedad: Su participación en esta entrevista es completamente voluntaria.

Confidencialidad: Toda la información proporcionada será tratada con la máxima confidencialidad y se utilizará únicamente con fines académicos y de desarrollo de políticas.

Anonimato: Sus respuestas serán anonimizadas y no se le identificará personalmente en ningún informe resultante de este estudio.

Retiro: Puede retirarse de la entrevista en cualquier momento sin necesidad de dar explicaciones.

Al continuar con esta entrevista, usted acepta participar en ella bajo las condiciones mencionadas.

Sección 1: Introducción

1. ¿Conoce usted que es la inteligencia artificial?

2. ¿Podría hablarme sobre su experiencia en el derecho penal con los avances tecnológicos, específicamente utilizando inteligencia artificial?
3. ¿Ha conocido usted de casos en los que la IA haya jugado un rol en actividades delictivas?

Sección 2: Marco Normativo Actual

4. Desde su perspectiva, ¿cómo evalúa la legislación penal ecuatoriana respecto a la capacidad para abordar delitos relacionados con la IA?
5. ¿Considera que las disposiciones legales actuales son suficientes para sancionar adecuadamente estos delitos? ¿Por qué?

Sección 3: Vacíos Legales

6. ¿Qué áreas o aspectos considera que no están regulados en relación con el uso de IA en actividades delictivas?
7. ¿Qué impacto cree que tienen estos delitos en el ámbito penal, en términos de daño a las víctimas y complejidad procesal?

Sección 4: Propuestas y Recomendaciones

8. ¿Qué reformas legales sugeriría para incluir delitos relacionados con IA en el COIP?
9. ¿Qué retos considera que podrían surgir al implementar estas reformas en el marco legislativo actual?
10. ¿Qué rol deben tener los fiscales, jueces y abogados en la identificación y resolución de estos vacíos legales?