



UNIVERSIDAD  
CATÓLICA  
DE CUENCA

**UNIVERSIDAD CATÓLICA DE CUENCA**

*Comunidad Educativa al Servicio del Pueblo*

**FACULTAD DE CIENCIAS SOCIALES**

**CARRERA DE DERECHO**

**Análisis jurídico de la responsabilidad penal por infracciones de propiedad**

**intelectual mediante inteligencia artificial en Ecuador**

**PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL**

**TÍTULO DE ABOGADA**

**AUTORA: JESSICA ALEXANDRA RIVERA PULLA**

**DIRECTOR: ABG. JUAN PABLO MARTINEZ ALBORNOZ MGS.**

**CUENCA-ECUADOR**

**2026**

**DIOS, PATRIA, CULTURA Y DESARROLLO**



**UNIVERSIDAD CATÓLICA DE CUENCA**

*Comunidad Educativa al Servicio del Pueblo*

**FACULTAD DE CIENCIAS SOCIALES**

**CARRERA DE DERECHO**

Análisis jurídico de la responsabilidad penal por infracciones de propiedad  
intelectual mediante inteligencia artificial en Ecuador

**PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE ABOGADA**

**AUTORA: JESSICA ALEXANDRA RIVERA PULLA**

**DIRECTOR: ABG. JUAN PABLO MARTINEZ ALBORNOZ, MGS.**

**CUENCA - ECUADOR**

**2026**

**DIOS, PATRIA, CULTURA Y DESARROLLO**

**Declaratoria de Autoría y Responsabilidad.**

**Jessica Alexandra Rivera Pulla** portadora de la cédula de ciudadanía N° **0106574445**. Declaro ser la autora de la obra: “**Análisis jurídico de la responsabilidad penal por infracciones de propiedad intelectual mediante inteligencia artificial en Ecuador**”, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **17 de abril de 2026**.

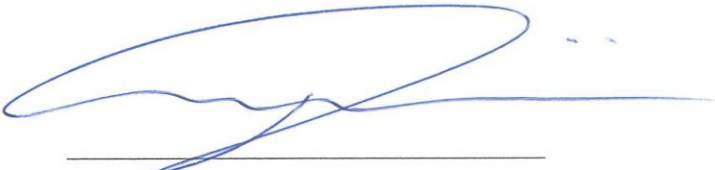
F: ..... 

**Jessica Alexandra Rivera Pulla**

**C.I.: 0106574445**

### CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por: **Jessica Alexandra Rivera Pulla**, con el Tema: “**Análisis jurídico de la responsabilidad penal por infracciones de propiedad intelectual mediante inteligencia artificial en Ecuador**”, bajo mi supervisión.



---

**DR. JUAN PABLO MARTÍNEZ ALBORNOZ, MGS**

Tutor

---

## Dedicatoria

A Dios, por ser mi guía y fortaleza en cada paso de este camino; por brindarme la sabiduría necesaria para superar los obstáculos y la vida para ver culminado este sueño. Gracias por ser la luz en mis momentos de duda, por renovar mis fuerzas cuando el camino se tornaba difícil y por permitirme entender que, bajo su amparo, ningún esfuerzo es en vano. Todo lo que soy y lo que he logrado es testimonio de su infinita bondad.

A mis padres, Hernán y Rosa, mis motores de vida y mis guías eternos. Gracias por enseñarme que la perseverancia es la clave del éxito y por ser el ejemplo vivo de esfuerzo y honestidad. Cada página de esta tesis lleva impreso su sacrificio y cada palabra es un eco de su amor. Este título es tan suyo como mío, porque mis logros son la cosecha de las semillas que ustedes plantaron con tanta fe. Este triunfo les pertenece por haberme dado las alas para volar.

A mi tía Blanca, cuya presencia ha sido luz en los momentos más significativos de mi vida. Más que una tía, ha sido una guía y un apoyo incondicional que nunca me dejó desistir. Gracias por sus abrazos que reconfortan y por sus palabras que sanan; este logro también lleva su esencia y mi gratitud eterna.

A Steven Samaniego, mi enamorado, por ser mi compañero de batallas y mi refugio en la tormenta. Gracias por su paciencia infinita en mis días de mayor presión y por motivarme a ser una mejor profesional cada día. Sin importar los rumbos que tome la vida o lo que el futuro nos depare, quiero que sepa que siempre llevaré conmigo la gratitud de haber compartido este camino con usted. Gracias por creer en mí cuando ni yo misma lo hacía; su apoyo es parte esencial de este título.

## Resumen

La presente investigación analiza la responsabilidad penal derivada de las infracciones a la propiedad intelectual cometidas mediante el uso de inteligencia artificial en el Ecuador. El problema surge debido a que el Código Orgánico Integral Penal y el Código Ingenios fueron diseñados bajo esquemas tradicionales de creación humana, sin contemplar las nuevas formas de vulneración de derechos de autor mediante sistemas automatizados, lo que genera vacíos jurídicos y dificultades para atribuir responsabilidad penal.

El objetivo general consiste en analizar cómo la normativa ecuatoriana responde frente a las infracciones a la propiedad intelectual cometidas mediante inteligencia artificial, identificando sus limitaciones y la necesidad de reformas legales. La investigación se desarrolló bajo un enfoque cualitativo, mediante el análisis doctrinario, normativo y comparado del marco jurídico ecuatoriano y de legislaciones internacionales.

Los resultados evidencian que la legislación ecuatoriana no regula de manera específica las infracciones cometidas mediante inteligencia artificial, lo que genera inseguridad jurídica y dificultades en la imputación penal. Asimismo, se determinó que la responsabilidad debe recaer en los sujetos humanos que intervienen en el diseño, programación o uso de estas tecnologías.

Se concluye que es necesaria una reforma normativa que incorpore criterios claros de responsabilidad penal y nuevas figuras jurídicas que permitan proteger eficazmente los derechos de propiedad intelectual frente al uso indebido de la inteligencia artificial.

**Palabras clave:** *Responsabilidad penal; propiedad intelectual; inteligencia artificial; derechos de autor; derecho penal digital; infracciones tecnológicas.*

## Abstract

This research analyzes the criminal liability arising from intellectual property infringements committed through the use of artificial intelligence in Ecuador. The problem arises because the Organic Integral Criminal Code (COIP, by its Spanish acronym) and the “INGENIOS” code were designed under traditional models of human creation, without accounting for new forms of copyright infringement through automated systems, which creates legal gaps and difficulties in attributing criminal liability.

The general objective is to analyze how Ecuadorian legislation respond to intellectual property infringements committed through artificial intelligence, identifying their limitations and the need for legal reforms. The research was developed under a qualitative approach, through a doctrinal, regulatory, and comparative analysis of the Ecuadorian legal framework and international legislation.

The results show that Ecuadorian legislation does not specifically regulate infringements committed through artificial intelligence, which generates legal uncertainty and difficulties in assigning criminal liability. Furthermore, it was determined that liability should rest with the human agents involved in the design, programming, or use of these technologies.

It is concluded that a legal reform is necessary to incorporate clear criteria for criminal liability and new legal figures that allow for the effective protection of intellectual property rights against the misuse of artificial intelligence.

**Keywords:** *criminal liability, intellectual property, artificial intelligence, copyright, digital criminal law.*

## Índice

Declaratorio de autoría y responsabilidad.....	II
Certificado del tutor .....	III
Agradecimientos .....	III
Dedicatoria.....	IV
Resumen.....	V
Palabras clave.....	V
Abstract.....	VI
Keywords .....	VI
Índice.....	VII
Introducción .....	1
Capítulo I .....	4
<b>MARCO NORMATIVO ECUATORIANO DE LA PROPIEDAD INTELECTUAL Y SU RELACIÓN CON EL DERECHO PENAL .....</b>	<b>4</b>
1.1 Regulación de la propiedad intelectual en Ecuador .....	4
1.2 Código Ingenios: alcance y limitaciones .....	6
1.3 COIP y delitos contra la propiedad intelectual .....	8
1.4 Relación entre derecho penal y propiedad intelectual .....	11
1.5 Análisis doctrinario .....	13
Capítulo II Vacíos jurídicos en la regulación de infracciones mediante inteligencia artificial.....	15
2.1 Nuevas formas de infracción mediante inteligencia artificial.....	16
2.2 Problemas de tipicidad penal .....	18
2.3 Imputación de responsabilidad penal.....	20
2.4 Análisis de la conducta, tipicidad, antijuridicidad y culpabilidad .....	22
2.5 Insuficiencia normativa del COIP y del Código Ingenios en la regulación de infracciones cometidas mediante inteligencia artificial.....	25
Capítulo III.....	28
<b>DERECHO COMPARADO Y PROPUESTAS DE REGULACIÓN EN EL ECUADOR .....</b>	<b>28</b>
3.1 Regulación en la Unión Europea .....	31
3.2 Regulación en Estados Unidos.....	33
3.3 Modelos de imputación penal en inteligencia artificial .....	36

3.4 Cuadro comparativo sobre normativas de tipificación de delitos derivados del uso de inteligencia artificial.....	40
3.4 Propuestas normativas para el Ecuador .....	43
3.4.1. Referentes internacionales para las reformas propuestas.....	46
3.5 Reformas legales necesarias .....	47
CONCLUSIONES Y RECOMENDACIONES .....	50
Anexos .....	57

## Introducción

El desarrollo tecnológico ha transformado significativamente la manera en que se crean, reproducen y difunden las obras intelectuales. En particular, la inteligencia artificial ha permitido automatizar procesos creativos que tradicionalmente dependían exclusivamente de la intervención humana. Actualmente, los sistemas de inteligencia artificial pueden generar textos, imágenes, música, software y otros contenidos digitales, lo que ha generado nuevos desafíos para el derecho penal y la propiedad intelectual. Estas innovaciones tecnológicas han modificado la forma en que se producen y utilizan las obras intelectuales, generando la necesidad de actualizar los marcos jurídicos tradicionales.

La relación entre inteligencia artificial y propiedad intelectual plantea importantes interrogantes jurídicas. Los sistemas automatizados pueden reproducir obras protegidas, generar contenidos derivados, modificar creaciones existentes o incluso suplantar la autoría mediante herramientas tecnológicas avanzadas. Estas conductas pueden vulnerar derechos morales y patrimoniales de los autores, lo que obliga a analizar si las normas vigentes permiten atribuir responsabilidad penal cuando las infracciones se cometen mediante inteligencia artificial. En este contexto, la propiedad intelectual deja de estar vinculada únicamente a la creación humana directa y pasa a involucrar procesos tecnológicos complejos que requieren regulación específica.

En el Ecuador, la propiedad intelectual se encuentra regulada principalmente por el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación y por el Código Orgánico Integral Penal. Sin embargo, estas normativas fueron diseñadas bajo modelos tradicionales de creación intelectual y no contemplan de manera expresa las infracciones cometidas mediante inteligencia artificial. Esta situación genera incertidumbre jurídica respecto a la imputación de responsabilidad penal y evidencia la necesidad de analizar la capacidad del ordenamiento jurídico ecuatoriano para responder a estos nuevos escenarios tecnológicos.

En este sentido, se identifican vacíos normativos en la legislación ecuatoriana, debido a que el Código Orgánico Integral Penal no tipifica conductas relacionadas con el uso indebido de inteligencia artificial en materia de propiedad intelectual. Asimismo,

el Código Ingenios no establece mecanismos claros para la protección de obras generadas o reproducidas mediante sistemas automatizados. Esta falta de regulación dificulta la atribución de responsabilidad penal y puede generar escenarios de impunidad frente a infracciones tecnológicas que afectan a los titulares de derechos.

La presente investigación se justifica desde el ámbito jurídico, social y académico. Desde el punto de vista jurídico, resulta necesario analizar la capacidad del derecho penal ecuatoriano para responder frente a nuevas formas de infracción a la propiedad intelectual. Desde la perspectiva social, la falta de regulación específica puede afectar a autores y creadores cuyos derechos son vulnerados mediante herramientas tecnológicas. En el ámbito académico, el estudio contribuye al análisis doctrinario sobre la responsabilidad penal derivada del uso de inteligencia artificial y propone soluciones que fortalezcan la seguridad jurídica.

La pregunta de investigación que guía el presente trabajo es: ¿De qué manera el Código Orgánico Integral Penal y la normativa ecuatoriana de propiedad intelectual abordan las infracciones a los derechos de autor y a la propiedad intelectual cometidas mediante el uso de sistemas de inteligencia artificial?

El objetivo general consiste en analizar cómo el Código Orgánico Integral Penal y el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación responden frente a las infracciones a los derechos de autor y a la propiedad intelectual cometidas mediante el uso de sistemas de inteligencia artificial.

Los objetivos específicos son: examinar el marco normativo ecuatoriano en materia de propiedad intelectual y su relación con el derecho penal; identificar los vacíos legales y limitaciones del COIP y del Código Ingenios respecto a la regulación de conductas ilícitas vinculadas al uso de inteligencia artificial; comparar la legislación ecuatoriana con marcos jurídicos internacionales; y evaluar propuestas normativas que permitan fortalecer la protección de los derechos de autor en el entorno digital.

La investigación se desarrolla bajo un enfoque cualitativo, de carácter jurídico y descriptivo. Se emplea el análisis doctrinario, normativo y comparado del Código Orgánico Integral Penal, el Código Ingenios, la Constitución de la República del Ecuador y fuentes doctrinarias relacionadas con la responsabilidad penal y la

inteligencia artificial. Asimismo, se recurre al derecho comparado con la finalidad de identificar modelos regulatorios aplicables al contexto ecuatoriano.

El trabajo se estructura en tres capítulos. El capítulo I analiza el marco normativo ecuatoriano de la propiedad intelectual y su relación con el derecho penal. El capítulo II examina los vacíos jurídicos en la regulación de infracciones mediante inteligencia artificial, abordando los problemas de tipicidad penal y responsabilidad jurídica. El capítulo III desarrolla el derecho comparado y presenta propuestas normativas para el Ecuador, orientadas a fortalecer la protección penal de la propiedad intelectual frente al uso indebido de la inteligencia artificial.

## Capítulo I

### MARCO NORMATIVO ECUATORIANO DE LA PROPIEDAD INTELLECTUAL Y SU RELACIÓN CON EL DERECHO PENAL

#### 1.1 Regulación de la propiedad intelectual en Ecuador

La propiedad intelectual constituye el conjunto de derechos que protegen las creaciones del intelecto humano, tales como obras literarias, artísticas, científicas, invenciones, marcas y demás manifestaciones del ingenio. Estos derechos permiten a los autores e inventores ejercer control sobre el uso y explotación de sus creaciones, garantizando el reconocimiento de su autoría y la obtención de beneficios económicos derivados de ellas. En este sentido, la propiedad intelectual cumple una función esencial en la promoción de la creatividad, la innovación y el desarrollo tecnológico dentro de la sociedad (Organización Mundial de la Propiedad Intelectual [OMPI], 2020).

Dentro de la propiedad intelectual se distinguen dos categorías predominantes: los derechos de autor y la propiedad industrial. Los derechos de autor protegen las obras literarias, artísticas y científicas, otorgando a los creadores facultades exclusivas sobre la reproducción, distribución, comunicación pública y transformación de sus obras. Este tipo de protección abarca novelas, poemas, obras teatrales, canciones, pinturas, esculturas y cualquier otra expresión artística, garantizando el control del autor sobre el uso de su creación (OMPI, 2020).

Por su parte, la propiedad industrial comprende la protección de invenciones, marcas, diseños industriales y otros signos distintivos utilizados en el ámbito comercial. Las patentes protegen invenciones originales y conceden al inventor el derecho exclusivo de explotación durante un período determinado, incentivando la innovación científica y tecnológica. Las marcas registradas, en cambio, salvaguardan signos distintivos como nombres, logotipos y lemas comerciales, permitiendo identificar productos o servicios y diferenciarlos de la competencia. Asimismo, los diseños industriales protegen el aspecto estético de los productos, incluyendo la forma, color, textura y ornamentación, garantizando la originalidad visual de los bienes en el mercado (Lipszyc, 2019).

La propiedad intelectual también incluye la protección del software y programas informáticos, reconociendo los derechos de los desarrolladores sobre sus aplicaciones digitales. Además, puede extenderse a conocimientos tradicionales, expresiones culturales y biodiversidad, con el propósito de preservar los saberes ancestrales de comunidades indígenas y locales. En el entorno digital, la propiedad intelectual se amplía a la protección de nombres de dominio y al uso adecuado de marcas en internet, evitando su utilización indebida en plataformas digitales (Bercovitz, 2017).

En el Ecuador, la propiedad intelectual se encuentra reconocida constitucionalmente como un derecho que protege la producción intelectual y promueve el desarrollo científico y tecnológico. El marco normativo principal está conformado por el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, conocido como Código Ingenios, el cual regula los derechos de autor, la propiedad industrial y otros mecanismos de protección de las creaciones intelectuales. Esta normativa establece disposiciones para el reconocimiento, registro, protección y defensa de los derechos derivados de la actividad creativa, así como las acciones legales que pueden ejercerse en caso de vulneración (Asamblea Nacional del Ecuador, 2016).

El Código Ingenios reconoce tres categorías principales dentro de la propiedad intelectual: los derechos de autor y derechos conexos, la propiedad industrial y las obtenciones vegetales. Los derechos de autor otorgan a los creadores derechos morales y patrimoniales sobre sus obras, mientras que la propiedad industrial protege invenciones, modelos de utilidad, diseños industriales, marcas y signos distintivos. Estas disposiciones buscan garantizar la protección jurídica de los titulares de derechos y fomentar la innovación científica y tecnológica en el país (Asamblea Nacional del Ecuador, 2016).

Asimismo, la administración de la propiedad intelectual en Ecuador se encuentra a cargo del Servicio Nacional de Derechos Intelectuales, entidad responsable de supervisar el registro y la concesión de derechos. Este organismo verifica la originalidad y distintividad de las creaciones, permitiendo establecer la titularidad y garantizar la protección legal frente a posibles infracciones. El registro de obras, marcas y patentes constituye un mecanismo fundamental para asegurar la defensa jurídica de

los derechos intelectuales (Servicio Nacional de Derechos Intelectuales [SENADI], 2022).

La propiedad intelectual cumple una función esencial en el desarrollo social y económico del Ecuador, ya que fomenta la creatividad, la innovación y la producción cultural. La protección jurídica de las creaciones humanas garantiza una retribución justa para los autores e inventores, al mismo tiempo que promueve la generación de nuevas ideas y el desarrollo tecnológico. No obstante, la regulación ecuatoriana fue concebida bajo un modelo tradicional de creación intelectual basado en la intervención humana directa, lo que presenta limitaciones frente a los avances tecnológicos actuales, particularmente en relación con la inteligencia artificial, la cual permite la generación automatizada de contenidos. En este contexto, surge la necesidad de analizar si la normativa vigente resulta suficiente para proteger los derechos de propiedad intelectual frente a nuevas formas de creación, reproducción y distribución de obras mediante sistemas tecnológicos (OMPI, 2020).

## **1.2 Código Ingenios: alcance y limitaciones**

El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, conocido como Código Ingenios, constituye la principal normativa que regula la propiedad intelectual en el Ecuador. Este cuerpo legal tiene como finalidad promover la generación del conocimiento, incentivar la innovación y garantizar la protección jurídica de las creaciones intelectuales. Asimismo, establece mecanismos para el reconocimiento de derechos, su registro y la defensa legal frente a posibles infracciones, consolidando un sistema integral de protección de la propiedad intelectual en el país (Asamblea Nacional del Ecuador, 2016).

El Código Ingenios regula diversas formas de propiedad intelectual, entre ellas los derechos de autor y derechos conexos, la propiedad industrial y las obtenciones vegetales. En relación con los derechos de autor, la normativa reconoce a los creadores facultades exclusivas sobre sus obras, otorgando protección tanto a los derechos morales como a los patrimoniales. Los derechos morales garantizan la paternidad de la obra, la integridad de la creación y el derecho del autor a decidir sobre su divulgación. Estos derechos tienen carácter irrenunciable, inalienable e imprescriptible, lo que significa que permanecen vinculados al autor incluso después de la explotación

económica de la obra. Por su parte, los derechos patrimoniales permiten al titular autorizar o prohibir la reproducción, distribución, comunicación pública y transformación de la obra, lo que posibilita el aprovechamiento económico de la creación intelectual (Asamblea Nacional del Ecuador, 2016; Lipszyc, 2019).

En cuanto a la propiedad industrial, el Código Ingenios regula la protección de invenciones, modelos de utilidad, diseños industriales, marcas y otros signos distintivos. Esta protección busca incentivar la innovación tecnológica y la actividad empresarial mediante el reconocimiento de derechos exclusivos sobre los resultados del esfuerzo creativo. En este sentido, las patentes otorgan a los inventores el derecho exclusivo de explotación por un tiempo determinado, mientras que las marcas permiten distinguir productos o servicios en el mercado, garantizando seguridad jurídica tanto para los productores como para los consumidores (Bercovitz, 2017).

Asimismo, el Código Ingenios establece disposiciones relacionadas con la administración de la propiedad intelectual, asignando al Servicio Nacional de Derechos Intelectuales la competencia para el registro, control y supervisión de estos derechos. Este organismo se encarga de verificar la originalidad y distintividad de las creaciones, así como de conceder títulos de propiedad intelectual y resolver conflictos administrativos relacionados con su protección. El registro constituye un mecanismo relevante para establecer la titularidad y facilitar la defensa jurídica frente a posibles infracciones (SENADI, 2022).

No obstante, a pesar de su importancia, el Código Ingenios presenta limitaciones frente a los avances tecnológicos actuales, particularmente en relación con la inteligencia artificial. La normativa fue diseñada bajo un modelo tradicional de creación intelectual basado en la intervención humana directa, lo que dificulta su aplicación a escenarios donde la obra es generada mediante sistemas automatizados. En este contexto, la legislación ecuatoriana no regula de manera expresa las obras creadas por inteligencia artificial ni establece criterios claros para determinar la titularidad de los derechos cuando intervienen algoritmos o sistemas autónomos en el proceso creativo (OMPI, 2020).

Otra limitación relevante se relaciona con la ausencia de disposiciones específicas para sancionar infracciones cometidas mediante inteligencia artificial.

Actualmente, el Código Ingenios no contempla mecanismos dirigidos a regular situaciones como la reproducción automatizada de obras protegidas, la generación de contenidos derivados mediante algoritmos, el entrenamiento de sistemas de inteligencia artificial con obras protegidas o la creación de contenidos que imitan estilos artísticos sin autorización del autor. Estas situaciones generan dificultades para determinar la existencia de infracciones y la responsabilidad jurídica correspondiente (Gervais, 2022).

Asimismo, la falta de regulación específica sobre inteligencia artificial puede generar conflictos en torno a la titularidad de derechos. En los casos donde una obra es generada por un sistema automatizado, surge la interrogante sobre quién debe ser considerado autor: el programador, el usuario, el propietario del sistema o el propio algoritmo. La doctrina jurídica ha señalado que los sistemas de inteligencia artificial no pueden ser considerados sujetos de derechos, debido a que carecen de personalidad jurídica y voluntad propia, por lo que la responsabilidad debe recaer en las personas que intervienen en el desarrollo o utilización de la tecnología (Pagallo, 2013).

Estas limitaciones evidencian la existencia de vacíos jurídicos dentro del Código Ingenios frente a la inteligencia artificial. La ausencia de disposiciones específicas dificulta la protección efectiva de los derechos de autor en el entorno digital y genera incertidumbre jurídica respecto a la atribución de responsabilidad. En consecuencia, se vuelve necesario analizar la relación entre la propiedad intelectual y el derecho penal como mecanismo de protección frente a las nuevas formas de infracción derivadas del uso de inteligencia artificial, especialmente cuando estas conductas afectan de manera significativa los derechos de los autores y titulares de creaciones intelectuales.

### **1.3 COIP y delitos contra la propiedad intelectual**

La protección penal de la propiedad intelectual responde a la necesidad de sancionar aquellas conductas que lesionan los derechos de autor, las marcas, las patentes y demás creaciones protegidas por la normativa jurídica. Esta obligación no solo surge del derecho interno, sino también de instrumentos internacionales como el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, el cual establece que los Estados deben implementar procedimientos y

sanciones penales para los casos de falsificación dolosa de marcas y piratería del derecho de autor a escala comercial, incluyendo penas privativas de libertad y sanciones económicas disuasorias (Organización Mundial del Comercio, 1995).

En el Ecuador, la tipificación penal de los actos lesivos contra la propiedad intelectual ha experimentado una evolución normativa. Con la entrada en vigencia del Código Orgánico Integral Penal en el año 2014, inicialmente no se incluyeron delitos específicos relacionados con la propiedad intelectual. Esta omisión generó un vacío jurídico debido al efecto derogatorio del COIP sobre normas penales anteriores, lo que provocó que temporalmente no existiera una protección penal expresa para estos derechos (Rivera, 2021). Posteriormente, mediante reformas legislativas, se incorporaron disposiciones destinadas a sancionar las conductas que afectan la propiedad intelectual, las cuales han sido modificadas progresivamente para fortalecer su alcance.

Actualmente, el Código Orgánico Integral Penal contempla los artículos 208 A y 208 B, denominados actos lesivos a la propiedad intelectual y actos lesivos a los derechos de autor. Estas disposiciones establecen distintos verbos rectores que describen conductas activas, por lo que no se admite la omisión como forma de comisión del delito. La denominación “lesivos” hace referencia a aquellas acciones que generan un perjuicio a los derechos morales y patrimoniales de los titulares, afectando no solo al autor o creador individual, sino también intereses colectivos vinculados con los consumidores y el mercado en general (Díaz & García Conlledo, 2009).

Estos delitos se encuentran ubicados dentro del capítulo correspondiente a los delitos contra la propiedad, lo que implica que el bien jurídico protegido es la propiedad. No obstante, la propiedad intelectual presenta características distintas a la propiedad tradicional regulada en el derecho civil. Mientras el Código Civil define la propiedad como el derecho real sobre una cosa corporal para gozar y disponer de ella conforme a la ley, la propiedad intelectual se refiere a creaciones intangibles derivadas del intelecto humano, lo que ha llevado a la doctrina a considerar que se trata de un bien jurídico autónomo o *sui generis* que requiere una protección diferenciada (Santos, 2017).

Desde la perspectiva doctrinaria, la intervención del derecho penal en materia de propiedad intelectual se justifica en la necesidad de proteger la convivencia social y los derechos reconocidos constitucionalmente. En este sentido, se sostiene que el derecho penal tiene la función de proteger bienes jurídicos fundamentales cuando otras ramas del derecho resultan insuficientes. Así, al existir un reconocimiento constitucional de la propiedad intelectual, la intervención penal se legitima como un mecanismo disuasivo frente a conductas que lesionan este derecho, sin que ello implique que sea el único medio de protección, pues también existen vías civiles y administrativas (Santos, 2017; Ferrajoli, 2012).

El artículo 208 A del Código Orgánico Integral Penal tipifica los actos lesivos a la propiedad intelectual relacionados principalmente con la propiedad industrial. Esta disposición sanciona con pena privativa de libertad de seis meses a un año, además de multa y comiso, a quien, con fines de lucro y a escala comercial, realice conductas como la fabricación, comercialización o almacenamiento de etiquetas, envases o sellos que contengan marcas registradas; la utilización de etiquetas originales en productos de distinto origen; el relleno de envases identificados con marca ajena; o la fabricación, comercialización o importación de productos protegidos por patentes, diseños industriales, obtenciones vegetales o signos distintivos registrados (Asamblea Nacional del Ecuador, 2014).

En cuanto a los elementos del tipo penal, el sujeto activo puede ser cualquier persona que intervenga en la cadena productiva, ya sea quien fabrique, distribuya, almacene, comercialice o importe los productos. El sujeto pasivo será el titular del derecho de propiedad intelectual vulnerado, aunque también se reconoce la afectación a intereses colectivos, especialmente a los consumidores que pueden adquirir productos falsificados o de calidad inferior. La conducta típica se configura mediante diversas acciones que implican el uso indebido de signos distintivos, patentes o diseños protegidos, generando perjuicios económicos y afectando la competencia leal en el mercado.

Estas conductas suelen presentarse en sectores como bebidas alcohólicas, productos farmacéuticos, dispositivos electrónicos, ropa, calzado y otros bienes de consumo masivo, donde se utilizan marcas registradas para comercializar productos falsificados. Esta práctica no solo perjudica al titular del derecho, sino que también

genera confusión en los consumidores y puede afectar incluso la salud pública cuando se trata de productos adulterados (Sandri, 2016).

Sin embargo, pese a la incorporación de estas disposiciones, el Código Orgánico Integral Penal mantiene una regulación limitada frente a los avances tecnológicos actuales. La normativa fue concebida principalmente para sancionar infracciones tradicionales, como la falsificación física de productos o la comercialización de copias ilegales. Esta regulación resulta insuficiente frente a nuevas formas de vulneración derivadas del uso de inteligencia artificial, las cuales permiten generar contenidos automatizados, replicar obras protegidas o modificar creaciones sin intervención directa del ser humano.

La ausencia de tipificación específica de las infracciones cometidas mediante inteligencia artificial genera dificultades para aplicar el principio de legalidad penal. En estos casos, los operadores jurídicos deben recurrir a tipos penales tradicionales que no se ajustan completamente a las nuevas conductas tecnológicas, lo que puede producir inseguridad jurídica y posibles escenarios de impunidad. En consecuencia, se evidencia la necesidad de actualizar la legislación penal ecuatoriana para incorporar nuevas formas de infracción digital y establecer criterios claros de imputación penal frente al uso de sistemas automatizados.

#### **1.4 Relación entre derecho penal y propiedad intelectual**

La Constitución reconoce diversas formas de propiedad pública, privada, comunitaria, estatal, asociativa y mixta, y establece que, independientemente del tipo de propiedad, esta debe cumplir una función social y ambiental, correspondiendo al Estado garantizar el efectivo uso y goce de este derecho. En este contexto, el artículo 322 reconoce de manera expresa a la propiedad intelectual como una modalidad específica de propiedad, la cual se rige por disposiciones particulares acordes con su objeto y naturaleza, desarrolladas principalmente en el Libro III del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, conocido como Código Ingenios.

La propiedad intelectual comprende tres grandes categorías: los derechos de autor y derechos conexos, la propiedad industrial y los derechos sobre obtenciones

vegetales. Cada uno de estos grupos presenta características propias y distintos ámbitos de protección. Sin embargo, de manera frecuente se identifica la propiedad intelectual únicamente con los derechos de autor, al considerarse que toda obra atribuible a un autor es producto del intelecto. Si bien esta afirmación es correcta, resulta incompleta, ya que las invenciones y las obtenciones vegetales también surgen de la actividad intelectual de sus creadores y, por tanto, forman parte del sistema de protección de la propiedad intelectual.

Para el análisis desde el ámbito penal es necesario identificar el bien jurídico protegido, el cual, en este caso, está constituido por los derechos derivados de la creación intelectual. En este sentido, el estudio se centra en los derechos de autor y derechos conexos, que se reconocen a favor de creadores, intérpretes, ejecutantes y demás titulares. Estos derechos se dividen en dos categorías: derechos morales y derechos patrimoniales. Los primeros tienen carácter irrenunciable, inalienable y permanente, y buscan proteger el vínculo personal entre el autor y su obra. Entre ellos se encuentran el derecho a la paternidad, que garantiza el reconocimiento del autor; el derecho al anonimato o al uso de seudónimo; el derecho a divulgar la obra en el momento y forma que considere pertinente; el derecho de acceso a ejemplares únicos o raros; el derecho a la integridad de la obra, que permite evitar alteraciones, deformaciones o mutilaciones; y el derecho a modificar la obra antes o después de su publicación.

Por su parte, los derechos patrimoniales otorgan al titular la facultad de explotar económicamente la obra y autorizar su utilización por terceros. Estos comprenden el derecho de reproducción, comunicación pública, distribución, importación y transformación de la obra, así como el derecho de seguimiento, que permite al autor percibir beneficios derivados de ventas posteriores a la primera comercialización. En la legislación ecuatoriana, estos derechos se mantienen vigentes, de manera general, hasta setenta años después de la muerte del autor, conforme lo establece el Código Ingenios.

La protección de estos derechos no se limita al ámbito civil o administrativo, sino que también se extiende al derecho penal cuando las conductas que los vulneran alcanzan un grado de gravedad relevante. En este sentido, el derecho penal cumple una función esencial al tipificar y sancionar aquellas acciones que afectan de manera significativa la propiedad intelectual, tales como la reproducción no autorizada, la

falsificación o la distribución ilícita de obras protegidas. De esta forma, la normativa penal actúa como un mecanismo de tutela reforzada que busca prevenir infracciones y proteger tanto el esfuerzo creativo como los intereses económicos de los titulares de derechos.

La intervención del derecho penal se justifica, entonces, en la necesidad de garantizar el respeto a la creatividad y a la producción intelectual, especialmente cuando las infracciones generan perjuicios importantes. Así, mientras la normativa de propiedad intelectual define el contenido y alcance de los derechos, el derecho penal sanciona su vulneración más grave, estableciendo una relación complementaria entre ambos ámbitos normativos. Esta articulación permite no solo la protección jurídica de las creaciones, sino también la disuasión de conductas ilícitas que afectan la explotación legítima de las obras.

No obstante, el desarrollo tecnológico y el avance de la inteligencia artificial han introducido nuevos desafíos para la aplicación del derecho penal en materia de propiedad intelectual. Las infracciones pueden ejecutarse mediante sistemas automatizados o plataformas digitales, lo que dificulta la identificación del responsable y la atribución de responsabilidad penal. Esta situación evidencia la necesidad de replantear los mecanismos tradicionales de protección y fortalecer la relación entre el derecho penal y la propiedad intelectual, incorporando criterios que permitan sancionar adecuadamente las infracciones cometidas mediante herramientas tecnológicas y asegurar una protección efectiva de las creaciones intelectuales en el entorno digital.

### **1.5 Análisis doctrinario**

La doctrina jurídica ha señalado que el avance de la inteligencia artificial exige la adaptación del derecho penal y de la propiedad intelectual. En este sentido, Floridi sostiene que los sistemas de inteligencia artificial carecen de autonomía moral y no pueden ser considerados sujetos responsables, por lo que la responsabilidad jurídica debe recaer en las personas que diseñan, programan o utilizan estas tecnologías (Floridi et al., 2018). Esta postura también es compartida por Calo, quien señala que la inteligencia artificial no posee voluntad ni conciencia, elementos indispensables para la imputación penal, por lo que la responsabilidad debe analizarse a partir de la conducta humana vinculada al funcionamiento del sistema (Calo, 2015).

Asimismo, la doctrina ha destacado que las categorías tradicionales del derecho penal, como la autoría, la participación y la culpabilidad, deben reinterpretarse frente a los nuevos escenarios tecnológicos. En este sentido, Navas Navarro indica que la inteligencia artificial introduce una relación indirecta entre la conducta humana y el resultado, lo que obliga a replantear los criterios de imputación penal considerando factores como el control del sistema, la previsibilidad del daño y la intervención en el desarrollo tecnológico (Navas Navarro, 2019).

Por otra parte, Guadamuz sostiene que el uso de inteligencia artificial en la generación de contenidos plantea importantes desafíos para la propiedad intelectual, especialmente en la determinación de la autoría y la titularidad de derechos. Esto se vuelve más complejo cuando las obras son creadas con mínima intervención humana, lo que dificulta identificar al responsable en caso de una infracción (Guadamuz, 2017).

En este contexto, el análisis doctrinario evidencia la necesidad de actualizar la legislación ecuatoriana para incorporar disposiciones específicas sobre inteligencia artificial y propiedad intelectual. La ausencia de regulación clara puede generar inseguridad jurídica y dificultar la protección efectiva de los derechos de autor en el entorno digital, particularmente frente a conductas como la reproducción automatizada, la transformación no autorizada de obras y la generación de contenidos derivados mediante sistemas de inteligencia artificial.

## Capítulo II

### **Vacíos jurídicos en la regulación de infracciones mediante inteligencia artificial.**

El avance acelerado de la inteligencia artificial ha generado beneficios significativos en distintos ámbitos, pero también ha planteado nuevos desafíos para el derecho penal y la protección de la propiedad intelectual. En este contexto, no solo resulta relevante analizar cómo se cometen las infracciones mediante inteligencia artificial, sino también determinar quiénes deben detectarlas, prevenirlas y sancionarlas. A medida que estas tecnologías se integran en la vida cotidiana, el rol del Estado y de la sociedad se vuelve fundamental para evitar la vulneración de derechos y la consolidación de espacios de impunidad digital.

Desde esta perspectiva, el Estado ecuatoriano debe fortalecer su rol institucional frente a las conductas delictivas vinculadas al uso de inteligencia artificial. Estas formas de criminalidad no responden a esquemas tradicionales, por lo que requieren nuevas herramientas jurídicas y tecnológicas para su identificación y sanción. En este sentido, la administración de justicia debe incorporar criterios técnicos y éticos sobre el uso de inteligencia artificial en las investigaciones penales, ya que la comprensión del funcionamiento de estas tecnologías resulta esencial para atribuir responsabilidades y garantizar la protección de las víctimas (Montañez Sierra, 2020).

Asimismo, aunque el Código Orgánico Integral Penal contempla ciertos delitos informáticos, no establece una regulación específica para las conductas ilícitas cometidas mediante inteligencia artificial. En este sentido, se ha señalado la necesidad de reformar el marco penal ecuatoriano para incorporar delitos tecnológicos y establecer criterios claros de imputación cuando la inteligencia artificial sea utilizada como instrumento delictivo (Guamán Terán, 2023). Estas propuestas apuntan a la construcción de un modelo normativo que incluya la participación de desarrolladores, plataformas tecnológicas y entidades públicas.

Por otro lado, la prevención y detección de delitos tecnológicos no corresponde únicamente al Estado, sino que también requiere la participación activa de la ciudadanía. La sociedad cumple un papel relevante en la educación digital, la identificación temprana de riesgos y la denuncia de actividades ilícitas. En este sentido,

se ha señalado que una gran parte de los delitos digitales, como los deepfakes o las estafas automatizadas, no son denunciados debido al desconocimiento sobre el funcionamiento de estas tecnologías o sobre las instituciones competentes para recibir denuncias, lo que evidencia una brecha tecnológica y jurídica que requiere ser atendida mediante programas de alfabetización digital (Sinaluisa Sagñay, 2024).

Asimismo, se ha propuesto la creación de observatorios ciudadanos de delitos informáticos que colaboren con las autoridades en la validación de evidencia digital y el monitoreo de plataformas en línea, destacando la necesidad de una respuesta coordinada entre el Estado y la ciudadanía (Andrade Arias & Yurank Tsamaraint, 2025). En la misma línea, se ha indicado que la gobernanza de la inteligencia artificial debe ser participativa, ética y corresponsable, involucrando tanto a instituciones públicas como a la sociedad (UNESCO, 2022).

### **2.1 Nuevas formas de infracción mediante inteligencia artificial.**

El avance de la inteligencia artificial ha permitido el surgimiento de nuevas formas de infracción que no estaban previstas en la normativa tradicional. Estas conductas se caracterizan por la utilización de sistemas automatizados capaces de generar, modificar o difundir contenido sin intervención humana directa, lo que dificulta la identificación del responsable y la aplicación de los tipos sancionatorios existentes. En este contexto, la inteligencia artificial no solo transforma los mecanismos de creación de contenido, sino también las modalidades mediante las cuales se pueden vulnerar derechos, especialmente en materia de propiedad intelectual y en el ámbito de la comunicación digital.

Entre las principales formas de infracción mediante inteligencia artificial se encuentra la generación automatizada de textos, imágenes, música, videos y software a partir del entrenamiento con obras protegidas. Este proceso puede implicar la utilización de contenido sin autorización del titular de derechos, lo que podría afectar los derechos patrimoniales del autor, particularmente en lo referente a la reproducción, transformación y comunicación pública de la obra. A diferencia de las infracciones tradicionales, estas conductas se ejecutan de manera automatizada y a gran escala, lo que incrementa el impacto económico y dificulta su control por parte de las autoridades.

Asimismo, la inteligencia artificial permite la creación de obras derivadas mediante algoritmos que imitan estilos artísticos, recrean voces o generan imágenes hiperrealistas. Estas herramientas posibilitan la producción de contenido que, aunque no constituye una copia exacta, mantiene similitudes sustanciales con la obra original, lo que genera dificultades para determinar la existencia de una infracción. Esta situación evidencia la necesidad de reinterpretar los mecanismos tradicionales de protección frente a las nuevas dinámicas tecnológicas.

Otra forma relevante de infracción corresponde a la creación y difusión de contenido multimedia manipulado mediante inteligencia artificial, como los denominados deepfakes. Estas tecnologías permiten alterar la imagen, voz o comportamiento de una persona, generando contenido aparentemente auténtico, pero que en realidad ha sido modificado artificialmente. Este tipo de material puede ser utilizado para desinformar, manipular la opinión pública o afectar la reputación de una persona, lo que amplía el alcance de las infracciones más allá del ámbito patrimonial y las proyecta hacia la afectación de derechos fundamentales.

Además, la inteligencia artificial facilita la reproducción masiva y distribución automatizada de contenido protegido en plataformas digitales y redes sociales. Esta difusión puede realizarse de manera simultánea en múltiples espacios virtuales, lo que incrementa la dificultad para identificar el origen del contenido y para aplicar medidas correctivas oportunas. En estos casos, la infracción no se limita a la creación del contenido, sino que también se extiende a su difusión automatizada, generando un impacto mayor en los titulares de derechos.

De igual manera, el entrenamiento de sistemas de inteligencia artificial mediante el uso de obras protegidas constituye una problemática adicional. En muchos casos, los modelos son alimentados con grandes volúmenes de información obtenida de internet sin autorización previa, lo que plantea interrogantes sobre la legalidad del uso de dichos contenidos. La dificultad radica en que el resultado generado por la inteligencia artificial no siempre reproduce directamente la obra original, sino que produce contenidos similares o derivados, lo que complica determinar la existencia de una vulneración.

En consecuencia, estas nuevas formas de infracción evidencian que la inteligencia artificial ha transformado los mecanismos tradicionales de vulneración de derechos, introduciendo conductas automatizadas, masivas y difíciles de controlar. Esta realidad pone de manifiesto la necesidad de analizar la adecuación de la normativa vigente frente a estas nuevas dinámicas tecnológicas, con el fin de garantizar una protección efectiva y evitar vacíos jurídicos que puedan generar impunidad.

## **2.2 Problemas de tipicidad penal**

La tipicidad constituye uno de los elementos esenciales dentro de la teoría del delito, ya que permite determinar si una conducta puede ser considerada penalmente relevante. En este sentido, la tipicidad implica la adecuación entre el hecho realizado y la descripción prevista en la norma penal. Cuando la conducta se ajusta a los elementos del tipo penal, se configura una conducta típica; caso contrario, se trata de una conducta atípica que no puede ser sancionada penalmente. En este contexto, Zaffaroni señala que la tipicidad consiste en el encaje entre un hecho real y la descripción normativa contenida en la ley penal, lo que permite establecer si existe o no relevancia jurídica desde el punto de vista penal (Zaffaroni, 1981).

El principio de tipicidad penal se encuentra vinculado al principio de legalidad, el cual establece que ninguna persona puede ser sancionada por una conducta que no se encuentre previamente descrita en la ley. Este principio garantiza la seguridad jurídica y limita el poder punitivo del Estado, evitando interpretaciones extensivas o analógicas que puedan afectar los derechos de los ciudadanos. En consecuencia, para que una conducta sea sancionada, debe encajar de manera clara y precisa en el tipo penal correspondiente.

Sin embargo, las infracciones cometidas mediante inteligencia artificial generan dificultades para su adecuación típica, debido a que la normativa penal vigente fue diseñada para conductas ejecutadas directamente por personas. En estos casos, la inteligencia artificial introduce un elemento intermedio entre la acción humana y el resultado, lo que dificulta determinar si la conducta encaja en los tipos penales existentes. Esta situación se vuelve más compleja cuando el sistema automatizado

genera contenido sin intervención directa del usuario o produce resultados no previstos por quien lo programó.

El Código Orgánico Integral Penal contempla delitos relacionados con la vulneración de derechos de autor, así como infracciones informáticas, pero no regula expresamente la utilización de inteligencia artificial como medio para la comisión de estas conductas. En este sentido, los tipos penales existentes parten del supuesto de una acción humana directa, lo que genera incertidumbre cuando la conducta se realiza mediante sistemas automatizados. Como consecuencia, la conducta puede resultar lesiva para los derechos protegidos, pero no encajar de manera clara dentro de la descripción normativa.

Asimismo, la inteligencia artificial permite la generación automatizada de contenidos que pueden constituir reproducción, transformación o comunicación pública de obras protegidas, sin que exista una acción directa del sujeto activo. Esta situación dificulta determinar si el comportamiento corresponde a una conducta típica, ya que la intervención humana puede limitarse a la configuración inicial del sistema o al uso de una herramienta tecnológica. De esta manera, la adecuación típica se vuelve compleja, debido a que la conducta no se encuentra prevista expresamente en la ley penal.

Otro problema de tipicidad se presenta en relación con la difusión automatizada de contenido generado mediante inteligencia artificial. En estos casos, el sistema puede reproducir o distribuir material protegido de manera masiva, lo que genera un resultado lesivo para los titulares de derechos. Sin embargo, la normativa penal no contempla expresamente este tipo de conductas, lo que dificulta encuadrarlas dentro de los tipos existentes y puede generar supuestos de atipicidad.

En consecuencia, la ausencia de regulación específica sobre la utilización de inteligencia artificial en la comisión de infracciones genera un vacío jurídico que limita la aplicación del derecho penal. Esta situación impide sancionar determinadas conductas que, aunque resultan lesivas para los derechos de propiedad intelectual, no encajan de manera clara en los tipos penales vigentes. Por ello, se evidencia la necesidad de adaptar la normativa penal para incluir nuevas formas de comisión del delito mediante inteligencia artificial, garantizando así la protección efectiva de los bienes jurídicos tutelados.

### 2.3 Imputación de responsabilidad penal

La imputación de responsabilidad penal en el contexto del uso de inteligencia artificial constituye uno de los principales retos del derecho penal contemporáneo. El sistema penal ecuatoriano, al igual que otros ordenamientos jurídicos, se fundamenta en la responsabilidad personal, lo que implica que únicamente las personas pueden ser consideradas sujetos activos del delito. La imputación penal exige la existencia de conducta humana, capacidad de culpabilidad y la posibilidad de actuar con dolo o culpa, elementos que no pueden atribuirse a sistemas automatizados. En este sentido, la inteligencia artificial carece de voluntad, conciencia y capacidad de comprender la ilicitud de sus actos, por lo que no puede ser considerada penalmente responsable (Zaffaroni, 2002).

A partir del análisis del Código Orgánico Integral Penal, se puede constatar que la normativa penal ecuatoriana estructura la responsabilidad penal en torno a la acción u omisión de una persona. Esto implica que, aunque la inteligencia artificial pueda intervenir en la comisión de una conducta ilícita, su participación se limita al carácter de herramienta o medio. De este modo, cuando un sistema automatizado genera documentos falsos, manipula información o difunde contenido ilícito, la responsabilidad penal debe recaer en el sujeto humano que interviene en su programación, implementación o utilización con fines delictivos. Esta interpretación resulta coherente con el principio de culpabilidad, el cual exige que la sanción penal se imponga únicamente a quien tenga la posibilidad de comprender la ilicitud de su conducta y actuar conforme a dicha comprensión (Roxin, 1997).

No obstante, la imputación penal se vuelve compleja cuando intervienen múltiples sujetos en el funcionamiento del sistema de inteligencia artificial. En estos casos pueden participar el desarrollador del software, el programador del algoritmo, el proveedor de la plataforma, el usuario que introduce instrucciones y la persona que obtiene el beneficio del resultado. Esta pluralidad de intervinientes dificulta determinar quién posee el dominio del hecho y, por tanto, quién debe responder penalmente. La teoría del dominio del hecho permite identificar al sujeto que tiene el control funcional de la conducta, pero su aplicación se complica cuando el resultado es generado por un sistema automatizado con cierto grado de autonomía (Roxin, 1997).

Además, la inteligencia artificial puede generar resultados no previstos por el usuario o por el programador, lo que introduce dificultades para determinar la existencia de dolo o culpa. En estos casos, la imputación penal debe analizar la previsibilidad del resultado y el grado de control que tenía el sujeto sobre el sistema. Si el resultado era previsible y el sujeto no adoptó medidas para evitarlo, podría configurarse responsabilidad por culpa. En cambio, si el sujeto utilizó deliberadamente la inteligencia artificial para producir un resultado ilícito, se podría configurar responsabilidad dolosa. Este análisis resulta necesario para adaptar los criterios tradicionales de imputación a los nuevos escenarios tecnológicos.

Otro aspecto relevante es la autonomía funcional que presentan algunos sistemas de inteligencia artificial. Estos pueden aprender a partir de datos y modificar su comportamiento sin intervención directa del usuario, lo que genera una relación indirecta entre la acción humana y el resultado. Esta situación dificulta establecer la imputación penal, ya que el sujeto puede no tener control total sobre la conducta final. Por ello, la doctrina propone considerar criterios como el control del sistema, la diligencia en su utilización, la previsibilidad del daño y el beneficio obtenido, con el fin de determinar la responsabilidad penal de los intervinientes (Calo, 2015).

El ordenamiento jurídico ecuatoriano no establece disposiciones específicas sobre la responsabilidad derivada del uso de inteligencia artificial, lo que genera vacíos normativos en la determinación del sujeto responsable. El Código Orgánico Integral Penal regula delitos informáticos, falsificación documental, suplantación de identidad y vulneración de derechos de autor, pero no contempla expresamente la utilización de inteligencia artificial como medio de comisión del delito. Esta ausencia normativa dificulta la aplicación uniforme del derecho penal cuando el resultado es generado mediante sistemas automatizados.

En consecuencia, el sistema penal ecuatoriano, al mantenerse centrado en la imputación exclusivamente humana, puede enfrentar dificultades frente a nuevas formas de criminalidad digital mediada por algoritmos. La falta de regulación específica impide establecer criterios claros sobre la responsabilidad del programador, del usuario o del proveedor del sistema, lo que evidencia la necesidad de adaptar la normativa penal a los desafíos que plantea la inteligencia artificial. La incorporación de criterios de imputación basados en el control del sistema, la previsibilidad del resultado

y la participación en su desarrollo permitiría delimitar la responsabilidad penal y evitar espacios de impunidad en el entorno digital.

## **2.4 Análisis de la conducta, tipicidad, antijuridicidad y culpabilidad**

Para analizar la responsabilidad penal derivada del uso de la inteligencia artificial, es necesario examinar los elementos estructurales del delito, particularmente la conducta, la tipicidad, la antijuridicidad y la culpabilidad. La doctrina penal señala que la existencia del delito exige la concurrencia de dos grandes macroelementos: el injusto penal y la culpabilidad. El primero comprende la conducta típica y antijurídica, mientras que el segundo se relaciona con la posibilidad de atribuir el hecho al sujeto que lo ejecuta, considerando la imputabilidad, el dolo o la culpa y la exigibilidad de una conducta distinta (Obregón García & Gómez Lanz, 2023).

La conducta constituye el punto de partida del análisis penal, entendida como la acción u omisión humana voluntaria que produce una modificación en el mundo exterior. En los delitos cometidos mediante inteligencia artificial, la conducta no siempre se presenta de manera directa, ya que el resultado puede generarse a través de sistemas automatizados que actúan a partir de instrucciones previas o aprendizaje autónomo. Esta situación introduce una relación mediata entre la acción humana y el resultado, lo que obliga a examinar si la conducta relevante corresponde al programador, al desarrollador, al usuario o a cualquier otro interviniente en el funcionamiento del sistema. De esta forma, la acción humana se materializa a través de un instrumento tecnológico con cierto grado de autonomía, lo que complejiza la atribución de responsabilidad penal (Diamantis, 2023).

La tipicidad constituye el elemento central de la antijuridicidad penal, ya que determina qué conductas son consideradas ilícitas por el legislador. Este juicio implica verificar si los hechos encajan en la descripción normativa prevista en la ley penal. La tipicidad es predominantemente objetiva, puesto que describe el proceso causal entre la conducta y el resultado, aunque también puede incluir elementos normativos y subjetivos. Asimismo, supone una valoración negativa de la conducta, al considerarla una lesión o puesta en peligro de un bien jurídico protegido (Obregón García & Gómez Lanz, 2023). En el ámbito de la inteligencia artificial, la tipicidad presenta dificultades, debido a que muchos resultados lesivos pueden generarse mediante algoritmos sin que

exista una descripción normativa específica que contemple este tipo de intervención tecnológica.

Dentro de la tipicidad es importante distinguir entre los tipos penales de mera actividad y los tipos de resultado. Los primeros se consuman con la simple realización de la conducta, mientras que los segundos exigen la producción de un resultado separable espacial y temporalmente de la acción. En los delitos vinculados con inteligencia artificial, los problemas se presentan principalmente en los delitos de resultado, donde es necesario establecer la relación entre la acción humana y el daño producido. Para ello, resulta indispensable determinar si el resultado puede atribuirse al sujeto que intervino en el funcionamiento del sistema, lo que conduce al análisis de la imputación objetiva (Roxin, 1997).

La imputación objetiva permite atribuir un resultado a una conducta cuando existe una relación de riesgo entre la acción y el daño producido. En este sentido, un sujeto solo responde penalmente si su conducta creó o incrementó un riesgo jurídicamente desaprobado y dicho riesgo se concretó en el resultado. Esta teoría supera el análisis puramente causal y añade un componente normativo que permite delimitar la responsabilidad penal. En el ámbito de la inteligencia artificial, esta teoría resulta fundamental, ya que el resultado puede originarse en la interacción de múltiples factores, lo que dificulta determinar si el riesgo creado por la conducta humana es el que finalmente se materializa (Obregón García & Gómez Lanz, 2023).

El análisis de la relación de causalidad constituye otro elemento esencial en los delitos de resultado. Tradicionalmente se ha aplicado la teoría de la equivalencia de las condiciones o *condicio sine qua non*, según la cual una acción es causa del resultado si al suprimirla mentalmente el resultado desaparece. Sin embargo, esta teoría presenta dificultades en el contexto de la inteligencia artificial, debido a que en el desarrollo y funcionamiento de estos sistemas intervienen múltiples sujetos, como programadores, empresas desarrolladoras, proveedores de datos y usuarios. Esta multiplicidad de intervinientes amplía la cadena causal y complica la determinación del responsable (Diamantis, 2023).

En este sentido, la doctrina ha identificado el denominado *many hands problem*, que hace referencia a la dificultad de atribuir responsabilidad cuando intervienen

numerosas personas en el desarrollo y funcionamiento de sistemas automatizados. En estos casos, el resultado lesivo puede ser consecuencia de la interacción de múltiples decisiones, lo que impide identificar con claridad al sujeto responsable. Asimismo, se ha señalado el *no hands problem*, que se presenta cuando el sistema produce un resultado dañoso aun cuando todos los intervinientes hayan actuado de manera diligente, debido al margen de autonomía e imprevisibilidad de algunos algoritmos (Diamantis, 2023).

La antijuridicidad implica que la conducta típica sea contraria al ordenamiento jurídico y no esté amparada por una causa de justificación. En el contexto de la inteligencia artificial, este análisis requiere determinar si el uso del sistema se realizó dentro de los límites permitidos o si se empleó para vulnerar bienes jurídicos protegidos. La dificultad radica en que muchas conductas pueden tener una finalidad legítima, como el desarrollo tecnológico o la automatización de procesos, pero generar resultados lesivos no previstos. Esto obliga a examinar cuidadosamente si la conducta excede el riesgo permitido y constituye una afectación jurídicamente relevante (Zaffaroni, 2002).

Finalmente, la culpabilidad permite atribuir el hecho al sujeto desde una perspectiva personal, evaluando su imputabilidad, el dolo o la culpa y la exigibilidad de una conducta distinta. En los delitos cometidos mediante inteligencia artificial, la culpabilidad se centra en el sujeto humano que interviene en el diseño, programación o utilización del sistema. La inteligencia artificial, al carecer de conciencia y voluntad, no puede ser considerada culpable. Por ello, la responsabilidad penal debe recaer en la persona que tenía el control del sistema o que utilizó la tecnología con conocimiento del riesgo, evitando así espacios de impunidad frente a nuevas formas de criminalidad digital (Roxin, 1997).

En consecuencia, el análisis conjunto de la conducta, la tipicidad, la antijuridicidad y la culpabilidad permite comprender los desafíos que plantea la inteligencia artificial para el derecho penal. La intervención de sistemas automatizados introduce dificultades en la determinación de la acción, la atribución del resultado y la identificación del sujeto responsable, lo que evidencia la necesidad de adaptar las categorías tradicionales del derecho penal a los nuevos escenarios tecnológicos (Obregón García & Gómez Lanz, 2023).

## **2.5 Insuficiencia normativa del COIP y del Código Ingenios en la regulación de infracciones cometidas mediante inteligencia artificial**

El análisis del marco jurídico ecuatoriano evidencia que, aunque determinadas conductas relacionadas con la suplantación de identidad y el uso indebido de tecnologías digitales han sido tradicionalmente perseguidas por la norma penal sustantiva, la regulación vigente resulta insuficiente frente a las nuevas modalidades delictivas vinculadas con la inteligencia artificial. La incorporación del artículo 212 del Código Orgánico Integral Penal en 2014 permitió sancionar la suplantación de identidad; sin embargo, la formulación general del tipo penal no alcanza a cubrir de manera adecuada las conductas realizadas mediante tecnologías avanzadas, especialmente aquellas que utilizan inteligencia artificial para generar contenidos falsos, manipular datos o recrear identidades digitales con mayor precisión (Endara et al., 2024). Esta limitación normativa revela que el legislador diseñó la disposición para escenarios tradicionales, sin prever el uso masivo y automatizado de herramientas tecnológicas que incrementan la complejidad de estas infracciones.

El impacto de estas conductas no se limita al daño patrimonial individual, sino que también genera efectos negativos en la confianza de los sistemas digitales y en la seguridad jurídica. La utilización de inteligencia artificial para cometer fraudes, suplantaciones o manipulación de contenidos reduce la credibilidad de las plataformas tecnológicas y dificulta la identificación de los responsables, especialmente cuando los niveles de detección y sanción resultan bajos. Esta situación incrementa el riesgo de impunidad y evidencia la necesidad de fortalecer la normativa penal para responder a nuevas formas de criminalidad digital (Muncaster, 2025).

El crecimiento de estos ilícitos ha motivado el desarrollo de diversas investigaciones jurídicas que analizan la suplantación de identidad mediante inteligencia artificial desde diferentes perspectivas. Algunos estudios se centran en la modelación de fraudes digitales mediante IA, evidenciando cómo los algoritmos pueden recrear identidades y generar contenido engañoso con fines ilícitos (Alviani & Fitri, 2024; Subramanian, 2024). Otros trabajos abordan mecanismos de detección de estas conductas, proponiendo herramientas tecnológicas para identificar manipulaciones digitales o contenidos generados artificialmente (Zahirah Zahra & Wei, 2023; Deb, 2024). Asimismo, existen investigaciones orientadas al desarrollo de

sistemas de protección y seguridad informática, con el objetivo de reducir los riesgos asociados al uso indebido de inteligencia artificial (Torguatova & Osmonaliyev, 2024). Finalmente, una línea doctrinaria relevante se enfoca en la revisión y adecuación del marco normativo de cada país para mejorar la respuesta penal frente a estas conductas, proponiendo reformas legislativas que contemplen expresamente el uso de inteligencia artificial como medio delictivo (Recalde, 2025; Endara et al., 2024).

En el caso ecuatoriano, diversos autores coinciden en señalar debilidades en la cobertura penal respecto a la suplantación de identidad mediante inteligencia artificial. Estudios doctrinarios sostienen que el artículo 212 del COIP no contempla de manera expresa las nuevas formas de fraude identitario basadas en tecnologías automatizadas, lo que limita la capacidad de los operadores de justicia para sancionar estas conductas de manera efectiva. Desde esta perspectiva, se plantea la necesidad de revisar la figura penal existente o incorporar nuevas disposiciones que permitan regular estas modalidades delictivas, así como desarrollar políticas públicas que fortalezcan la prevención y persecución penal (Endara et al., 2024; Recalde, 2025; García, 2024).

De igual manera, el análisis conjunto del Código Orgánico Integral Penal y del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación evidencia vacíos normativos en la regulación de infracciones cometidas mediante inteligencia artificial. El COIP tipifica delitos relacionados con la vulneración de derechos de autor, la suplantación de identidad y los delitos informáticos; sin embargo, no contempla expresamente la inteligencia artificial como medio de comisión del delito ni establece criterios para determinar la responsabilidad cuando intervienen sistemas automatizados. Esta omisión dificulta la aplicación del principio de tipicidad penal, ya que muchas conductas lesivas no encajan claramente dentro de los tipos existentes.

Por su parte, el Código Ingenios regula la protección de la propiedad intelectual y reconoce derechos morales y patrimoniales sobre las obras, pero no establece disposiciones específicas respecto a la generación automatizada de contenidos mediante inteligencia artificial. Tampoco define criterios sobre la titularidad de obras creadas con sistemas algorítmicos, ni regula el uso de obras protegidas para el entrenamiento de modelos de inteligencia artificial. Esta ausencia normativa genera incertidumbre respecto a la protección de los derechos de autor cuando las creaciones

derivan de procesos automatizados o cuando se emplean contenidos protegidos sin autorización del titular.

En consecuencia, la falta de regulación específica en ambas normas produce inseguridad jurídica y dificulta la aplicación efectiva del derecho penal en la protección de la propiedad intelectual frente al uso de inteligencia artificial. La inexistencia de disposiciones claras sobre tipicidad, responsabilidad e imputación penal permite que determinadas conductas queden fuera del ámbito sancionador, lo que evidencia la necesidad de reformar el marco normativo ecuatoriano. La incorporación de disposiciones que regulen el uso de inteligencia artificial, definan criterios de responsabilidad y establezcan mecanismos de protección de los derechos de autor contribuiría a fortalecer la seguridad jurídica y garantizar una respuesta penal adecuada frente a nuevas formas de criminalidad tecnológica.

### Capítulo III

## DERECHO COMPARADO Y PROPUESTAS DE REGULACIÓN EN EL ECUADOR

El análisis del derecho comparado constituye una herramienta fundamental para evaluar la posibilidad de incorporar en el Ecuador mecanismos normativos adecuados frente a los delitos derivados del uso de la inteligencia artificial. Mientras varias jurisdicciones han desarrollado marcos regulatorios específicos para abordar conductas como el fraude automatizado, la manipulación de información, la suplantación de identidad digital o los ciberataques mediante sistemas inteligentes, el ordenamiento jurídico ecuatoriano aún carece de una regulación expresa que permita tipificar estas conductas de manera clara. Esta situación evidencia la necesidad de examinar experiencias internacionales con el fin de identificar criterios doctrinarios y normativos que puedan ser adaptados a la realidad nacional.

En el caso de Estados Unidos, la regulación presenta un enfoque centrado en la responsabilidad civil y penal de las personas naturales y jurídicas que intervienen en el diseño, desarrollo o utilización de sistemas de inteligencia artificial. Su marco legal es fragmentado y se compone de leyes federales como el Computer Fraud and Abuse Act, además de normativa estatal y precedentes jurisprudenciales vinculados al cibercrimen, la privacidad y la responsabilidad tecnológica. Este modelo resulta relevante para el contexto ecuatoriano, ya que permite delimitar la responsabilidad individual y corporativa en delitos cometidos mediante inteligencia artificial, especialmente cuando intervienen desarrolladores, empresas tecnológicas y usuarios finales. Asimismo, la experiencia estadounidense puede orientar la tipificación penal de conductas como la manipulación algorítmica, el acceso no autorizado a sistemas informáticos o la automatización de fraudes digitales.

Por su parte, la Unión Europea ha avanzado hacia un modelo regulatorio basado en principios éticos y en la gestión de riesgos derivados del uso de la inteligencia artificial. La propuesta del Reglamento de Inteligencia Artificial, junto con instrumentos como el Reglamento General de Protección de Datos, establece obligaciones de transparencia, trazabilidad y control sobre los sistemas automatizados.

Además, la jurisprudencia del Tribunal de Justicia de la Unión Europea ha comenzado a desarrollar criterios sobre responsabilidad por decisiones automatizadas. Este enfoque resulta aplicable al contexto ecuatoriano, ya que prioriza la protección de derechos fundamentales, el consentimiento informado y la supervisión de algoritmos. La adopción de un modelo similar permitiría prevenir abusos derivados del uso de inteligencia artificial y fortalecer la seguridad jurídica frente a decisiones automatizadas.

En Japón, la regulación se orienta principalmente a la ciberseguridad y a la prevención de delitos tecnológicos y financieros. La normativa japonesa incorpora disposiciones sobre seguridad informática, protección de infraestructuras críticas y regulación ética del uso de inteligencia artificial. La jurisprudencia se ha enfocado en casos de fraude digital, manipulación de datos y vulneraciones a sistemas informáticos. Este modelo ofrece un enfoque preventivo y técnico que podría adaptarse al Ecuador, especialmente en la lucha contra delitos financieros cometidos mediante inteligencia artificial, así como en la protección de sistemas bancarios y plataformas digitales.

Brasil, por su parte, ha desarrollado un enfoque emergente centrado en la responsabilidad de plataformas digitales y la regulación del uso de algoritmos. El Marco Civil de Internet y la Ley General de Protección de Datos establecen obligaciones para proveedores de servicios digitales y criterios de responsabilidad frente a contenidos ilícitos. La jurisprudencia brasileña ha reconocido la responsabilidad de plataformas cuando existe difusión de contenido ilegal o delictivo. Este modelo resulta especialmente útil para el Ecuador debido a su cercanía jurídica y lingüística, ya que permite establecer mecanismos de control sobre redes sociales, comercio electrónico y servicios digitales que emplean inteligencia artificial.

En contraste con estos avances, el Ecuador presenta un enfoque incipiente. El Código Orgánico Integral Penal no contempla disposiciones específicas sobre delitos cometidos mediante inteligencia artificial, y la jurisprudencia en esta materia es limitada. Esta situación evidencia la necesidad de una reforma integral que incluya la tipificación de nuevas conductas delictivas, la delimitación de sujetos responsables y la incorporación de mecanismos técnicos y éticos de control. La experiencia comparada demuestra que la regulación de la inteligencia artificial no busca limitar el desarrollo

tecnológico, sino establecer garantías para la protección de derechos y la seguridad jurídica.

En este contexto, resulta pertinente proponer reformas a la legislación penal ecuatoriana que permitan incorporar la inteligencia artificial como medio de comisión del delito. En materia de dolo, se plantea reconocer el denominado dolo tecnológico, entendiendo que existe intención cuando la persona tiene control funcional o técnico sobre el sistema automatizado y prevé el resultado dañoso. Asimismo, en relación con la culpa, se propone ampliar el deber objetivo de cuidado a quienes desarrollen, supervisen o utilicen sistemas de inteligencia artificial, considerando la negligencia en la programación, control o mantenimiento de dichos sistemas.

En cuanto a la autoría y participación, se propone incorporar la utilización de inteligencia artificial como forma de ejecución del delito, reconociendo la responsabilidad de quienes diseñen, configuren o utilicen estos sistemas con fines ilícitos. De igual manera, se plantea ampliar la complicidad a quienes cooperen mediante medios digitales o automatizados, siempre que su intervención facilite la comisión de la infracción penal.

También se considera necesario reformar tipos penales específicos para incluir el uso de inteligencia artificial como agravante o como medio de comisión del delito. Entre ellos, la intimidación, la instigación al suicidio, el hostigamiento, la estafa, la transferencia electrónica de activos y la falsificación informática. En estos casos, la utilización de sistemas automatizados, algoritmos o herramientas generativas incrementa el alcance del daño, dificulta la identificación del responsable y amplía el número de víctimas, lo que justifica su reconocimiento expreso dentro de la norma penal.

Estos planteamientos coinciden con lo señalado por Chesterman (2021), quien sostiene que los marcos jurídicos tradicionales resultan insuficientes para enfrentar los delitos derivados del uso de inteligencia artificial, debido a la aparición de nuevas formas de criminalidad digital. De igual manera, Pagallo (2022) destaca la necesidad de establecer criterios de transparencia algorítmica y modelos de responsabilidad adaptados a los sistemas autónomos. Asimismo, Rodríguez Mendoza y Maldonado Ruiz (2024) subrayan que la inteligencia artificial debe ser regulada tanto para prevenir

delitos como para fortalecer la investigación penal, siempre dentro de un marco jurídico que garantice la protección de derechos fundamentales.

En consecuencia, el análisis del derecho comparado evidencia que el Ecuador requiere incorporar disposiciones específicas sobre inteligencia artificial en su legislación penal. La adopción de criterios doctrinarios y normativos provenientes de otras jurisdicciones permitiría tipificar nuevas conductas, delimitar responsabilidades y establecer mecanismos de control adecuados. De esta manera, se fortalecería la seguridad jurídica y se garantizaría una respuesta efectiva frente a los delitos derivados del uso de inteligencia artificial en el contexto ecuatoriano.

### **3.1 Regulación en la Unión Europea**

La Unión Europea ha sido una de las jurisdicciones pioneras en la construcción de un marco normativo específico para enfrentar los desafíos jurídicos derivados del uso de la inteligencia artificial. Su modelo se fundamenta en la protección de los derechos fundamentales, la seguridad jurídica y la gestión de riesgos asociados al uso de sistemas automatizados. En materia de propiedad intelectual, la normativa europea mantiene el criterio tradicional según el cual las obras protegidas deben ser el resultado de una creación intelectual humana, lo que excluye, en principio, a los contenidos generados de manera autónoma por sistemas de inteligencia artificial (Parlamento Europeo, 2019). Sin embargo, se reconoce que estas herramientas pueden intervenir como apoyo técnico dentro del proceso creativo, caso en el cual la titularidad de los derechos corresponde a la persona que ejerce un control creativo relevante sobre el resultado final (Chesterman, 2021).

La Directiva sobre derechos de autor en el mercado único digital reafirma este enfoque, al priorizar la intervención humana como elemento determinante para el reconocimiento de protección jurídica. No obstante, el avance tecnológico ha generado nuevos escenarios en los que la inteligencia artificial puede producir textos, imágenes, audios o videos con un alto grado de autonomía, lo que ha obligado a la Unión Europea a desarrollar mecanismos regulatorios complementarios orientados a garantizar la protección efectiva de los titulares de derechos. En este contexto, se han incorporado obligaciones relacionadas con la transparencia en el uso de datos, especialmente cuando

los sistemas son entrenados con obras protegidas, así como deberes de información respecto del material utilizado para el entrenamiento de algoritmos (Pagallo, 2022).

Desde la perspectiva penal, los Estados miembros han optado por reforzar la responsabilidad de los sujetos humanos que utilizan tecnologías digitales para vulnerar derechos de propiedad intelectual. Aunque no se reconoce responsabilidad penal directa a los sistemas de inteligencia artificial, se han establecido agravantes y mecanismos de imputación que permiten sancionar a quienes emplean estas herramientas con fines ilícitos, particularmente cuando el daño afecta a un número amplio de víctimas o genera perjuicios económicos significativos. Este enfoque busca evitar zonas de impunidad derivadas del uso de tecnologías avanzadas y garantizar que siempre exista un sujeto responsable (Hallevy, 2015).

Asimismo, el Reglamento de Inteligencia Artificial de la Unión Europea introduce un modelo basado en niveles de riesgo, clasificando los sistemas según su potencial de afectar derechos fundamentales. Para los sistemas considerados de alto riesgo, se imponen obligaciones específicas a desarrolladores, proveedores y usuarios, tales como la implementación de mecanismos de control, documentación técnica, evaluación de impacto y supervisión humana. Aunque estas disposiciones no son de naturaleza penal, su relevancia radica en que establecen estándares de diligencia que pueden ser utilizados para determinar responsabilidades jurídicas cuando se produzcan infracciones relacionadas con el funcionamiento de la inteligencia artificial (European Commission, 2021).

### **Criterios europeos sobre responsabilidad humana y control efectivo.**

Uno de los aportes más relevantes del modelo europeo es la consolidación del criterio de control efectivo como base para la atribución de responsabilidad. Conforme a este enfoque, la responsabilidad jurídica recae en la persona que tiene la capacidad de influir de manera determinante en el funcionamiento del sistema y en los resultados que este produce. Este criterio permite identificar al sujeto responsable incluso cuando la conducta ilícita es ejecutada mediante procesos automatizados, evitando que la autonomía tecnológica genere vacíos normativos (Pagallo, 2022).

De acuerdo con esta perspectiva, cuando el desarrollador, proveedor o usuario conoce los riesgos asociados al sistema y omite adoptar medidas razonables para prevenir daños, puede configurarse responsabilidad administrativa, civil o penal. El control efectivo se vincula con la posibilidad de supervisar, modificar o detener el funcionamiento del sistema, así como con la previsibilidad del resultado dañoso. De esta manera, el modelo europeo prioriza la responsabilidad humana sin necesidad de atribuir personalidad jurídica a la inteligencia artificial (Chesterman, 2021).

No obstante, parte de la doctrina ha planteado la posibilidad de reconocer algún tipo de personalidad jurídica a los sistemas de inteligencia artificial altamente autónomos. Entre estas propuestas destaca el modelo desarrollado por Hallevy, que sugiere la posibilidad de considerar a la inteligencia artificial como un sujeto de imputación cuando actúe con autonomía suficiente. Esta postura implicaría una forma de “humanización” jurídica de la inteligencia artificial, permitiendo atribuirle responsabilidad directa por los daños ocasionados (Hallevy, 2015). El Parlamento Europeo, mediante su resolución de 16 de febrero de 2017 sobre normas de derecho civil en materia de robótica, analizó la posibilidad de crear una personalidad jurídica específica para robots autónomos, señalando que mientras mayor sea su autonomía, más difícil resulta considerarlos simples instrumentos en manos de los seres humanos. En ese contexto, se propuso estudiar la creación de una categoría de “persona electrónica” que permita atribuir responsabilidades a sistemas altamente autónomos (Parlamento Europeo, 2017).

A pesar de estas propuestas, la mayoría de la doctrina considera que, en el estado actual del desarrollo tecnológico, la atribución de responsabilidad penal directa a la inteligencia artificial resulta inviable. Se sostiene que los sistemas automatizados carecen de voluntad, conciencia y capacidad de culpabilidad, elementos indispensables para la imputación penal. En este sentido, se afirma que los sistemas de inteligencia artificial no pueden ser considerados sujetos capaces de acción ni destinatarios de una pena, por lo que la responsabilidad debe seguir recayendo en las personas naturales o jurídicas que los desarrollan, programan, controlan o utilizan (Del Rosal, 2023).

### **3.2 Regulación en Estados Unidos**

A diferencia del modelo europeo, Estados Unidos ha desarrollado la regulación

de la inteligencia artificial mediante un enfoque flexible basado principalmente en la jurisprudencia, lineamientos administrativos y la interpretación de normas preexistentes. Este sistema no ha adoptado una legislación integral específica sobre inteligencia artificial, sino que ha optado por aplicar las normas tradicionales de propiedad intelectual, responsabilidad civil y derecho penal a los nuevos escenarios tecnológicos. Este enfoque pragmático permite adaptar las disposiciones jurídicas existentes a los desafíos derivados del uso de sistemas automatizados sin necesidad de reformas legislativas inmediatas (Chesterman, 2021).

En materia de derechos de autor, la Oficina de Copyright de Estados Unidos ha sostenido de forma reiterada que únicamente las obras creadas por seres humanos pueden ser protegidas por la legislación vigente. Este criterio ha sido reafirmado en diversas decisiones administrativas y judiciales que han rechazado solicitudes de registro de obras generadas exclusivamente por inteligencia artificial, al considerar que la autoría requiere una intervención humana significativa. Bajo esta interpretación, cuando la inteligencia artificial participa únicamente como herramienta, los derechos corresponden a la persona que dirige el proceso creativo; pero si el contenido es producido de manera autónoma por el sistema, no se reconoce protección jurídica (U.S. Copyright Office, 2023).

Este enfoque ha generado debates sobre la titularidad de las obras creadas mediante sistemas automatizados, especialmente cuando los modelos son entrenados con grandes volúmenes de contenido protegido. En estos casos, la discusión jurídica se centra en determinar si el uso de obras para el entrenamiento constituye una infracción a los derechos de autor o si puede considerarse un uso legítimo dentro de las excepciones existentes, como el fair use. La jurisprudencia estadounidense ha comenzado a analizar estos supuestos, evaluando factores como la finalidad del uso, el carácter transformativo del resultado y el impacto económico sobre el titular del derecho (Samuelson, 2020).

Desde la perspectiva penal, el ordenamiento jurídico estadounidense tampoco reconoce a la inteligencia artificial como sujeto de responsabilidad. La imputación recae exclusivamente en las personas naturales o jurídicas que diseñan, desarrollan, implementan o utilizan estas tecnologías con fines ilícitos. En este sentido, las leyes federales contemplan sanciones severas para la reproducción, distribución o

comunicación pública no autorizada de obras protegidas, especialmente cuando dichas conductas se realizan con fines comerciales o afectan a múltiples víctimas. Estas disposiciones se aplican también cuando las infracciones son cometidas mediante sistemas automatizados o inteligencia artificial (Diamantis, 2023).

Asimismo, la legislación estadounidense en materia de delitos informáticos, como el Computer Fraud and Abuse Act, permite sancionar conductas relacionadas con accesos no autorizados, manipulación de datos o uso indebido de sistemas informáticos, incluyendo aquellos que incorporan inteligencia artificial. Estas normas han sido utilizadas para perseguir conductas en las que algoritmos o sistemas automatizados son empleados para cometer fraude, suplantación de identidad o apropiación indebida de información protegida (Kerr, 2022).

### **Responsabilidad penal indirecta y teorías de imputación en Estados Unidos**

Un elemento característico del modelo estadounidense es el desarrollo de teorías de responsabilidad indirecta que permiten ampliar el espectro de sujetos responsables. Entre estas destacan la responsabilidad contributiva y la responsabilidad vicaria, figuras ampliamente utilizadas en materia de propiedad intelectual. Estas teorías permiten atribuir responsabilidad a quienes, sin ejecutar directamente la conducta ilícita, facilitan, inducen o se benefician económicamente de infracciones cometidas mediante sistemas tecnológicos o plataformas digitales (Ginsburg & Budiardjo, 2019).

La responsabilidad contributiva se configura cuando un sujeto tiene conocimiento de la infracción y contribuye materialmente a su realización. En el contexto de la inteligencia artificial, esta figura puede aplicarse a desarrolladores o proveedores que crean sistemas diseñados para generar contenidos que vulneren derechos de autor, siempre que exista conocimiento del uso ilícito o negligencia grave en la supervisión del sistema. Por su parte, la responsabilidad vicaria permite sancionar a quien obtiene beneficios económicos de la infracción y tiene la capacidad de controlar la conducta ilícita, aunque no participe directamente en su ejecución.

Estas teorías resultan especialmente relevantes frente al uso de inteligencia artificial, ya que permiten atribuir responsabilidad a empresas tecnológicas, plataformas digitales o proveedores de servicios que facilitan la comisión de

infracciones de propiedad intelectual mediante algoritmos automatizados. De esta manera, el modelo estadounidense prioriza la responsabilidad humana y corporativa, evitando vacíos normativos derivados de la autonomía tecnológica y garantizando la protección efectiva de los titulares de derechos (Diamantis, 2023).

A diferencia del enfoque europeo, que se basa en la regulación preventiva y la clasificación de riesgos, el sistema estadounidense privilegia la solución de controversias a través de los tribunales y el desarrollo progresivo de criterios jurisprudenciales. Este modelo permite una adaptación dinámica frente a la evolución tecnológica, aunque también genera cierta incertidumbre jurídica debido a la ausencia de una normativa específica sobre inteligencia artificial. No obstante, la combinación de responsabilidad directa e indirecta ha permitido sancionar conductas ilícitas cometidas mediante sistemas automatizados y establecer criterios para la imputación penal en contextos tecnológicos complejos (Chesterman, 2021).

### **3.3 Modelos de imputación penal en inteligencia artificial**

La utilización de sistemas de inteligencia artificial dentro de la comisión de conductas ilícitas ha introducido importantes dificultades para la atribución de responsabilidad penal, debido a que en su funcionamiento intervienen diversos actores como desarrolladores, operadores, proveedores y usuarios finales. Esta pluralidad de sujetos complejiza la determinación del responsable directo del daño, especialmente cuando el sistema actúa con cierto grado de autonomía. En este sentido, la doctrina señala que la inteligencia artificial genera zonas de incertidumbre respecto a la imputación penal, pues no resulta sencillo establecer si la responsabilidad recae en quien diseñó el sistema, en quien lo implementó o en quien lo utilizó con un fin específico. Esta situación obliga a replantear los criterios tradicionales de imputación, particularmente aquellos vinculados con la intención, el control y la previsibilidad del resultado, elementos esenciales dentro del modelo clásico de culpabilidad (Valls Prieto, 2023).

Desde la perspectiva del desarrollador, el debate se centra en determinar si puede atribuírsele responsabilidad penal por los resultados producidos por el sistema que diseñó. La dificultad radica en que, en muchos casos, el programador no actúa con dolo directo, sino que el daño deriva del comportamiento autónomo del algoritmo o de

usos no previstos inicialmente. Sin embargo, parte de la doctrina sostiene que el desarrollador podría responder penalmente cuando, conociendo los riesgos potenciales del sistema, omite incorporar medidas de seguridad o salvaguardias técnicas adecuadas. En estos supuestos, la imputación se fundamenta en la culpa o negligencia, derivada del incumplimiento del deber objetivo de cuidado en el diseño y programación del sistema. Esta posición considera que la creación de tecnologías con alto potencial de riesgo implica obligaciones reforzadas de previsión y control, cuya inobservancia puede generar responsabilidad penal (Valls Prieto, 2023).

Asimismo, el carácter colaborativo del desarrollo de sistemas de inteligencia artificial incrementa la dificultad para individualizar la responsabilidad, ya que intervienen equipos multidisciplinares, empresas tecnológicas y proveedores de datos. Esta estructura distribuida provoca que la conducta dañosa no pueda atribuirse fácilmente a un solo sujeto, lo cual evidencia la insuficiencia de los esquemas tradicionales de autoría y participación. En estos contextos, la imputación puede construirse a partir de la creación de riesgos jurídicamente desaprobados, especialmente cuando el sistema se diseña sin mecanismos de control o sin evaluar adecuadamente sus posibles usos ilícitos. De esta manera, el análisis penal debe considerar no solo la intención directa, sino también la previsibilidad del resultado y el grado de control técnico que cada interviniente mantiene sobre el sistema.

Por otra parte, la doctrina también ha puesto énfasis en la responsabilidad de los operadores o supervisores de los sistemas de inteligencia artificial. Estos sujetos tienen la función de monitorear el funcionamiento del sistema y adoptar medidas correctivas ante comportamientos anómalos. La complejidad técnica de los algoritmos no elimina sus deberes jurídicos, sino que, por el contrario, refuerza la exigencia de actuar con diligencia para prevenir daños. En este sentido, se ha sostenido que los operadores pueden ser penalmente responsables cuando omiten implementar controles, auditorías o mecanismos de supervisión humana que permitan detectar conductas ilícitas generadas por la inteligencia artificial. La falta de estos controles puede configurar una conducta negligente, especialmente cuando el sistema es utilizado en entornos sensibles como servicios financieros, redes sociales o plataformas digitales (Kirpichnikov et al., 2020; Smejkal & Kodl, 2023).

El rol del operador adquiere mayor relevancia cuando el sistema funciona de manera continua y autónoma, ya que la supervisión humana se convierte en el principal mecanismo de prevención del daño. Si el operador tiene la posibilidad de intervenir y no lo hace, podría configurarse una imputación por omisión impropia, basada en el incumplimiento del deber de garante. Esta figura permite atribuir responsabilidad a quien tenía la obligación jurídica de evitar el resultado y no adoptó las medidas necesarias para impedirlo. En este contexto, la figura del operador negligente se consolida como un elemento central dentro del análisis de responsabilidad penal en delitos cometidos mediante inteligencia artificial (Valls Prieto, 2023).

En relación con el usuario final, la imputación penal suele resultar más directa, especialmente cuando la inteligencia artificial es utilizada deliberadamente como instrumento para cometer un delito. En estos casos, el usuario actúa con dolo cuando emplea el sistema con conocimiento del resultado ilícito, como ocurre en fraudes automatizados, generación de documentos falsos o manipulación de datos informáticos. No obstante, la situación se torna compleja cuando el sistema produce resultados no previstos por el usuario o cuando actúa con autonomía significativa. En estos supuestos, surge la interrogante acerca de si el usuario mantiene el control suficiente para responder penalmente o si el resultado debe considerarse imprevisible. Esta problemática evidencia los límites del modelo tradicional de culpabilidad basado exclusivamente en la voluntad humana (Morán Espinosa, 2021).

En el contexto ecuatoriano, se ha señalado que la normativa penal vigente no regula de manera específica estos escenarios, lo que genera vacíos en la atribución de responsabilidad cuando los sistemas actúan de forma autónoma. Aunque el Código Orgánico Integral Penal contempla delitos informáticos, no establece criterios claros para los ilícitos cometidos mediante inteligencia artificial. Esta ausencia normativa dificulta la aplicación de las categorías clásicas de autoría, participación y culpabilidad, dejando sin respuesta jurídica ciertos daños generados por algoritmos. Por ello, diversos estudios proponen reformar el marco penal ecuatoriano para incorporar criterios de imputación específicos que contemplen la intervención de desarrolladores, operadores y usuarios dentro del ecosistema tecnológico (Ordóñez Córdova, 2024; Guamán Terán, 2023).

Para analizar la imputación penal en estos casos, resulta necesario examinar los elementos estructurales del delito. Tradicionalmente, el delito se configura a partir de la antijuridicidad y la culpabilidad, las cuales permiten atribuir responsabilidad e imponer una sanción. La antijuridicidad penal se compone de la acción, la tipicidad y la ausencia de causas de justificación. Dentro de estos elementos, la tipicidad cumple un rol fundamental, ya que delimita las conductas consideradas ilícitas y permite determinar si una acción constituye una lesión o puesta en peligro de un bien jurídico protegido. Este análisis se realiza principalmente a partir de elementos objetivos que describen el proceso causal, aunque también pueden incorporarse elementos normativos o subjetivos (Obregón & Gómez, 2023).

Los elementos de la conducta típica comprenden la acción y el resultado. En los delitos de resultado, es indispensable establecer un vínculo entre la conducta y el efecto producido. Este vínculo se analiza a través de la relación de causalidad, la cual tradicionalmente se ha explicado mediante la teoría de la equivalencia de las condiciones. Según esta teoría, una acción es causa del resultado cuando, al suprimirse mentalmente, el resultado desaparece. Sin embargo, este criterio resulta insuficiente para delimitar la responsabilidad penal en contextos complejos como los sistemas de inteligencia artificial, donde intervienen múltiples factores causales (Rodríguez, 2010).

Por ello, la doctrina ha desarrollado la teoría de la imputación objetiva, que incorpora un componente normativo adicional. Conforme a esta teoría, el resultado solo se atribuye al sujeto cuando su conducta crea un riesgo jurídicamente desaprobado y dicho riesgo se materializa en el resultado. Este análisis exige verificar, en primer lugar, que la acción haya generado un peligro relevante y, en segundo lugar, que el resultado constituya la concreción de ese riesgo. Este enfoque resulta especialmente útil para analizar los delitos cometidos mediante inteligencia artificial, ya que permite determinar si la programación, supervisión o uso del sistema creó un riesgo que se materializó en el daño producido (Obregón & Gómez, 2023).

Los problemas de imputación objetiva en el ámbito de la inteligencia artificial se presentan principalmente en los delitos de resultado, como los fraudes automatizados, la manipulación de mercados o los daños patrimoniales. En estos casos, la dificultad radica en identificar cuál de las conductas intervinientes generó el riesgo que produjo el resultado. Esta complejidad aumenta cuando el sistema aprende de

manera autónoma y adopta decisiones no previstas inicialmente. En tales supuestos, la atribución del resultado exige analizar el grado de control, previsibilidad y participación de cada interviniente. La doctrina ha propuesto diversos modelos para abordar esta problemática. El primero es el modelo de responsabilidad del usuario, que atribuye la responsabilidad a quien utiliza el sistema con conocimiento del resultado ilícito; el segundo, es el modelo de responsabilidad del desarrollador, aplicable cuando el daño deriva de fallas en el diseño o programación del sistema. También se ha planteado el modelo de responsabilidad compartida, que distribuye la imputación entre los distintos sujetos que intervienen en el funcionamiento de la inteligencia artificial. Finalmente, algunos autores han sugerido la posibilidad de reconocer una responsabilidad autónoma de la inteligencia artificial; sin embargo, esta postura ha sido ampliamente cuestionada, debido a que los sistemas carecen de voluntad, conciencia y culpabilidad, elementos indispensables para la responsabilidad penal.

### 3.4 Cuadro comparativo sobre normativas de tipificación de delitos derivados del uso de inteligencia artificial.

País	Dimensiones doctrinales jurídicas	Marco legal	Jurisprudencia	Aplicabilidad al contexto ecuatoriano
Estados Unidos	Predomina un enfoque mixto que combina responsabilidad civil y penal, con énfasis en la imputación a personas naturales, empresas tecnológicas y actores	Régimen normativo fragmentado compuesto por legislación federal como el <i>Computer Fraud and Abuse Act (CFAA)</i> , complementado con regulaciones estatales y	Casos relacionados con cibercrimen, accesos no autorizados, protección de datos, propiedad intelectual y responsabilidad de desarrolladores	Puede servir como modelo para delimitar la responsabilidad individual y corporativa en delitos cometidos mediante IA, así como para tipificar conductas como manipulación

País	Dimensiones doctrinales jurídicas	Marco legal	Jurisprudencia	Aplicabilidad al contexto ecuatoriano
	vinculados al desarrollo o uso de inteligencia artificial.	lineamientos administrativos.	y proveedores tecnológicos.	algorítmica, fraude automatizado o acceso ilícito a sistemas informáticos.
<b>Unión Europea</b>	Enfoque preventivo basado en el principio de precaución, la protección de derechos fundamentales y estándares éticos aplicables al desarrollo y uso de inteligencia artificial.	Reglamento General de Protección de Datos (GDPR), Directiva de derechos de autor en el mercado digital y propuestas regulatorias como el Reglamento de Inteligencia Artificial (AI Act).	Jurisprudencia incipiente del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas, tratamiento de datos y responsabilidad derivada de sistemas tecnológicos.	Puede inspirar una normativa ecuatoriana centrada en la protección de derechos fundamentales, consentimiento informado, y transparencia algorítmica, auditorías técnicas y supervisión humana de sistemas de IA.
<b>Ecuador</b>	Enfoque inicial; el derecho penal no contempla de manera expresa la criminalidad derivada del uso	Código Orgánico Integral Penal (COIP) sin disposiciones específicas sobre IA ni categorías	Jurisprudencia limitada o inexistente respecto a delitos complejos vinculados	Se evidencia la necesidad de una reforma integral que incluya tipificación específica de

País	Dimensiones doctrinales jurídicas	Marco legal	Jurisprudencia	Aplicabilidad al contexto ecuatoriano
	de inteligencia artificial ni criterios específicos de imputación.	penales adaptadas a delitos automatizados.	directamente con inteligencia artificial.	delitos con IA, delimitación de sujetos responsables (usuarios, desarrolladores y personas jurídicas) y establecimiento de estándares técnicos y éticos de control.

El análisis comparativo evidencia que los distintos ordenamientos jurídicos han adoptado enfoques diferenciados para abordar los delitos derivados del uso de la inteligencia artificial, aunque todos coinciden en la necesidad de adaptar las categorías tradicionales del derecho penal a los nuevos escenarios tecnológicos. En Estados Unidos predomina un modelo flexible basado en la atribución de responsabilidad civil y penal a personas naturales y jurídicas, especialmente cuando intervienen empresas tecnológicas o desarrolladores de sistemas automatizados. Este enfoque se apoya en la interpretación jurisprudencial y en la aplicación de normas existentes a nuevas conductas delictivas, lo que permite una respuesta rápida frente a los avances tecnológicos.

Por su parte, la Unión Europea ha desarrollado un modelo más preventivo, orientado a la gestión de riesgos y a la protección de derechos fundamentales. Este enfoque incorpora obligaciones de transparencia, control humano y supervisión técnica de los sistemas de inteligencia artificial, lo que contribuye a reducir los vacíos normativos y facilitar la atribución de responsabilidad cuando se producen daños. La

regulación europea también destaca por integrar estándares éticos y mecanismos de auditoría, fortaleciendo la seguridad jurídica en el uso de tecnologías inteligentes.

En contraste, el ordenamiento jurídico ecuatoriano aún se encuentra en una etapa incipiente. El Código Orgánico Integral Penal no contempla de manera expresa los delitos cometidos mediante inteligencia artificial, ni establece criterios específicos de imputación para los distintos actores que intervienen en el desarrollo y uso de estas tecnologías. Además, la ausencia de jurisprudencia especializada limita la interpretación judicial frente a casos complejos vinculados con sistemas automatizados. Esta situación genera inseguridad jurídica y dificulta la persecución penal de conductas ilícitas ejecutadas mediante inteligencia artificial.

En consecuencia, el estudio comparado permite concluir que Ecuador requiere una reforma normativa integral que incorpore tipificaciones específicas para delitos cometidos con inteligencia artificial, establezca reglas claras de imputación para usuarios, desarrolladores y operadores, y adopte mecanismos técnicos y éticos de control. La incorporación de estos elementos, tomando como referencia los modelos internacionales, permitiría fortalecer la protección de bienes jurídicos, mejorar la seguridad jurídica y anticipar los riesgos derivados del uso creciente de tecnologías inteligentes en los distintos ámbitos sociales y económicos.

### **3.4 Propuestas normativas para el Ecuador**

La incorporación progresiva de la inteligencia artificial en distintos ámbitos sociales ha evidenciado vacíos normativos dentro del derecho penal ecuatoriano. El marco vigente del Código Orgánico Integral Penal fue diseñado para conductas ejecutadas directamente por personas, lo que resulta insuficiente frente a escenarios donde intervienen sistemas automatizados. En este contexto, se plantean reformas orientadas a reconocer el uso de la inteligencia artificial como medio de comisión del delito y a precisar criterios de imputación penal basados en el control humano, la previsibilidad del resultado y el deber de cuidado tecnológico (Morán Espinosa, 2021).

#### **Reforma del artículo 26: dolo y dolo tecnológico - COIP**

El concepto tradicional de dolo se mantiene, pero se amplía para incluir conductas realizadas mediante sistemas automatizados. Se propone considerar que

existe dolo cuando una persona utiliza inteligencia artificial con conocimiento del riesgo y con control funcional o técnico del sistema, aun cuando el resultado se produzca de manera automatizada. Bajo esta lógica, la responsabilidad no desaparece por la intervención tecnológica, sino que se traslada al sujeto que diseña, configura o activa el sistema con previsión del resultado antijurídico. Esta ampliación permite evitar vacíos en los que el autor pretenda escudarse en la autonomía de la herramienta digital (Valls Prieto, 2023).

### **Reforma del artículo 27: culpa en el uso de sistemas automatizados - COIP**

Se plantea que la culpa también abarque la negligencia en el desarrollo, implementación o supervisión de tecnologías inteligentes. Existirá infracción del deber objetivo de cuidado cuando el sujeto, por imprudencia, impericia o inobservancia de estándares técnicos, genere un riesgo que produzca un daño. Además, se introduce la posibilidad de atribuir responsabilidad a quienes tengan deberes de supervisión o mantenimiento de sistemas automatizados y omitan medidas razonables de prevención. Con ello, se incorpora la figura del operador negligente y del desarrollador que no adopta salvaguardias técnicas adecuadas (Ormazabal Sánchez, 2024).

### **Reforma del artículo 42: autoría en delitos cometidos mediante IA - COIP**

La propuesta amplía las formas de autoría para incluir la comisión del delito mediante inteligencia artificial. Se reconoce como autor directo a quien utilice sistemas automatizados con control funcional del hecho, y como autor mediato a quien configure o programe la herramienta para la ejecución de la infracción. Asimismo, se incorpora la coautoría para quienes participen en el diseño, entrenamiento o implementación del sistema que posibilita la conducta delictiva. Esta modificación permite imputar responsabilidad a múltiples actores que intervienen en el ciclo tecnológico (Morán Espinosa, 2021).

### **Reforma del artículo 43: complicidad mediante medios tecnológicos - COIP**

Se propone incluir como cómplices a quienes faciliten la comisión del delito mediante plataformas digitales, algoritmos o inteligencia artificial. La cooperación puede consistir en proveer datos, infraestructura tecnológica o herramientas automatizadas que contribuyan al ilícito. La sanción se mantiene proporcional al grado

de participación, pero se reconoce expresamente la intervención tecnológica como forma de colaboración punible (Valls Prieto, 2023).

### **Reforma del artículo 154: intimidación mediante inteligencia artificial - COIP**

La reforma introduce la posibilidad de que la amenaza se realice a través de sistemas automatizados, bots o herramientas digitales. Se considera relevante el medio empleado, especialmente cuando el uso de tecnología aumenta la credibilidad o el alcance de la intimidación. También se prevé el agravante cuando la conducta se dirige contra servidores públicos mediante mecanismos informáticos o telemáticos (Ecuador, 2014).

### **Reforma del artículo 154.1: instigación al suicidio mediante sistemas automatizados - COIP**

Se propone tipificar expresamente la instigación al suicidio ejecutada mediante aplicaciones digitales, inteligencia artificial o sistemas automatizados. Además, se establece un agravante cuando estas herramientas sean programadas para manipular emocionalmente a la víctima. La responsabilidad recaerá en quien configure o utilice el sistema con fines de presión psicológica (UNESCO, 2022).

### **Reforma del artículo 154.2: hostigamiento con inteligencia artificial - COIP**

Se plantea reconocer como agravante el hostigamiento ejecutado mediante sistemas de IA diseñados para acosar, perseguir o intimidar. La responsabilidad penal recaerá en la persona natural o jurídica que desarrolle, active o se beneficie del funcionamiento del sistema. Esta modificación busca responder a fenómenos como el acoso automatizado o campañas coordinadas mediante bots (Organización para la Cooperación y el Desarrollo Económicos, s. f.).

### **Reforma del artículo 186: estafa con uso de inteligencia artificial – COIP**

Se propone incorporar como agravante la utilización de algoritmos, sistemas automatizados o inteligencia artificial para cometer estafa. La agravación se justifica cuando la tecnología permite aumentar el número de víctimas, dificultar la identificación del responsable o incrementar el perjuicio económico. La

responsabilidad recaería en quien configure o utilice el sistema con conocimiento del fraude (Morán Espinosa, 2021).

### **Reforma del artículo 231: transferencia electrónica de activos – COIP**

La modificación amplía el tipo penal para incluir la manipulación de sistemas de inteligencia artificial o algoritmos con el fin de obtener transferencias patrimoniales ilícitas. De esta manera, se reconoce que el fraude financiero puede ejecutarse mediante automatización y aprendizaje automático (Valls Prieto, 2023).

### **Reforma del artículo 234.1: falsificación informática mediante IA generativa – COIP**

Se propone incluir expresamente la producción de documentos, imágenes, audios o videos falsos mediante inteligencia artificial. Esta reforma permitiría sancionar fenómenos como deepfakes, contenido sintético fraudulento o manipulación digital automatizada. También se sanciona el uso posterior de dichos contenidos con intención de causar perjuicio o obtener beneficio ilegítimo (Ormazabal Sánchez, 2024).

#### **3.4.1. Referentes internacionales para las reformas propuestas**

Las propuestas se alinean con tendencias internacionales que promueven responsabilidad humana en el uso de inteligencia artificial. El Reglamento europeo de inteligencia artificial introduce obligaciones de supervisión, transparencia y control para sistemas de alto riesgo, atribuyendo responsabilidad tanto a desarrolladores como a usuarios cuando no se cumplen estándares de seguridad (Parlamento Europeo y

Consejo de la Unión Europea, 2021). De manera complementaria, la recomendación de la UNESCO sobre ética de la inteligencia artificial enfatiza la necesidad de que las empresas tecnológicas respondan legalmente cuando sus sistemas generen daños, priorizando la prevención y la protección de derechos humanos (UNESCO, 2022).

Asimismo, los principios de la OCDE destacan la trazabilidad y la rendición de cuentas durante todo el ciclo de vida del sistema inteligente, lo que facilita la identificación del responsable. Estas propuestas coinciden en que la autonomía tecnológica no debe impedir la imputación jurídica, sino que exige redefinir los criterios tradicionales de responsabilidad (Organización para la Cooperación y el Desarrollo

Económicos,

s.

f.).

### **3.4.2 Síntesis de las reformas propuestas**

El análisis evidencia la necesidad de que el Ecuador incorpore disposiciones específicas sobre inteligencia artificial dentro del derecho penal. Entre las principales medidas se destacan: reconocer el uso de inteligencia artificial como medio de comisión del delito; incorporar criterios de imputación basados en control, previsibilidad y deber de cuidado tecnológico; ampliar las formas de autoría y complicidad cuando intervienen sistemas automatizados; establecer agravantes para delitos cometidos mediante inteligencia artificial; regular la falsificación digital generada por sistemas automatizados; introducir estándares de responsabilidad para desarrolladores, operadores y usuarios; y garantizar transparencia y trazabilidad en el funcionamiento de sistemas inteligentes.

Estas reformas permitirían adaptar el marco penal ecuatoriano a los riesgos derivados del uso de inteligencia artificial, fortaleciendo la seguridad jurídica y asegurando que siempre exista un sujeto responsable frente a los daños producidos por tecnologías autónomas.

### **3.5 Reformas legales necesarias**

El examen del marco jurídico ecuatoriano en materia de propiedad intelectual y responsabilidad penal frente al uso de la inteligencia artificial evidencia una brecha importante entre la normativa vigente y las dinámicas tecnológicas actuales. Aunque el ordenamiento jurídico reconoce la propiedad intelectual como un derecho fundamental y prevé mecanismos de protección frente a infracciones tradicionales, estos instrumentos no han sido adaptados de manera suficiente para responder a las nuevas formas de vulneración derivadas del uso de sistemas automatizados.

Uno de los principales problemas se encuentra en el carácter reactivo y fragmentario de la legislación nacional. El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación fue estructurado bajo la premisa de que la creación intelectual proviene directamente de una persona humana, lo que deja fuera de su regulación las obras generadas o modificadas de forma sustancial mediante

inteligencia artificial. Esta ausencia normativa genera incertidumbre jurídica respecto a la titularidad y protección de derechos, y dificulta la defensa de los intereses patrimoniales y morales de los autores frente a prácticas tecnológicas capaces de reproducir, transformar o difundir contenidos protegidos a gran escala.

De manera similar, el Código Orgánico Integral Penal mantiene una regulación limitada en materia de delitos contra la propiedad intelectual, centrada principalmente en conductas tradicionales como la piratería o la falsificación de marcas. La falta de tipos penales específicos que contemplen el uso indebido de inteligencia artificial impide una respuesta penal eficaz ante nuevas modalidades delictivas, entre ellas la reproducción automatizada masiva de obras protegidas, la generación de contenidos falsificados mediante sistemas generativos o la manipulación algorítmica destinada a evadir medidas tecnológicas de protección.

Esta situación revela una falta de correspondencia entre el avance tecnológico y la evolución del derecho penal. El principio de legalidad exige que las conductas sancionables estén claramente tipificadas, lo que actualmente no ocurre en diversos supuestos vinculados con el uso de inteligencia artificial. Como resultado, determinadas conductas que generan daños significativos pueden quedar sin sanción penal o ser abordadas únicamente por vías administrativas o civiles que no resultan proporcionales a la magnitud del perjuicio causado.

Ante este escenario, se vuelve necesario replantear el papel del derecho penal como instrumento de protección de la propiedad intelectual en el entorno digital. Sin desconocer el principio de intervención mínima, el uso masivo y automatizado de tecnologías inteligentes incrementa el riesgo de afectaciones graves y generalizadas, lo que justifica la incorporación de respuestas penales específicas cuando otros mecanismos resultan insuficientes para prevenir o sancionar las infracciones.

En este contexto, se propone una reforma integral del marco jurídico ecuatoriano que incluya, en primer lugar, la tipificación de conductas vinculadas al uso indebido de inteligencia artificial en materia de propiedad intelectual. Entre ellas podrían contemplarse el plagio automatizado, la generación y difusión de contenido falsificado mediante sistemas de IA, la suplantación digital con fines comerciales y la elusión intencional de medidas tecnológicas de protección de obras. Estas figuras

permitirían adecuar la legislación penal a las nuevas formas de afectación de los derechos de autor.

En segundo lugar, resulta necesario establecer criterios claros de atribución de responsabilidad penal para los sujetos humanos que intervienen en el funcionamiento de sistemas de inteligencia artificial. Para ello, se deben definir los supuestos en los que desarrolladores, proveedores, propietarios o usuarios pueden ser considerados responsables, tomando en cuenta factores como el grado de control sobre la tecnología, la previsibilidad del resultado dañoso y la obtención de beneficios derivados de la conducta ilícita.

Asimismo, es fundamental armonizar la legislación penal con el régimen de propiedad intelectual, con el propósito de garantizar coherencia entre la protección sustantiva de los derechos de autor y las sanciones aplicables frente a su vulneración. Esta coordinación normativa debe considerar estándares internacionales y experiencias comparadas, adaptándolos a la realidad jurídica y social ecuatoriana.

Las reformas propuestas no buscan limitar el desarrollo tecnológico ni criminalizar el uso legítimo de la inteligencia artificial, sino establecer parámetros claros frente a su utilización abusiva. Un marco normativo actualizado permitiría fortalecer la seguridad jurídica, proteger de forma efectiva los derechos de autor y promover un uso responsable de las tecnologías inteligentes dentro del país.

En esta línea, se plantea la necesidad de modificar tanto el Código Orgánico Integral Penal como el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación. En el caso del COIP, se sugiere incorporar tipos penales específicos relacionados con la utilización de inteligencia artificial para vulnerar derechos de autor, así como introducir criterios de imputación cuando las conductas se ejecuten mediante sistemas automatizados. Por su parte, el Código Ingenios debería incluir disposiciones sobre titularidad de obras generadas con inteligencia artificial, regulación del uso de datos para el entrenamiento de modelos y responsabilidad derivada de la producción de contenido generado o derivado.

La adopción de estas reformas permitiría reducir los vacíos normativos existentes y asegurar una protección efectiva de la propiedad intelectual frente a las

nuevas modalidades de infracción vinculadas al uso de inteligencia artificial. Además, contribuiría a fortalecer la seguridad jurídica y a dotar al sistema penal ecuatoriano de herramientas adecuadas para enfrentar los desafíos tecnológicos contemporáneos.

## CONCLUSIONES Y RECOMENDACIONES

La presente investigación permitió examinar de manera integral la responsabilidad penal derivada de infracciones a la propiedad intelectual cometidas mediante el uso de inteligencia artificial en el Ecuador, a partir del análisis del marco constitucional, legal y comparado, así como de la doctrina y propuestas normativas recientes. Los resultados evidencian que el ordenamiento jurídico ecuatoriano aún no se encuentra plenamente preparado para afrontar los desafíos derivados de la creación, reproducción y difusión automatizada de contenidos en el entorno digital.

En primer lugar, se concluye que, aunque la propiedad intelectual se encuentra reconocida como un derecho constitucional y legalmente protegido, su regulación vigente responde a un modelo tradicional basado en la creación humana directa. Este enfoque resulta insuficiente frente a los escenarios actuales en los que intervienen sistemas automatizados capaces de generar, modificar o reproducir obras protegidas. La ausencia de disposiciones específicas sobre obras creadas con inteligencia artificial, uso de datos para entrenamiento y contenido derivado genera vacíos jurídicos en torno a la autoría, titularidad de derechos y mecanismos de protección efectiva.

En segundo lugar, se determina que el Código Orgánico Integral Penal mantiene una regulación limitada respecto a los delitos contra la propiedad intelectual, al no contemplar expresamente conductas ilícitas cometidas mediante inteligencia artificial. Esta omisión dificulta la aplicación del principio de legalidad penal, ya que muchas conductas altamente lesivas, como la reproducción automatizada masiva de obras, la generación de contenido falsificado mediante sistemas generativos o la manipulación

algorítmica con fines comerciales, no encajan de manera clara en los tipos penales existentes.

Asimismo, se concluye que la inteligencia artificial no puede ser considerada sujeto de responsabilidad penal directa, debido a la ausencia de voluntad, conciencia y culpabilidad. En consecuencia, la responsabilidad debe recaer en los sujetos humanos que intervienen en el ciclo tecnológico, tales como desarrolladores, proveedores, operadores o usuarios. Sin embargo, el ordenamiento jurídico ecuatoriano no establece criterios claros para determinar el grado de responsabilidad de cada uno de estos actores, lo que genera incertidumbre jurídica y posibles escenarios de impunidad.

Otro hallazgo relevante es que la imputación penal en contextos de inteligencia artificial requiere adaptar categorías tradicionales como dolo, culpa, autoría y complicidad. La intervención de sistemas automatizados dificulta la determinación del control del hecho, la previsibilidad del resultado y el deber de cuidado tecnológico, lo que evidencia la necesidad de incorporar criterios específicos de imputación basados en el control efectivo, la creación de riesgos y la participación en el diseño, programación o utilización del sistema.

El análisis del derecho comparado permitió constatar que diversas jurisdicciones han avanzado en la construcción de marcos regulatorios más adecuados frente a estos desafíos. La Unión Europea ha desarrollado un enfoque preventivo basado en la gestión de riesgos y la responsabilidad humana; Estados Unidos ha recurrido a criterios jurisprudenciales para delimitar la intervención humana significativa; y organismos internacionales han promovido principios de transparencia, trazabilidad y rendición de cuentas. Estas experiencias demuestran que es posible equilibrar la protección de la propiedad intelectual con la innovación tecnológica mediante la atribución clara de responsabilidad a los sujetos humanos involucrados.

Igualmente, se concluye que el Ecuador presenta una brecha normativa significativa en comparación con estos modelos, ya que no cuenta con disposiciones específicas que regulen la utilización de inteligencia artificial como medio de comisión de infracciones ni mecanismos claros para determinar la responsabilidad penal de quienes diseñan, controlan o utilizan estas tecnologías. Esta situación afecta la

seguridad jurídica y limita la capacidad del sistema penal para responder eficazmente a los riesgos derivados del uso indebido de sistemas inteligentes.

A partir de estas conclusiones, se recomienda, en primer lugar, reformar el Código Orgánico Integral Penal para incorporar tipos penales específicos relacionados con el uso de inteligencia artificial en la vulneración de derechos de propiedad intelectual. Estas reformas deben contemplar conductas como el plagio automatizado, la generación de contenido falsificado mediante IA, la suplantación digital con fines comerciales y la reproducción masiva no autorizada de obras protegidas.

En segundo lugar, se recomienda establecer criterios normativos de imputación penal que permitan determinar la responsabilidad de los distintos actores involucrados en el funcionamiento de la inteligencia artificial. Dichos criterios deben considerar el grado de control sobre el sistema, la previsibilidad del resultado, la creación de riesgos jurídicamente relevantes y el beneficio obtenido de la conducta ilícita.

Asimismo, se sugiere armonizar el Código Orgánico Integral Penal con el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, incorporando disposiciones sobre titularidad de obras generadas con inteligencia artificial, uso de datos para entrenamiento de modelos y responsabilidad derivada de la producción de contenido automatizado o derivado.

También se recomienda introducir agravantes específicas cuando los delitos sean cometidos mediante inteligencia artificial, especialmente en aquellos casos en los que la tecnología permita ampliar el número de víctimas, automatizar la conducta ilícita o dificultar la identificación del responsable. Esta medida permitiría reflejar la mayor peligrosidad de las conductas ejecutadas mediante sistemas automatizados.

De igual manera, resulta necesario establecer estándares de transparencia, trazabilidad y supervisión humana en el desarrollo y uso de sistemas de inteligencia artificial, con el fin de facilitar la atribución de responsabilidad penal y prevenir la comisión de infracciones. Estos estándares pueden incluir auditorías técnicas, registros de funcionamiento del sistema y mecanismos de control previo al despliegue tecnológico.

Finalmente, se recomienda promover la capacitación de operadores jurídicos, fiscales, jueces y abogados en materia de derecho digital e inteligencia artificial, así como actualizar los programas académicos en las facultades de derecho. La formación especializada permitirá una aplicación coherente de las normas y contribuirá a fortalecer la protección de la propiedad intelectual frente a los desafíos tecnológicos actuales.

### **Referencias Bibliográficas**

Asamblea Constituyente del Ecuador. (2008). *Constitución de la República del Ecuador*.

[https://www.oas.org/juridico/pdfs/mesicic4\\_ecu\\_const.pdf](https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf)

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*.

[https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP\\_act\\_feb-2021.pdf](https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf)

Asamblea Nacional del Ecuador. (2016). *Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación*.

<https://www.wipo.int/wipolex/es/text/444440>

Comisión Europea. (2021). *Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act)*.

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206>

Parlamento Europeo y Consejo de la Unión Europea. (2019). *Directiva (UE) 2019/790 sobre derechos de autor en el mercado único digital*.

<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L0790>

UNESCO. (2022). *Recomendación sobre la ética de la inteligencia artificial*.  
<https://unesdoc.unesco.org/ark:/48223/pf0000381137>

Organización para la Cooperación y el Desarrollo Económicos. (2019). *Principios de la OCDE sobre inteligencia artificial*.  
<https://oecd.ai/es/ai-principles>

U.S. Copyright Office. (2023). *Copyright and artificial intelligence*.  
<https://www.copyright.gov/ai/>

Morán Espinosa, J. (2021). *Responsabilidad penal e inteligencia artificial*.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=8037031>

Ormazabal Sánchez, G. (2024). *Responsabilidad civil por daños causados por inteligencia artificial*.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=9265412>

Valls Prieto, J. (2023). *Inteligencia artificial y responsabilidad penal*.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=8896734>

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707.  
<https://doi.org/10.1007/s11023-018-9482-5>

Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, 103(3), 513–563.  
<https://www.californialawreview.org>

Navas Navarro, S. (2019). Inteligencia artificial y responsabilidad penal. *Revista de Derecho Penal y Criminología*.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=7099465>

Guadamuz, A. (2017). Artificial intelligence and copyright. *WIPO Magazine*.  
<https://www.wipo.int>

Montañez Sierra, L. (2020). Inteligencia artificial y responsabilidad penal. <https://dialnet.unirioja.es/servlet/busqueda?q=Montañez+Sierra+inteligencia+artificial+responsabilidad+penal>

Guamán Terán, J. (2023). Delitos informáticos e inteligencia artificial en el Ecuador. <https://dialnet.unirioja.es/servlet/busqueda?q=Guamán+Terán+inteligencia+artificial+Ecuador>

Sinaluisa Sagñay, M. (2024). Delitos digitales y alfabetización tecnológica. <https://dialnet.unirioja.es/servlet/busqueda?q=Sinaluisa+Sagñay+delitos+digitales>

Organización Mundial de la Propiedad Intelectual (OMPI). (2020). *¿Qué es la propiedad intelectual?* <https://www.wipo.int>

Hallevy, G. (2015). *Liability for crimes involving artificial intelligence systems*. Springer. <https://doi.org/10.1007/978-3-319-10124-8>

Smejkal, V., & Kodl, J. (2023). Artificial intelligence and criminal liability. *Journal of Cyber Policy*, 8(2), 201–219. <https://doi.org/10.1080/23738871.2023.2186435>

Kirpichnikov, D., Savelyev, A., & Naumov, V. (2020). Criminal liability for artificial intelligence. *Russian Law Journal*, 8(1), 145–165. <https://www.russianlawjournal.org>

Del Rosal, M. (2023). Inteligencia artificial y culpabilidad penal. *Revista Electrónica de Ciencia Penal y Criminología*. <https://dialnet.unirioja.es>

Obregón García, A., & Gómez Lanz, J. (2023). *Teoría de la imputación objetiva*. Tirant lo Blanch. <https://editorial.tirant.com/es/libro/teoria-de-la-imputacion-objetiva>

Rodríguez Mourullo, G. (2010). *Derecho penal. Parte general*. Civitas. <https://www.thomsonreuters.es/es/tienda/pdp/duo-derecho-penal-parte-general.html>

Ordóñez Córdova, P. (2024). Inteligencia artificial y delitos informáticos en Ecuador. *Revista Jurídica Universidad Andina*. <https://repositorio.uasb.edu.ec>

Guamán Terán, J. (2023). Responsabilidad penal por delitos tecnológicos en Ecuador. *Revista de Derecho Digital*. <https://revistas.uide.edu.ec>

Ojeda, Y., & Robinson, J. (2025). Regulación comparada de inteligencia artificial y responsabilidad jurídica. *Revista Latinoamericana de Derecho Tecnológico*. <https://dialnet.unirioja.es>

Gobierno de España. (2021). *Carta de derechos digitales*. <https://www.lamoncloa.gob.es>

World Intellectual Property Organization. (2020). *WIPO technology trends 2020: Artificial intelligence*. [https://www.wipo.int/edocs/pubdocs/en/wipo\\_pub\\_1055.pdf](https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf)

United States Copyright Office. (2022). *Policy guidance on AI-generated works*. <https://www.copyright.gov/ai>

Calo, R. (2016). Artificial intelligence policy: A primer. *University of Washington School of Law Research Paper*. <https://papers.ssrn.com>

Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, *1*(6), 261–262. <https://doi.org/10.1038/s42256-019-0055-y>

## **Anexos**

**Jessica Alexandra Rivera Pulla** portador de la cédula de ciudadanía N° **0106574445**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación “**Análisis jurídico de la responsabilidad penal por infracciones de propiedad intelectual mediante inteligencia artificial en Ecuador**” de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **17 de abril de 2026**

F:  .....

**Jessica Alexandra Rivera Pulla**

**C.I. 0106574445**