



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS**

CARRERA DE DERECHO

TEMA:

“Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos”

AUTORES:

Kevin Augusto Chicaiza Salazar

Leonardo David Estrella Ríos

Trabajo de titulación previo a la obtención del título de
ABOGADO

TUTOR:

Ab. María Patricia Iñiguez Cevallos, Mgs.

Guayaquil, Ecuador

2026



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS**

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Kevin Augusto Chicaiza Salazar** y **Leonardo David Estrella Ríos**, como requerimiento para la obtención del título de Abogado.

TUTORA



**Maria Patricia
Iniguez Cevallos**



f.....

Ab. María Patricia Iñiguez Cevallos, Mgs.

DIRECTORA DE LA CARRERA

f.....

Dra. Nuria Pérez Puig-Mir, PHD

Guayaquil, a los 23 del mes de agosto del año 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **Kevin Augusto Chicaiza Salazar**
y **Leonardo David Estrella Ríos**

DECLARAMOS QUE:

El Trabajo de Titulación, “**Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos**” previo a la obtención del título de **Abogado**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

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

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. 
Kevin Augusto Chicaiza Salazar
C.I. Nro: 050434193-4

f. 
Leonardo David Estrella Ríos
C.I. Nro: 070454360-2



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

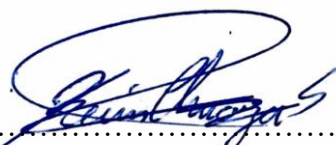
AUTORIZACIÓN

Nosotros, **Kevin Augusto Chicaiza Salazar**
y **Leonardo David Estrella Ríos**

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, **“Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos”**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. 
Kevin Augusto Chicaiza Salazar
C.I. Nro: 050434193-4

f. 
Leonardo David Estrella Ríos
C.I. Nro: 070454360-2



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

INFORME DE ANTIPLAGIO



Informe de análisis

Compilatio Magister+ | UCSG-EC- Universidad Católica de Santiago de Guayaquil

LEONARDO 3

ID : d4e89c0b02aed99e79ecf4d62dc2bba9b7e80114



5%

Textos sospechosos

Nombre del fichero : LEONARDO 3.txt
Tamaño del archivo original : 68,22 kB
Número de palabras : 7138

Depositante : Maria Patricia Iñiguez Cevallos
Fecha de depósito : 23 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 23 de agosto de 2026

Resumen (sección 1/3)

Localización de los textos sospechosos en el documento :



LOS AUTORES

f.

Kevin Augusto Chicaiza Salazar
C.I. Nro: 050434193-4

f.

Leonardo David Estrella Ríos
C.I. Nro: 070454360-2

TUTORA



Maria Patricia
Iñiguez Cevallos



f.

Ab. María Patricia Iñiguez Cevallos, Mgs.

AGRADECIMIENTO

A los pilares esenciales de mi vida, mi familia, por ser la luz constante en los días de incertidumbre y el impulso sereno en cada paso de esta travesía. Su fe inquebrantable en mis capacidades ha sido el refugio y la fortaleza que me permitieron no solo soñar, sino transformar las metas en realidad. Cada página de este trabajo lleva impresa la gratitud infinita por su amor incondicional y sus sacrificios.

A mi tutora, cuya sabiduría, generosidad académica y perspectiva crítica guiaron este proyecto con una paciencia admirable. Gracias por enseñarme a mirar más allá de lo evidente, por sus valiosos consejos en los momentos de mayor reto y por inculcar en mí la pasión por la excelencia profesional.

A la Universidad Católica de Santiago de Guayaquil, por abrirme sus puertas y convertirse en el escenario donde florecieron mis ideas, vocación e ideales. A los docentes que dejaron huella en mi formación, gracias por compartir sus conocimientos y cultivar en mí un compromiso riguroso con el saber.

Finalmente, a mis queridos amigos, quienes convirtieron los desvelos en risas y las dudas en certezas compartidas. A todas aquellas personas que, de forma silenciosa, con una palabra de aliento o un gesto amigable, sumaron fuerzas a este propósito, este logro también les pertenece.

- Kevin Augusto Chicaiza Salazar

AGRADECIMIENTO

Agradezco, en primer lugar, a Dios, por concederme la fortaleza, la sabiduría y la perseverancia necesarias para culminar esta importante etapa de mi formación profesional.

A mi madre, Gloria Ríos Bustamante, por su amor incondicional, sus enseñanzas y el apoyo que me ha brindado a lo largo de mi vida. A mi esposa, por acompañarme con paciencia, comprensión y cariño durante este proceso; y a mis hijos, por ser mi mayor inspiración y la razón que me impulsa a superarme cada día.

A todos ustedes, mi gratitud eterna.

- Leonardo David Estrella Ríos

DEDICATORIA

Dedico este trabajo de titulación, en primer lugar, a Dios, por haberme concedido la fortaleza, la sabiduría y la perseverancia necesarias para llegar hasta este momento tan importante de mi vida.

A mis padres, por ser el pilar fundamental de mi formación, por sus sacrificios, sus consejos y por enseñarme que cada meta alcanzada es el resultado de la constancia, la disciplina y la confianza en uno mismo.

A mi familia, por acompañarme en cada etapa de este camino, por creer en mí y por brindarme su apoyo incluso en aquellos momentos en los que alcanzar esta meta parecía difícil.

Finalmente, me dedico este logro a mí mismo, por haber tenido el valor de continuar, por superar cada obstáculo y por demostrarme que los sueños se alcanzan cuando existe determinación para perseguirlos. Este trabajo de titulación representa no solo la culminación de una etapa académica, sino también el resultado de años de esfuerzo, sacrificio y crecimiento personal.

Con gratitud, dedico este logro a todos quienes formaron parte de este camino.

- Kevin Augusto Chicaiza Salazar

DEDICATORIA

Dedico este trabajo a mis hijos, quienes son mi mayor motivación y la fuerza que me impulsa a alcanzar cada una de mis metas. Deseo que este logro les recuerde que, con esfuerzo, perseverancia y fe, es posible superar las dificultades y cumplir los sueños.

También lo dedico a mis estudiantes, quienes enriquecen diariamente mi vocación docente y me inspiran a continuar aprendiendo y creciendo.

Espero que este trabajo constituya para ellos un ejemplo de constancia y los anime a confiar en sus capacidades, valorar la educación y luchar por sus propios objetivos.

- Leonardo David Estrella Ríos



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS
SOCIALES Y POLÍTICAS**

CARRERA DE DERECHO



**Maria Patricia
Iniguez Cevallos**



f.....

**Ab. María Patricia Iñiguez Cevallos, Mgs.
TUTORA**

f.....

**Dra. Nuria Pérez Puig-Mir, PHD
DIRECTORA DE LA CARRERA**

f.....

**Dr. Xavier Zavala Egas
DECANO**

f.....

**Kevin Augusto Chicaiza Salazar
OPONENTE**

f.....

**Leonardo David Estrella Ríos
OPONENTE**



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia Ciencias Sociales y Políticas.

Carrera: Derecho.

Semestre: A 2026.

Fecha: 24 de agosto de 2026.

ACTA DE INFORME FINAL

La abajo firmante, docente tutora del Trabajo de Titulación denominado: **“Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos”**, elaborado por el estudiante **Kevin Augusto Chicaiza Salazar Y Leonardo David Estrella Ríos**, certifica que durante el proceso de acompañamiento dicho estudiante ha obtenido la calificación de **10/10 (Diez)**, lo cual lo califica como **APTO PARA LA SUSTENTACIÓN**.



Maria Patricia
Iniguez Cevallos



Ab. María Patricia Ñíguez Cevallos

ÍNDICE

RESUMEN.....	XII
ABSTRACT	XIII
INTRODUCCIÓN	2
CAPÍTULO I.....	4
1.1. Inteligencia artificial	4
1.2. <i>Deepfakes</i> , clonación de voz y simulación digital de identidad.....	4
1.3. Identidad digital y suplantación en entornos tecnológicos.....	5
1.4. Engaño fraudulento y afectación patrimonial	6
1.5. Legalidad, taxatividad e intervención mínima	6
1.6. Intervención humana y atribución de responsabilidad.....	7
1.7. Antecedentes investigativos y posición crítica.....	8
CAPÍTULO II	10
FUNDAMENTACIÓN JURÍDICA Y ANÁLISIS DEL PROBLEMA	10
2.1. Protección constitucional de la identidad y límites de la intervención penal.....	10
2.2. Suplantación de identidad prevista en el artículo 212 del COIP.....	10
2.3. La estafa y el uso de contenidos sintéticos como medio de engaño....	11
2.4. Relación entre suplantación de identidad y estafa.....	12
2.5. Autoría, coautoría y complicidad	13
2.6. Realidad ecuatoriana y respuesta institucional frente a los <i>deepfakes</i>	14
2.7. Regulación comparada de los contenidos sintéticos	14
2.8. Discusión de los resultados	15
2.9. Propuesta de criterios jurídico-penales para la aplicación de los artículos 186 y 212 del COIP	16
2.10. Posición jurídica de la investigación	18
CONCLUSIONES	19

RECOMENDACIONES	21
BIBLIOGRAFÍA.....	22

RESUMEN

La inteligencia artificial ha ampliado las posibilidades de generar imágenes, audios y videos capaces de reproducir con elevado realismo la identidad de una persona. Cuando estos contenidos se utilizan para inducir a error y obtener un beneficio económico, surgen dificultades para determinar la respuesta penal aplicable. La presente investigación analiza la suficiencia de los artículos 186 y 212 del Código Orgánico Integral Penal frente a la suplantación de identidad mediante inteligencia artificial con fines fraudulentos. Se empleó un enfoque cualitativo, documental y jurídico-doctrinal, apoyado en los métodos exegético, analítico-sintético y comparativo, mediante el estudio de normativa, jurisprudencia, doctrina especializada y documentos institucionales. Los resultados permiten establecer que la inteligencia artificial constituye un medio de ejecución y no modifica, por sí misma, los elementos jurídicos de la estafa o la suplantación de identidad. De igual forma, la concurrencia de ambos tipos penales debe resolverse según la unidad o pluralidad de conductas, mientras que la responsabilidad de los intervinientes exige valorar individualmente el conocimiento, la voluntad y la relevancia de cada aporte. Se concluye que el COIP presenta una suficiencia normativa condicionada, cuya aplicación requiere criterios claros sobre adecuación típica, concurso de infracciones e individualización de responsabilidades. En consecuencia, se propone una guía de criterios jurídico-penales para orientar la actuación de los operadores de justicia.

Palabras clave: inteligencia artificial, suplantación de identidad, estafa, responsabilidad penal, concurso de infracciones.

ABSTRACT

Artificial intelligence has expanded the possibilities of generating images, audio recordings, and videos capable of reproducing a person's identity with a high degree of realism. When such content is used to deceive others and obtain an economic benefit, difficulties arise in determining the applicable criminal-law response. This research analyzes the sufficiency of Articles 186 and 212 of Ecuador's Comprehensive Organic Criminal Code (COIP) regarding identity impersonation through artificial intelligence for fraudulent purposes. A qualitative, documentary, and legal-doctrinal approach was adopted, supported by exegetical, analytical-synthetic, and comparative methods through the examination of legislation, case law, specialized legal doctrine, and institutional documents. The findings indicate that artificial intelligence operates as a means of committing the offense and does not, by itself, alter the legal elements of fraud or identity impersonation. Likewise, the concurrence of both criminal offenses must be determined according to whether there is a single act or several autonomous acts, while the liability of each participant requires an individual assessment of knowledge, intent, and the relevance of the contribution made. The study concludes that the COIP provides conditional normative sufficiency, although its application requires clear criteria regarding legal classification, concurrence of offenses, and individual attribution of criminal responsibility. Accordingly, a set of legal-criminal interpretative criteria is proposed to guide justice system operators.

Keywords: artificial intelligence, identity impersonation, fraud, criminal liability, concurrence of offenses.

INTRODUCCIÓN

La inteligencia artificial ha ampliado la capacidad de crear y desarrollar textos, imágenes, audios inclusive videos con tanta precisión que cada vez se asemejan más a la realidad. (Franganillo, 2023). Una de las facultades de estos sistemas es que, por medio de ellos es posible crear nuevos contenidos, a partir de patrones ya aprendidos. Por su parte Sanfrutos (2026), manifiesta que estas capacidades pueden incorporarse a hechos delictivos en el ámbito de la ciberdelincuencia. Desde el punto de vista penal, estas afirmaciones toman relevancia, cuando se implementa estas tecnologías para clonar la voz de una persona o realizar montajes a su imagen o lo que es más perjudicial crear un video de *deepfake*, en el cual se presenta a dicha persona dando una información o actuación que jamás ha realizado.

En el contexto ecuatoriano, el problema ya no puede considerarse únicamente hipotético. En este sentido el Ministerio del Interior (2024) advierte que la utilización de inteligencia artificial para manipular voces, imágenes y videos puede convertirse en un recurso para ejecutar suplantaciones de identidad y distintas modalidades de fraude en línea. En el ámbito legislativo, existe un el Proyecto de Ley Orgánica destinado a regular el uso de simulaciones de imágenes, voces, audios y videos de personas generados mediante inteligencia artificial (Asamblea Nacional del Ecuador, 2026). Aunque, esta propuesta aún no forma parte del ordenamiento jurídico vigente, su presentación evidencia la necesidad de regular la aplicación de las nuevas tecnologías en la sociedad.

Ante este escenario, el Código Orgánico Integral Penal contempla disposiciones que pueden resultar aplicables según las particularidades de cada caso. Al enunciar el artículo 212 este regula la suplantación de identidad, cuando una persona suplanta a otra con el fin de obtener un beneficio para sí mismo o para un tercero, ocasionando un perjuicio para la persona suplantada. Por su parte, el artículo 186 tipifica la estafa cuando, con finalidad patrimonial, se induce a error a la víctima mediante la simulación, deformación u ocultamiento de hechos, provocando con ello una disposición perjudicial de carácter patrimonial (Código Orgánico Integral Penal, COIP, 2021). El punto conflictivo aparece cuando el mismo elemento sirve, para presentarse como otra persona y al mismo tiempo para construir el engaño patrimonial.

De aquí la necesidad de aplicar la jurisprudencia visualizando los límites que imponen la legalidad, la tipicidad y la taxatividad. Debido a que la Constitución del Ecuador prohíbe expresamente juzgar o sancionar conductas no tipificadas y vincula paralelamente a la seguridad jurídica con normas vigentes, claras y públicas (Constitución de la República del Ecuador, 2008, arts. 76.3 y 82). Por su parte la Corte Constitucional también ha resaltado la necesidad de una base normativa previa para atribuir responsabilidad (Corte Constitucional del Ecuador, 2023).

Por lo antes expuesto, la aparición de nuevas tecnologías digitales no habilita la posibilidad de permitir nuevos delitos por vía interpretativa ni a prescindir de los elementos que el legislador exige. Es por ello, que el objeto de estudio es la respuesta jurídico-penal ecuatoriana frente a la suplantación de identidad mediante inteligencia artificial con fines fraudulentos. El análisis de la presente investigación se centra en determinar cómo estas conductas pueden encuadrarse dentro de los artículos 186 y 212 del COIP, considerando además los mecanismos aplicables al concurso de infracciones y las distintas formas de participación penal. A partir de ello, la investigación busca responder la siguiente interrogante: **¿hasta qué punto los tipos penales actualmente previstos en el COIP permiten sancionar estas conductas sin acudir a interpretaciones extensivas que puedan vulnerar los principios de legalidad y taxatividad penal?** Al analizar la normativa vigente surgen mecanismos que permiten abordar gran parte de los casos que involucran el uso de inteligencia artificial. Pero su correcta aplicación requiere de criterios jurídicos claros y sistemáticos, que permitan una interpretación fiable conforme a los límites del Derecho penal.

El objetivo general consiste en analizar la suficiencia de dichos mecanismos y formular criterios jurídico-penales que permitan la adecuación típica, la determinación del concurso de infracciones y la individualización de las responsabilidades de un hecho delictivo. Para ello, se adopta un enfoque cualitativo, documental, jurídico y doctrinal, mismo que incorpora los métodos exegético, analítico, sintético y comparativo. En función de ello, se toma como base el análisis de la normativa vigente, la jurisprudencia y la doctrina especializada e institucional.

CAPÍTULO I

1.1. Inteligencia artificial

La inteligencia artificial permite desarrollar contenido nuevo a partir de datos, instrucciones y patrones previamente aprendidos. Sus aplicaciones abarcan textos, imágenes, audios y videos, y hoy forman parte de actividades creativas, educativas y productivas (Franganillo, 2023). Sin embargo, el origen sintético de un contenido no determina por sí mismo su ilicitud. La valoración jurídica depende del modo en que la herramienta se emplea, de los bienes jurídicos comprometidos y de la conducta que pueda atribuirse a una persona concreta.

Desde el ámbito penal, Sanfrutos Ruiz (2026) sostiene que la inteligencia artificial puede ser utilizada para facilitar, automatizar e incluso perfeccionar conductas delictivas que ya se encuentran reconocidas por el Derecho penal. En esta investigación resulta relevante precisamente ese carácter instrumental, pues mediante estas herramientas es posible reproducir rasgos propios de una persona real y generar ante terceros una apariencia convincente de autenticidad. Sin embargo, la responsabilidad penal no recae sobre la tecnología en sí misma, sino sobre la conducta de las personas que intervienen en el hecho y que, de acuerdo con las circunstancias del caso, cumplen los presupuestos jurídicos de autoría o participación.

Esta precisión resulta relevante porque una misma herramienta admite usos radicalmente distintos. Un generador de voz puede emplearse con fines de accesibilidad o producción audiovisual y, en otro escenario, servir para aparentar una llamada inexistente. Por esa razón, el análisis no parte de criminalizar la tecnología, sino de identificar qué finalidad tuvo su uso y qué intervención concreta corresponde al agente que la incorporó a la conducta examinada.

1.2. *Deepfakes*, clonación de voz y simulación digital de identidad

Los *deepfakes* son contenidos de imagen, audio o video creados o modificados mediante IA con capacidad para representar de forma convincente a personas o acontecimientos inexistentes o alterados. En el caso de la voz, la clonación puede reproducir características de timbre, ritmo y entonación para generar mensajes nuevos. Franganillo (2023) destaca que producir este tipo de material exige hoy menos barreras técnicas, mientras que Romero Moreno (2024) advierte que su expansión incrementa riesgos para la privacidad, la reputación y la confianza en las comunicaciones digitales.

En el ámbito normativo, el Parlamento Europeo y Consejo de la Unión Europea (2024) define como deepfake aquel contenido generado o manipulado mediante inteligencia artificial que puede ser percibido de manera errónea como auténtico, estableciendo además determinadas obligaciones de transparencia según el uso que se le otorgue. Esta regulación europea resulta pertinente para el análisis porque permite diferenciar entre la forma técnica en que se produce el contenido y la finalidad concreta con la que posteriormente es utilizado. Dentro de esta investigación, una voz clonada o un video sintético adquieren relevancia jurídica cuando reproducen elementos identificables de una persona real y se emplean para proyectar frente a terceros una apariencia de identidad. Por ello, la sola existencia de un contenido tecnológicamente falso no basta, por sí misma, para considerar configurados los delitos de suplantación de identidad o estafa.

En términos prácticos, estos contenidos pueden reforzar la confianza de quien recibe el mensaje. Una imagen, una voz o un video suelen funcionar como señales sociales de autenticidad y, por ello, pueden reducir las dudas de la víctima. De ahí que el análisis jurídico deba separar dos cuestiones: por un lado, la manipulación técnica del contenido; por otro, la función que esa manipulación cumple dentro del hecho atribuido.

1.3. Identidad digital y suplantación en entornos tecnológicos

La identidad digital se construye a partir del conjunto de datos y atributos que permiten reconocer a una persona en entornos tecnológicos. La identidad digital puede estar conformada de distintas formas, como nombres, perfiles, fotografías, voces, cuentas o direcciones electrónicas. De acuerdo con Martínez Galindo (2024) esta identidad no depende únicamente de un solo dato, sino que suele construirse a partir de varios rasgos, que, al estar en conjunto, permiten identificar a una persona dentro de los entornos digitales. Espinosa Carvajal y Paredes Fuentes (2025) vinculan la suplantación digital con la protección de los datos personales y la seguridad en los entornos digitales afectando directamente a la seguridad digital.

A partir de ello, resulta necesario diferenciar la suplantación de identidad de la creación de una identidad completamente ficticia. En el primer caso, se emplean datos o características pertenecientes a otra persona con el propósito de hacerse pasar por ella; en el segundo, puede no existir una persona real cuya identidad haya sido

utilizada. El desarrollo de la inteligencia artificial amplía estas posibilidades al permitir la reproducción de la voz, la imagen o incluso determinados gestos capaces de generar confianza en terceros. Pero, aun así, para que exista responsabilidad penal además del hecho de alterar una fotografía, cambiar la voz o adulterar los datos sin autorización, es indispensable comprobar que concurren los elementos exigidos por el artículo 212 del COIP.

La distinción anterior a su vez evita reducir la identidad digital a cualquier información personal. Si esa apariencia se utiliza para obtener un beneficio y ocasionar un perjuicio, la identidad deja de operar solo como información y pasa a integrar la ejecución de una conducta con posible relevancia penal.

1.4. Engaño fraudulento y afectación patrimonial

En los hechos analizados, la identidad ajena cumple una función concreta: aportar credibilidad a una solicitud o instrucción con contenido económico. Bustos Rubio (2023) explica que la digitalización cambia las formas de ejecución de la ciberestafa, pero no elimina la necesidad de demostrar la conexión entre el engaño y el perjuicio patrimonial. Por su parte, Martínez Galindo (2024) identifica los usos económicamente lesivos de la suplantación digital, las solicitudes de dinero, las operaciones con datos ajenos y las comunicaciones empresariales falsas.

Es decir, para que exista una acción jurídicamente relevante debe identificarse el hecho engañoso, el error de la víctima, el acto de disposición y sobre todo el perjuicio patrimonial. Actualmente la IA puede hacer más creíble varios de estos mecanismos, pero no reemplaza a ninguno de los elementos necesarios para configurar la estafa. A partir de esa secuencia corresponde establecer si el hecho encaja en suplantación, estafa o en una relación concursal entre ambas figuras.

1.5. Legalidad, taxatividad e intervención mínima

La legalidad exige que la conducta sancionada esté prevista con anterioridad en una norma penal; la taxatividad, a su vez, reclama una descripción suficientemente determinada. De aquí la necesidad de garantizar la implementación de nuevas tecnologías de forma segura, recalando que es necesario que el Derecho evolucione conjuntamente con el avance tecnológico. De acuerdo con Romero Moreno (2024) la regulación de los *deepfakes* establece la necesidad de contar con normas previsibles y suficientemente claras, que permitan la capacidad de diferenciar usos legítimos de la tecnología, con los que representan un riesgo para la vulneración de derechos.

Junto con ello, debe considerarse el principio de intervención mínima, conforme al cual el Derecho penal debe operar como un recurso excepcional y no como respuesta frente a cualquier forma de edición, falsedad o utilización no autorizada de información. Es decir, que la alteración de información digital por sí sola no requiere de una intervención penal, sino que previamente debe analizarse la gravedad del hecho y la posible afectación de bienes protegidos jurídicamente. De forma paralela, Martínez Galindo (2024) recuerda que la tutela penal de la identidad digital debe enmarcarse en la gravedad del comportamiento y a los bienes jurídicos afectados. Por consiguiente, antes de proponer una reforma es necesario comprobar si la legislación vigente permite resolver el caso a través de una interpretación restrictiva.

1.6. Intervención humana y atribución de responsabilidad

Un fraude apoyado en contenidos sintéticos puede distribuir tareas entre varias personas: una obtiene las muestras, otra genera el material, una tercera contacta a la víctima y alguien distinto recibe el beneficio. De acuerdo con Alé Martínez y Aguilar Campos (2025), la posible responsabilidad jurídica debe analizarse de manera prolija y diferenciada en relación al tipo de intervención o roles de los desarrolladores, programadores y usuarios. En una línea similar, Navarro-Dolmestch (2025) demarca a la inteligencia artificial como una herramienta que puede ser utilizada por una persona dentro de la ejecución de una conducta penalmente relevante, mientras que Sanfrutos Ruiz (2026) destaca los problemas probatorios que pueden presentarse en los diferentes ámbitos de la vida cotidiana cuando intervienen sistemas con mayores niveles de autonomía.

La existencia de funciones distintas dentro de un mismo hecho impide atribuir responsabilidad de manera uniforme a todas las personas involucradas. Demkin (2024), por ejemplo, diferencia entre la persona cuya identidad es representada, quienes crean o difunden el contenido sintético y los proveedores de la tecnología utilizada. Esta distinción resulta necesaria para determinar, en cada caso, cuál fue la intervención concreta de cada sujeto y qué relevancia tuvo su actuación dentro de la conducta investigada.

Para atribuir responsabilidad resulta necesario precisar qué hizo cada sujeto, qué sabía sobre la finalidad ilícita y qué relevancia tuvo su aporte en la suplantación, el engaño o la obtención del beneficio.

1.7. Antecedentes investigativos y posición crítica

La literatura internacional aborda el problema desde ángulos distintos. Franganillo (2023) estudia las capacidades generativas de estas herramientas, es decir que pueden desarrollar de forma sintética; Romero Moreno (2024) examina los *deepfakes* a partir de los derechos fundamentales; y Demkin (2024) compara modelos que combinan transparencia, actividades de plataformas y aplicación de normas ya existentes. Al analizar el potencial de estas herramientas es necesario considerar que su diversa empleabilidad; por ello, resulta necesario atender al propósito con el que fueron utilizados y a las consecuencias que producen sobre los derechos o bienes jurídicos de terceros. Esta característica de uso dual explica por qué una misma tecnología puede servir tanto para actividades legítimas como para la ejecución de conductas ilícitas.

En el ámbito ecuatoriano, buena parte de la discusión académica se ha dirigido hacia la conveniencia de fortalecer o modificar la respuesta penal frente a la suplantación digital y al empleo indebido de inteligencia artificial. Así, Endara-Chamorro et al. (2024), Recalde (2025) y Amores Medina et al. (2025) plantean, desde distintas perspectivas, posibles reformas o ajustes normativos. Frente a estas propuestas, la presente investigación parte de una posición diferente: antes de afirmar la existencia de un vacío legal, analiza de manera conjunta los artículos 186 y 212 del COIP, la eventual relación concursal entre ambos y la responsabilidad que podría corresponder a cada uno de los intervinientes.

Esta diferencia en el enfoque constituye uno de los principales aportes del trabajo. Mientras los antecedentes nacionales cuestionan, en distintos grados, si la normativa vigente ofrece una respuesta suficiente, esta investigación examina primero las posibilidades reales de aplicación de los tipos penales existentes, así como las condiciones jurídicas que deberían cumplirse para hacerlo de manera coherente. De este modo, el análisis no se limita a plantear una eventual reforma, sino que busca determinar hasta dónde puede llegar el marco penal actual sin apartarse de los principios que limitan la interpretación en materia penal. Incorporar el concurso de

infracciones y las formas de participación permite valorar no solo qué delito podría configurarse, sino también cómo evitar duplicaciones sancionatorias o atribuciones de responsabilidad que excedan la conducta efectivamente probada.

CAPÍTULO II

FUNDAMENTACIÓN JURÍDICA Y ANÁLISIS DEL PROBLEMA

2.1. Protección constitucional de la identidad y límites de la intervención penal

El marco constitucional ecuatoriano protege diversos derechos relacionados con la suplantación de identidad, entre ellos el honor y buen nombre, protección de datos personales, derecho a la protección de la intimidad e identidad, además la protección de imagen y voz de una persona (Constitución de la República del Ecuador, 2008, art. 66). La Ley Orgánica de Protección de Datos Personales (Asamblea Nacional República del Ecuador, 2021) y la Ley Orgánica de Gestión de la Identidad y Datos Civiles (Registro Oficial, 2016), de igual forma complementan esa misma protección. Sin embargo, estas normas no sustituyen el examen de tipicidad que corresponde realizar conforme al COIP.

En materia penal, el artículo 76 numeral 3 de la Constitución y el artículo 13 del COIP exigen legalidad e interpretación estricta, mientras que el artículo 82 garantiza la seguridad jurídica. La Sentencia 1364-17-EP/23 se ocupó de los límites de la extensión de un tipo penal, y la Sentencia 106-20-IN/24 abordó problemas de determinación normativa y mínima intervención (Corte Constitucional del Ecuador, 2023, 2024). La Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026) constituye un referente dentro del proceso de adaptación institucional frente a los riesgos derivados del entorno digital. Sin embargo, su incorporación al ordenamiento jurídico no altera los elementos constitutivos de los delitos analizados en esta investigación ni sustituye las exigencias de tipicidad previstas en el COIP.

En consecuencia, la vulneración de la identidad o de los datos personales no implica, por sí sola, la existencia de responsabilidad penal. El principio de mínima intervención atiende principalmente a conflictos a través de mecanismos civiles, administrativos o de protección de datos, de aquellos casos en los que concurren elementos necesarios para configurar una infracción penal. Esta distinción resulta indispensable para evitar que el Derecho penal se emplee de forma indiscriminada frente a cualquier afectación producida en entornos digitales.

2.2. Suplantación de identidad prevista en el artículo 212 del COIP

El artículo 212 del COIP sanciona a quien, de cualquier forma, suplante la identidad de otra persona para obtener un beneficio propio o de un tercero en perjuicio

de alguien, con pena de uno a tres años (COIP, 2014, art. 212). De esta disposición se identifica varios elementos que deben concurrir para que exista suplantación de identidad con relevancia penal: la acción de asumir la identidad de otra persona, la existencia de una persona real afectada, la intención de obtener un beneficio propio o para un tercero y la producción de un perjuicio. En ese sentido, el simple uso del nombre, la fotografía u otro rasgo identificable de una persona no permite concluir, de manera automática, que el delito se encuentra configurado.

La expresión “*de cualquier forma*” contenida en la norma permite entender que la suplantación no se encuentra limitada a una modalidad específica de ejecución. Por ello, una voz clonada, una imagen creada mediante inteligencia artificial o un video manipulado podrían adquirir relevancia penal cuando sean utilizados para generar en terceros la convicción de que una persona real participó en una comunicación o actuación determinada.

Un antecedente informado mediante boletín de presa por la Fiscalía General del Estado, informa sobre una sentencia condenatoria por el delito de suplantación de identidad y uso de documento falso con el fin de obtener un beneficio económico emanado por el estado, permite visualizar que la conducta prevista en el artículo 212 del COIP, puede presentarse conjuntamente con otras infracciones (Fiscalía General del Estado, 2024). Sin embargo, que la norma admita distintas formas de ejecución no implica que se dejen de lado los requisitos previstos en dicho artículo.

De esta forma la utilización de nuevas tecnologías modifica únicamente el medio empleado para cometer un delito, lo que no exime de comprobar el resto de elementos exigidos por el tipo penal. De ahí que, al aplicarlo a un deepfake exige demostrar que el contenido fue empleado para asumir la identidad de una persona sin su autorización y no solo para reproducir su imagen o su voz. También deben acreditarse la finalidad de beneficio y el perjuicio. Con esta lectura, el tipo puede abarcar medios nuevos sin convertir “*de cualquier forma*” en una cláusula ilimitada.

2.3. La estafa y el uso de contenidos sintéticos como medio de engaño

El artículo 186 del COIP sanciona a quien, con finalidad patrimonial, simula hechos falsos o deforma u oculta hechos verdaderos para inducir a error y provocar un acto perjudicial para el patrimonio propio o ajeno (COIP, 2014, art. 186). Una voz clonada, un video sintético o una imagen manipulada pueden formar parte de esa

simulación; aun así, la subsunción sigue dependiendo de la relación entre engaño, error, disposición y perjuicio (Bustos Rubio, 2023).

Como referencia nacional sobre estafa, podemos mencionar de la Sentencia 2588-21-EP/25 que muestran un caso en el que un tribunal penal consideró ejecutada la estafa después de que una representación falsa condujera a la víctima a entregar USD 3.000 dólares americanos (Corte Constitucional del Ecuador, 2025). Por esta razón, dicho antecedente se emplea únicamente como referencia de la aplicación del artículo 186 en sede penal. En un caso relacionado con *deepfakes*, sería igualmente necesario demostrar que el contenido sintético tuvo incidencia real en el error de la víctima y que, como consecuencia de ese engaño, se produjo el acto de disposición patrimonial.

El engaño debe valorarse en relación a las circunstancias concretas en las que se produjo, además considerar los factores que llevaron a la víctima a confiar en la autenticidad de la interacción realizada. En consecuencia, la capacidad persuasiva del material o contenido generado mediante inteligencia artificial permite reforzar la figura del fraude. Paralelamente es indispensable probar el error o su aplicación con la afectación patrimonial. La semejanza de una voz o una imagen generada por la IA, no configura una prueba del error, ni de la disposición patrimonial. En otras palabras, la tecnología puede fortalecer el mecanismo engañoso sin alterar la estructura jurídica básica del delito de estafa.

2.4. Relación entre suplantación de identidad y estafa

Cuando el mismo contenido sintético se utiliza para asumir una identidad y obtener una disposición patrimonial, los artículos 212 y 186 pueden entrar en relación. El artículo 20 regula el concurso real cuando existen delitos autónomos e independientes; el artículo 21, por su parte, contempla el concurso ideal cuando varios tipos son subsumibles a una misma conducta (COIP, 2014, arts. 20 y 21). Samaniego Paguay y Pozo Cabrera (2025) destacan que diferenciar unidad y pluralidad de acciones es indispensable para una aplicación correcta y para preservar la seguridad jurídica.

Una llamada única con voz clonada que suplanta a un familiar y, en ese mismo acto, induce una transferencia puede conducir al examen del concurso ideal. La situación cambia si la suplantación se desarrolla de manera autónoma y posteriormente se ejecuta una operación patrimonial independiente, supuesto en el que podría

corresponder el concurso real. Además, según las circunstancias del caso, debe verificarse si existe un concurso aparente que determine el desplazamiento de una norma. El antecedente de Píllaro confirma que la suplantación puede presentarse junto con otros tipos, aunque no resuelve específicamente su relación con la estafa (Fiscalía General del Estado, 2024).

En consecuencia, es necesario analizar ambos tipos penales, la suplantación de identidad y el perjuicio económico. Donde la suplantación conserva una entidad propia respecto del engaño patrimonial, de esta forma verificar si se desarrolla antes o después de la disposición económica y cuál es su función dentro de la conducta ejecutada. Al desarrollar este análisis se establece una mejor precisión entre la relación de las infracciones cometidas; evitando una doble sanción por un mismo hecho.

2.5. Autoría, coautoría y complicidad

Los artículos 41, 42 y 43 del COIP regulan autoría y complicidad y permiten individualizar la responsabilidad cuando participan varias personas (COIP, 2014, arts. 41-43). En un fraude con contenido audiovisual manipulado mediante inteligencia artificial, la calificación depende del aporte probado por quienes ejecutan directamente el engaño, mismo que pueden responder como autor o autores; es decir quien realiza un aporte principal puede ser analizado desde la coautoría; y quien presta una colaboración dolosa secundaria, desde la complicidad.

Alé Martínez y Aguilar Campos (2025) advierten que diseñadores, programadores y usuarios ocupan posiciones distintas, lo que obliga a descartar cualquier forma de responsabilidad objetiva. Navarro-Dolmestch (2025) estudia la inteligencia artificial como instrumento que puede ser usado por una persona y no como un sujeto que comete un delito directamente, por su parte Sanfrutos Ruiz (2026) resalta que la conducta ilícita adoptada por una persona debe ser vinculada probatoriamente a cada interviniente. Ni la sola generación técnica del contenido ni la recepción del dinero bastan para presumir participación sin conocimiento y voluntad.

Cuando responsabilidades de las acciones delictivas se distribuyen entre varias personas, la prueba adquiere un papel fundamental para determinar la responsabilidad de cada interviniente. Elementos como los registros de instrucciones, resguardo de información, archivos de edición, transferencias bancarias pueden contribuir a establecer quién conocía la finalidad fraudulenta y cuál fue su participación concreta en cada uno de los hechos.

Desde esta perspectiva, la titularidad de una cuenta utilizada para recibir dinero o el acceso a una herramienta de inteligencia artificial no constituyen por sí solos, elementos suficientes para atribuir responsabilidad a todos los involucrados.

2.6. Realidad ecuatoriana y respuesta institucional frente a los *deepfakes*

De acuerdo con el Ministerio del Interior en la actualidad, el uso de *deepfakes* incrementa el riesgo de fraude digital en el cual se manipulan imágenes, audios o videos y advierte que los mecanismos tradicionales de validación han perdido eficacia. (Ministerio del Interior, 2024). Esta afirmación muestra que el avance de la inteligencia artificial incrementa notablemente el riesgo de cometer este tipo de delitos, y al mismo tiempo complica la investigación de los hechos y las personas involucradas, aunque no reemplaza los elementos jurídicos de la estafa o la suplantación.

Desde el ámbito normativo institucional, existe un proyecto de ley que involucra la regulación de simulaciones de imágenes, voces, audios y videos generados por inteligencia artificial (Asamblea Nacional del Ecuador, 2026), así como la Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Ambos antecedentes reflejan un proceso de adaptación frente al entorno digital. Con todo, aún no se identifica un criterio jurisprudencial consolidado que resuelva, en un caso de IA con finalidad patrimonial, la interacción entre los artículos 186 y 212 y la participación de varios sujetos; esa carencia explica la utilidad de formular criterios interpretativos.

En este contexto, una propuesta interpretativa resulta de gran utilidad para orientar la aplicación del Derecho penal, mientras se desarrolla jurisprudencia específica sobre estos supuestos.

Para que proceda la intervención penal, debe comprobarse el cumplimiento de los elementos previstos en los artículos 186 o 212 del COIP, así como la intervención concreta del sujeto investigado. En consecuencia, las fuentes institucionales permiten demostrar la actualidad y relevancia del riesgo, pero no sustituyen la valoración de la prueba ni el análisis de adecuación típica que corresponde efectuar en cada caso.

2.7. Regulación comparada de los contenidos sintéticos

El derecho comparado se emplea aquí como criterio de contraste y no como mecanismo para trasladar automáticamente soluciones extranjeras. Demkin (2024) identifica modelos que permiten combinar identificación de contenidos y aplicación de figuras delictivas tradicionales. De forma paralela, la Unión Europea, en su

Reglamento (UE) 2024/1689 opta principalmente por obligaciones de transparencia en el desarrollo y transmisión de contenidos sintéticos. De igual forma vincula la responsabilidad penal nacional cuando estos se utilizan para cometer infracciones. De acuerdo con Romero Moreno (2024) sostiene que la regulación de los *deepfakes* debe garantizar el derecho a la protección de la privacidad y uso de la información, de forma equilibrada con la libertad de expresión.

Desde la realidad ecuatoriana, el análisis comparado permite precisar que las acciones jurídicas no siempre tienen el mismo efecto, es así que el etiquetado de contenidos y las obligaciones de transparencia tienen un carácter preventivo, por su parte la intervención del Derecho penal exige que se configuren todos los elementos propios de una infracción.

De esta forma, la experiencia comparada permite adquirir una mejor visión antes de incorporar un nuevo tipo penal, permitiendo valorar primero si las normas vigentes pueden ofrecer una respuesta adecuada frente a estas conductas.

2.8. Discusión de los resultados

Los resultados respaldan parcialmente la premisa de investigación. La fórmula “*de cualquier forma*” del artículo 212 puede comprender una voz clonada, una imagen sintética o un video deepfake cuando estos se utilizan para asumir la identidad de una persona real y se acreditan el beneficio y el perjuicio. De manera paralela, el artículo 186 puede operar cuando el contenido sintético forma parte de una simulación que induce a error y provoca una disposición patrimonial perjudicial. En ambos escenarios, la IA funciona como medio de ejecución y no sustituye los elementos del tipo.

La dificultad más significativa aparece cuando esas dos estructuras coinciden. La doctrina ecuatoriana reciente ha defendido reformas o tipos específicos para la suplantación digital (Amores Medina et al., 2025; Endara-Chamorro et al., 2024; Recalde, 2025), pero el análisis realizado no permite afirmar que exista una ausencia absoluta de tipificación. La respuesta concursal debe construirse a partir de la unidad o pluralidad de conductas, cuestión que Samaniego Paguay y Pozo Cabrera (2025) identifican como sensible para la seguridad jurídica.

Un segundo resultado se relaciona con la atribución de responsabilidad. El empleo de IA no convierte automáticamente en responsables a todos quienes participaron técnicamente. Los aportes de Alé Martínez y Aguilar Campos (2025), Navarro-Dolmestch (2025) y Sanfrutos Ruiz (2026) permiten sostener que la

imputación debe individualizarse según el dolo, el conocimiento y la relevancia del aporte. A partir de lo expuesto, puede sostenerse que la respuesta del COIP presenta una suficiencia condicionada. Esto significa que el ordenamiento penal vigente dispone de tipos que pueden aplicarse frente a estas conductas, pero su utilización requiere criterios precisos para determinar la adecuación típica, la posible relación concursal entre infracciones y el grado de participación de cada interviniente.

Comparar el ámbito doctrinario con la normativa vigente ha permitido optar por posiciones jurídicamente fundamentadas y coherentes con el marco normativo. No sería adecuado afirmar que el COIP carece por completo de herramientas para responder a la suplantación de identidad mediante inteligencia artificial, pero tampoco puede desconocerse que estas tecnologías introducen nuevas dificultades en la aplicación práctica del Derecho penal. Cuando en un mismo hecho coinciden la utilización de una identidad sintética, un engaño de carácter patrimonial y la intervención de varias personas con funciones distintas, la decisión jurídica exige una motivación especialmente rigurosa para evitar interpretaciones incompatibles o atribuciones de responsabilidad que excedan lo realmente probado.

Precisamente frente a estas dificultades se plantea la propuesta interpretativa de la investigación. Su finalidad no es establecer una respuesta única para todos los casos, sino proporcionar una secuencia de análisis que permita examinar cada situación de acuerdo con sus particularidades. Para ello, deberá determinarse si existe una persona real cuya identidad fue suplantada, si el contenido sintético generó una apariencia efectiva de autenticidad, si se produjo un engaño con consecuencias patrimoniales, cuál fue la actuación concreta de cada participante y qué tipo de relación existe entre las infracciones que podrían configurarse.

2.9. Propuesta de criterios jurídico-penales para la aplicación de los artículos 186 y 212 del COIP

A partir de los resultados se propone una guía de criterios interpretativos para fiscales, jueces, defensores y demás operadores de justicia. Su propósito es ordenar el examen de casos en los que contenidos generados o manipulados mediante IA se utilicen para suplantar a una persona con finalidad fraudulenta. La propuesta formulada no pretende crear una nueva figura delictiva ni alterar los elementos que actualmente integran los tipos penales analizados. Su finalidad consiste en orientar la aplicación de los artículos 186 y 212 del COIP mediante criterios ordenados,

restrictivos y compatibles con los principios de legalidad y taxatividad que rigen en materia penal.

Primero. Verificación de la existencia de una persona real. Debe identificarse con precisión a la persona cuya identidad habría sido utilizada o asumida. La creación de un personaje completamente ficticio no permite, por sí sola, considerar cumplido este elemento del artículo 212 del COIP.

Segundo. Comprobación de una apariencia efectiva de identidad. Es necesario establecer que el contenido generado o manipulado fue empleado para hacer creer a terceros que la persona real participó en una comunicación, impartió una instrucción o realizó el acto que se le atribuye.

Tercero. Determinación de la finalidad de beneficio y del perjuicio. Para la aplicación del artículo 212 debe demostrarse que la conducta estuvo dirigida a obtener un beneficio propio o para un tercero y que, además, produjo el perjuicio exigido por la norma.

Cuarto. Verificación independiente de los elementos de la estafa. La aplicación del artículo 186 requiere comprobar de manera específica la existencia de una simulación, deformación u ocultamiento relevante, el error de la víctima, el acto de disposición patrimonial perjudicial y la relación causal entre estos elementos. La sola falsedad o manipulación del contenido no permite presumir que el delito de estafa se encuentra configurado.

Quinto. Individualización de la participación de cada interviniente. Debe determinarse qué actuación concreta desarrolló cada persona dentro del hecho, identificando, entre otros aspectos, quién lo planificó, quién obtuvo la información necesaria, quién generó o utilizó el contenido sintético y quién recibió el eventual beneficio. Esta valoración debe considerar el conocimiento, la voluntad y la importancia real del aporte efectuado.

Sexto. Análisis de la relación concursal. Cuando una misma conducta reúna los elementos de los artículos 186 y 212, deberá examinarse la posible existencia de un concurso ideal. Si, por el contrario, se presentan hechos autónomos e independientes, corresponderá valorar el concurso real. Asimismo, según las particularidades del caso, deberá considerarse la eventual existencia de un concurso aparente de normas.

Séptimo. Interpretación restrictiva y exigencia probatoria. La expresión “*de cualquier forma*” contenida en el artículo 212 permite que el tipo penal abarque nuevas modalidades tecnológicas de ejecución; sin embargo, ello no autoriza a prescindir de

los demás elementos exigidos por la norma ni a presumir la intención, el conocimiento, el beneficio o el perjuicio sin respaldo probatorio suficiente.

La aplicación de los criterios sigue un orden lógico: primero se verifica la suplantación; luego se examinan el engaño y la afectación patrimonial; después se individualiza la intervención de cada sujeto; y, finalmente, se resuelve la relación concursal. Con ello se evita que la novedad tecnológica desplace el análisis jurídico que exige cada caso.

2.10. Posición jurídica de la investigación

El análisis permite sostener que los artículos 186 y 212 del COIP ofrecen una base normativa para sancionar una parte relevante de las conductas de suplantación mediante IA con finalidad fraudulenta. El artículo 212 no se encuentra limitado a una tecnología concreta y el artículo 186 tampoco restringe el medio empleado para construir la simulación. En consecuencia, la IA puede operar como instrumento de ejecución cuando los hechos cumplen los elementos exigidos por cada tipo.

Esa suficiencia, sin embargo, no es absoluta. Persisten dificultades para resolver el concurso y para individualizar responsabilidades cuando intervienen varias personas, a lo que se suma la ausencia de jurisprudencia consolidada sobre *deepfakes* vinculados simultáneamente con los artículos 186 y 212.

La evolución de los casos concretos será determinante para identificar si las herramientas jurídicas actuales ofrecen una respuesta suficiente o si se requiere de una intervención normativa adicional.

Por ello, la posibilidad de una futura reforma legislativa no queda descartada, pero debería responder asertivamente a problemas que puedan demostrarse en la práctica. Si con el desarrollo de casos concretos se evidencia conductas graves que no pueden ser abordadas mediante los tipos penales existentes, o que persisten criterios contradictorios en su aplicación, podría justificarse una modificación específica del COIP. Es así que mientras no exista evidencia suficiente de esa insuficiencia, la alternativa más eficiente de acuerdo con los principios de legalidad e intervención mínima consiste en aplicar las disposiciones actualmente vigentes mediante criterios uniformes y restrictivos.

CONCLUSIONES

1. El análisis realizado permite concluir que la inteligencia artificial generativa, por sí misma, no modifica la estructura jurídica de los delitos estudiados. Herramientas como los *deepfakes*, las imágenes sintéticas o la clonación de voz pueden incrementar la apariencia de autenticidad de un contenido falso, pero su relevancia penal depende de la conducta desplegada por las personas involucradas y del cumplimiento de los elementos que exige cada tipo penal.

2. La expresión “*de cualquier forma*”, enunciada en el artículo 212 del COIP, permite considerar modalidades de suplantación desarrolladas con inteligencia artificial, siempre que pueda atribuirse a una persona real cuya identidad haya sido asumida, y se produzca el perjuicio requerido por la norma.

3. Respecto del artículo 186 del COIP, este puede ser aplicable cuando el contenido generado o manipulado mediante inteligencia artificial forme parte de un mecanismo de engaño capaz de inducir a error a la víctima y provocar una disposición patrimonial perjudicial. Para ello, deben comprobarse de forma independiente la finalidad patrimonial, el error, el acto de disposición, el perjuicio ocasionado y la relación existente entre estos elementos.

4. La posible concurrencia de los artículos 186 y 212 no puede resolverse de manera automática, debido a que depende de las circunstancias particulares desarrolladas. Cuando un mismo hecho reúna los elementos de ambos tipos penales, deberá analizarse la posible existencia de un concurso ideal; en cambio, si se presentan conductas autónomas e independientes, podría configurarse un concurso real. De esta forma evitar la doble sanción y la absorción indebida de una afectación autónoma a la identidad.

5. La atribución de responsabilidad penal exige determinar de manera individual la participación en los hechos delictivos. Como el hecho del conocimiento de la finalidad ilícita, la voluntad de participar y la importancia del aporte realizado constituyen aspectos esenciales para establecer el grado de responsabilidad. Con ello, evitar interpretaciones incorrectas de la ley que perjudique a desarrolladores, personas que desarrollaron el contenido, quienes mantuvieron contacto con la víctima o quienes recibieron el beneficio económico sin contar con prueba suficiente sobre su intervención concreta.

6. En relación a la presente investigación se puede concluir que el COIP presenta una suficiencia normativa condicionada frente a la suplantación de identidad

mediante inteligencia artificial con fines fraudulentos. Los tipos penales vigentes contienen herramientas relevantes, aunque su aplicación requiere de criterios claros sobre adecuación típica, concurso de infracciones y formas de participación.

RECOMENDACIONES

1. Promover espacios de formación y actualización dirigidos a fiscales, jueces, defensores públicos y demás operadores de justicia, con el propósito de fortalecer la correcta diferenciación entre la suplantación de identidad y la estafa cuando intervienen contenidos generados o manipulados mediante inteligencia artificial. Este análisis debería partir de la verificación de los elementos propios de cada tipo penal y, posteriormente, examinar la posible relación concursal entre ambos.

2. La expresión “*de cualquier forma*” contenida en el artículo 212 del COIP debe ser aplicada de manera restrictiva. Es decir, debe comprobarse la existencia de una persona real suplantada, la finalidad de obtener un beneficio económico y el perjuicio correspondiente.

3. Si se considera aplicar una reforma legislativa, es necesario realizar un seguimiento permanente de las decisiones fiscales y judiciales relacionadas con la suplantación de identidad digital, la estafa cometida mediante inteligencia artificial y el concurso de infracciones. Esta revisión hará posible la identificación de posibles diferencias de criterio en la práctica, y paralelamente valorar, con base en la evidencia concreta y en concordancia con las exigencias de la interacción social.

4. En el debate legislativo, es necesario separar las medidas preventivas de transparencia, aquellas que involucren respuestas penales. De esta forma una eventual reforma del COIP debería ser tecnológicamente neutral, contemplando los usos legítimos de la tecnología, y principalmente evitar tipificar conductas ya cubiertas por los artículos 186 y 212.

BIBLIOGRAFÍA

- Alé Martínez, V. I., & Aguilar Campos, P. (2025). Responsabilidad penal en la era de la inteligencia artificial: De la agencia humana a la autonomía de la machina sapiens. *Revista de Estudios de la Justicia Facultad de Derecho Facultad de Derecho*, 153-183. doi:<https://doi.org/10.5354/0718-4735.2025.77061>
- Amores Medina, G. E., Larrea Del Pozo, R. J., & Alvarado Alija, L. A. (2025). La suplantación de identidad mediante la inteligencia artificial y su adecuación en el COIP. *Revista de Investigación en Ciencias Jurídicas, LEX*. doi:<https://doi.org/10.33996/revistalex.v9i31.434>
- Asamblea Nacional del Ecuador. (2026). *Proyecto de Ley Orgánica que regula el uso de las simulaciones de imágenes, voces, audio y video de personas generadas por inteligencia artificial*. Obtenido de <https://www.asambleanacional.gob.ec/es/node/115325>
- Asamblea Nacional República del Ecuador. (2014). www.asambleanacional.gob.ec. Obtenido de <https://www.asambleanacional.gob.ec/sites/default/files/coip.pdf>
- Asamblea Nacional República del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Quito · Ecuador. Obtenido de <https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos>
- Asamblea Nacional República del Ecuador. (2026). Registro Oficial del día: Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Obtenido de <https://www.lexis.com.ec/noticias/registro-oficial-del-dia-ley-organica-para-el-fortalecimiento-de-la-ciberseguridad>
- Bustos Rubio, M. (2023). La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal. (D. y. Revista de Internet, Ed.) *Universidad Internacional de La Rioja*(1-11). doi:<https://doi.org/10.7238/idp.v0i38.413222>
- Código Orgánico Integral Penal, COIP. (2021). *República del Ecuador Asamblea Nacional*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Constitución de la República del Ecuador. (2008). Quito: Lexis. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

- Constitución de la República del Ecuador. (2008). *Registro Oficial Órgano de la República del Ecuador*. Obtenido de <https://www.registroficial.gob.ec/245427-2/>
- Corte Constitucional del Ecuador. (2023). *SENTENCIA 1364-17-EP/23*. Corte Constitucional del Ecuador, Quito, Ecuador. Obtenido de https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcNBLdGE6J3RyYW1pdGUnLCB1dWlkOic2NDhjN2U1OS03ZWVhLTQ5MzEtYTliZC1jMDllYTE0MjFiYWUucGRmJ30=
- Corte Constitucional del Ecuador. (2024). *Sentencia 106-20-IN/24*. 106-20-IN/24, Quito. Obtenido de https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiIxOTIhNjMxMy0yYzZkLTQ3OTctOTM0My1mYTg0OGQxNGRkYzcucGRmIn0=
- Corte Constitucional del Ecuador. (2025). *Sentencia 2588-21-EP/25*. CASO 2588-21-EP. Obtenido de https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiIzMmIwMTZmNy1jMWY3LTQ1NzEtYmJlZC01MmM5NDhhYTljMzkucGRmIn0=
- Demkin, V. O. (2024). Deepfakes: en busca de un modelo de regulación legal. *Legal Issues in the Digital Age*, 73–91. doi:<https://doi.org/10.17323/2713-2749.2024.4.73.91>
- Endara-Chamorro, R. E., Espinoza-Jiménez, J. S., López-Fuel, E. R., & Santander-Moreno, J. J. (2024). Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador. *Dialnet*, 240-250. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=9545770>
- Espinosa Carvajal, G. G., & Paredes Fuentes, F. E. (2025). Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano. *Revista de Investigación en Ciencias Jurídicas, LEX*, 559–572. doi:<https://doi.org/10.33996/revistalex.v9i28.302>
- Fiscalía General del Estado. (2024). *Sentenciada a 5 años por suplantación de identidad*. BOLETÍN DE PRENSA FGE N° 385-DC-2024. Obtenido de <https://www.fiscalia.gob.ec/sentenciada-a-5-anos-por-suplantacion-de-identidad/>

- Franganillo, J. (2023). La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos. *methaodos.Revista De Ciencias Sociales*(Vol. 11 Núm. 2). doi:<https://orcid.org/0000-0003-4128-6546>
- Martínez Galindo, G. (2024). *Suplantación de identidad digital: hacia una necesaria tutela penal*. España: Universidad Internacional de La Rioja (UNIR). doi:<https://doi.org/10.18543/ed.3105>
- Ministerio del Interior. (2024). Deepfakes y fraude digital: la nueva era de las estafas en línea. *Legal Issues in the Digital Age*, 73-91. doi:<https://doi.org/10.17323/2713-2749.2024.4.73.91>
- Navarro-Dolmestch, R. (2025). Inteligencia artificial como «actuante» en el derecho penal. Una primera aproximación. *IDP. Revista de Internet, Derecho y Política*, 1-16. doi:<https://doi.org/10.7238/idp.v0i43.432787>
- Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. *Diario Oficial de la Unión Europea*. Obtenido de <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Recalde, D. (2025). Análisis crítico jurídico sobre la Suplantación de identidad por medios electrónicos como un tipo penal independiente en el Código Orgánico Integral Penal. *Instituto Superior Tecnológico Universitario Corporativo Edwards*. Obtenido de <https://www.centroseditorial.com/index.php/revista/article/view/374>
- Registro Oficial. (2016). *Ley Orgánica de Gestión de la Identidad y Datos Civiles. Registro Oficial Segundo Suplemento 684*. Obtenido de <https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/155-ley-identidad-datos-civiles/TD-ley-datos-civiles-28-01-2016.pdf>
- Romero Moreno, F. (2024). Inteligencia artificial generativa y deepfakes: un enfoque de derechos humanos para abordar el contenido dañino. *Revista Internacional de Derecho, Informática y Tecnología* , 297-326. doi:<https://doi.org/10.1080/13600869.2024.2324540>
- Samaniego Paguay, A. P., & Pozo Cabrera, E. E. (2025). Concurrence of offenses and connection in the COIP: An essential distinction for proper interpretation and application in the ecuadorian judicial system. *Resistances. Journal of the Philosophy of History*. doi:<https://doi.org/10.46652/resistances.v6i11.182>

Sanfrutos Ruiz, C. (2026). Ciberdelitos e inteligencia artificial. Desafíos en el ámbito jurídico-penal. *Cuadernos De RES PUBLICA En Derecho Y criminología*, 1-28. doi:<https://doi.org/10.46661/respublica.13548>



**Presidencia
de la República
del Ecuador**



**Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes**



SENESCYT
Secretaría Nacional de Educación Superior,
Ciencia, Tecnología e Innovación

DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **KEVIN AUGUSTO CHICAIZA SALAZAR** con C.I **050434193-4** y **LEONARDO DAVID ESTRELLA RÍOS** con **070454360-2** respectivamente, autores del trabajo de titulación: **Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos**, previo a la obtención del título de Abogado en la Universidad Católica de Santiago de Guayaquil:

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

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

Guayaquil, 23 del mes de agosto del año 2026.

f. 
Kevin Augusto Chicaiza Salazar
C.I. Nro: 050434193-4

f. 
Leonardo David Estrella Ríos
C.I. Nro: 070454360-2



**Presidencia
de la República
del Ecuador**



**Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes**



SENESCYT
Secretaría Nacional de Educación Superior,
Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Suficiencia del COIP ante la suplantación de identidad mediante inteligencia artificial con fines fraudulentos		
AUTOR (ES)	Kevin Augusto Chicaiza Salazar Leonardo David Estrella Ríos		
REVISOR(ES)/TUTOR(ES)	Ab. María Patricia Iñiguez Cevallos, Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TÍTULO OBTENIDO:	Abogado		
FECHA DE PUBLICACIÓN:	23 de agosto de año 2026	No. DE PÁGINAS:	25
ÁREAS TEMÁTICAS:	Derecho Penal		
PALABRAS CLAVES/ KEYWORDS:	Inteligencia artificial, suplantación de identidad, estafa, responsabilidad penal, concurso de infracciones.		
RESUMEN/ABSTRACT: La inteligencia artificial ha ampliado las posibilidades de generar imágenes, audios y videos capaces de reproducir con elevado realismo la identidad de una persona. Cuando estos contenidos se utilizan para inducir a error y obtener un beneficio económico, surgen dificultades para determinar la respuesta penal aplicable. La presente investigación analiza la suficiencia de los artículos 186 y 212 del Código Orgánico Integral Penal frente a la suplantación de identidad mediante inteligencia artificial con fines fraudulentos. Se empleó un enfoque cualitativo, documental y jurídico-doctrinal, apoyado en los métodos exegético, analítico-sintético y comparativo, mediante el estudio de normativa, jurisprudencia, doctrina especializada y documentos institucionales. Los resultados permiten establecer que la inteligencia artificial constituye un medio de ejecución y no modifica, por sí misma, los elementos jurídicos de la estafa o la suplantación de identidad. De igual forma, la concurrencia de ambos tipos penales debe resolverse según la unidad o pluralidad de conductas, mientras que la responsabilidad de los intervinientes exige valorar individualmente el conocimiento, la voluntad y la relevancia de cada aporte. Se concluye que el COIP presenta una suficiencia normativa condicionada, cuya aplicación requiere criterios claros sobre adecuación típica, concurso de infracciones e individualización de responsabilidades. En consecuencia, se propone una guía de criterios jurídico-penales para orientar la actuación de los operadores de justicia.			
ADJUNTO PDF:	SI	NO	
CONTACTO CON AUTOR/ES:	Teléfono: 097 939 0497 098 580 3803	E-mail: leosscounter@gmail.com kevin99chicaiza@gmail.com	
CONTACTO CON LA INSTITUCIÓN	Nombre: Ab. Ángela Paredes Cavero, Mgtr. Teléfono: +593-99 760 4781		
	E-mail: angela.paredes01@cu.ucsg.edu.ec		

