



UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD CIENCIAS POLÍTICAS Y ADMINISTRATIVAS
CARRERA DE DERECHO

La suplantación de identidad mediante inteligencia artificial y la
insuficiencia del marco jurídico Penal

**Trabajo de Titulación para optar al título de Abogada de los
Tribunales y Juzgados de la República de Ecuador**

Autores:

García Mosquera, Leslie Estefanía
Gavilanes Viteri, Joselyn Jemima

Tutor:

Mgs. Wendy Pilar Romero Noboa

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Nosotras, **Leslie Estefanía García Mosquera**, con cédula de ciudadanía 1804511762, y **Joselyn Jemima Gavilanes Viteri** con cedula de ciudadanía 1206032805, autoras del trabajo de investigación titulado: **La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

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

En Riobamba, 13 de abril de 2026.



Leslie Estefanía García Mosquera

C.I: 1804511762



Joselyn Jemima Gavilanes Viteri

C.I: 1206032805

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Wendy Pilar Romero Noboa catedrático adscrito a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal, bajo la autoría de Leslie Estefanía García Mosquera, y Joselyn Jemima Gavilanes Viteri; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 13 del mes de abril de 2026



Mgs. Wendy Pilar Romero Noboa

C.I: 0604453589

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

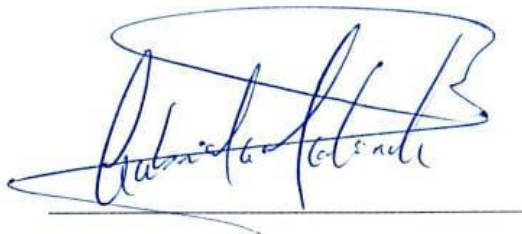
Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal, presentado por **Leslie Estefanía García Mosquera**, con cédula de ciudadanía 1804511762, y, **Joselyn Jemima Gavilanes Viteri** con cedula de ciudadanía 1206032805, bajo la tutoría de Mgs. Wendy Romero; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 13 de julio de 2026.

Dr. Bécquer Carvajal Flor
PRESIDENTE DEL TRIBUNAL DE GRADO



Mgs. Gabriela Yosua Medina Garces
MIEMBRO DEL TRIBUNAL DE GRADO



Dr. Juan Gonzalo Montero Chávez
MIEMBRO DEL TRIBUNAL DE GRADO





Dirección
Académica
VICERRECTORADO ACADÉMICO



UNACH-RGF-01-04-08.17
VERSIÓN 01: 06-09-2021

CERTIFICACIÓN

Que, **GARCÍA MOSQUERA LESLIE ESTEFANIA** con CC: **1804511762** y **GAVILANES VITERI JOSELYN JEMIMA** con CC: **1206032805** estudiantes de la Carrera de **DERECHO**, Facultad de **CIENCIAS POLÍTICAS Y ADMINISTRATIVAS**; han trabajado bajo mi tutoría el trabajo de investigación titulado **"La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal"**, cumple con el 3% de plagio y 3% de IA, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentajes aceptados de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 12 de junio de 2026

Mgs. Wendy Pilar Romero Noboa
TUTOR(A)

DEDICATORIA

A **Dios**, fuente de luz y fortaleza, por sostenerme en el silencio de las dudas,
guiar mis pasos con paciencia infinita y concederme la fe necesaria
para transformar el esfuerzo en logro y el camino en propósito.

A quienes fueron el primer refugio y la lección más constante de entrega,
maestros silenciosos de mis valores y convicciones, sostén firme en cada caída y luz
paciente en cada duda; a quienes me enseñaron que la justicia comienza en casa
y que el amor también es una forma de responsabilidad; mis padres, **Gloria y Carlos**.

A las compañeras de vida que caminaron a mi lado desde el inicio, testigos de mis aciertos
y errores, presencia leal en los días de calma y en las horas difíciles,
hogar compartido y fuerza incondicional;
mis hermanas, **Ingrid, Sofía y Vanessa**.

A la memoria viva de la experiencia, manos que guardan historias y palabras que aún
orientan, sabiduría heredada que trasciende el tiempo
permanece como abrigo y guía constante;
mi abuelita y mis tíos, **Diocelina, Margarita, Margoth y Jorge**.

A quienes eligieron quedarse, convirtiendo la amistad en familia,
aportando risas, apoyo sincero y complicidad en el largo camino de la formación
académica y personal;
mis amigos, **Melanie, Marcos, Favio, y Pricila**

A la amistad que se volvió compañera de camino y de propósito,
por las horas compartidas entre ideas, desvelos y aprendizajes,
por la confianza mutua, la paciencia y el apoyo constante;
porque este trabajo no solo se construyó con esfuerzo académico,
sino también con lealtad, respeto y complicidad, a mi amiga tesista **Joselyn**

Y, finalmente,
a cada persona que, de manera visible o silenciosa,
formó parte de este proceso,
dejando una huella en estas páginas
y un espacio permanente en mi corazón.

Leslie Estefanía García Mosquera

DEDICATORIA

Dedico esta tesis primeramente al creador tierra, el universo y todo lo que habita en ella, a quien me escogió desde el vientre de mi madre y ha hecho innumerables promesas, aquel que me acompañó en las noches más frías y desoladas, a quien demostró su amor en mí. Esta tesis es para mí **DIOS, YAHWEH.**

A mis padres **Elba y Geovanny** quienes fueron un puntal fundamental en mi crecimiento, gracias a su crianza soporte cada dificultad en mi camino sin rendirme, por su apoyo incondicional en este proceso y sobre todo por inculcarme la fe que me sostuvo en mis peores momentos.

A mis hermanas **Anahi y Nayely** quienes con su carisma encendían una chispa de convicción en mí, motivo por el cual me mantuve firme en esta brecha y con orgullo me he convertido en su ejemplo a seguir.

A **Tita y Milo** mis queridas mascotas, quienes estuvieron en cada noche de desvelo, en medio de tareas y cuadernos, códigos y lecturas de sentencias, ellos que con sus ojitos abiertos me daban el ánimo para seguir.

A mi prima **Fahiru**, mi compañera de cuarto, mi paño de lágrimas y mi amiga fiel, quien me ha acompañado todo este periodo universitario, en donde aprendimos juntas que todo lo que pasa en nuestras vidas es parte de crecer.

A la persona que ha dado su esfuerzo y dedicación en este trabajo, aportando con sus ideas y mediando situaciones complejas, aquella que se ha convertido en una amiga que sin importar las circunstancias sé que siempre permanecerá fiel a su esencia. Mi amiga tesista **Leslie García.**

A todos aquellos **familiares, amigos y hermanos en Cristo** que oraron por mí, hoy puedo decir que, sin sus oraciones, yo no estaría aquí.

Finalmente, a la promesa que nos dejó nuestro Señor, la cual estuvo conmigo desde el inicio de mis estudios hasta culminar mi carrera y fielmente la llevo en mi corazón.

“Mira que te mando que te esfuerces y seas valiente; no temas ni desmayes, porque Jehová tu Dios estará contigo en dondequiera que vayas.” Josué 1:9

Joselyn Jemima Gavilanes Viteri

AGRADECIMIENTO

Agradecemos la **Universidad Nacional de Chimborazo** por el respaldo institucional y la formación académica brindada a lo largo de nuestra carrera, la cual permitió consolidar conocimientos jurídicos, fortalecer el pensamiento crítico y desarrollar un compromiso ético con el Derecho y la justicia. Asimismo, expresamos nuestra gratitud a sus autoridades y docentes, con una mención especial a nuestra tutora y mentora la Mgsc. Wendy Romero, cuyo acompañamiento académico y humano contribuyó de manera significativa a nuestro proceso de aprendizaje y crecimiento profesional.

Leslie Estefanía García Mosquera
Joselyn Jemima Gavilanes Viteri

ÍNDICE GENERAL

DECLARATORIA DE AUTORÍA

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

CERTIFICADO ANTIPLAGIO

DEDICATORIA

DEDICATORIA

AGRADECIMIENTO

ÍNDICE GENERAL

ÍNDICE DE TABLAS

RESUMEN

ABSTRACT 14

CAPÍTULO I. 15

2. INTRODUCCIÓN..... 15

2.1 Planteamiento del problema 16

2.2 Justificación..... 17

2.3 Objetivos..... 19

Objetivo General..... 19

Objetivos Específicos 19

CAPÍTULO II..... 20

3. MARCO TEÓRICO 20

3.1 Estado del arte..... 20

3.2 Aspecto teórico 22

3.2.1 UNIDAD I: SUPLANTACIÓN DE IDENTIDAD..... 22

3.2.2 UNIDAD II: MARCO NORMATIVO Y ANÁLISIS DEL DERECHO PENAL
ECUATORIANO 28

3.2.3	UNIDAD III: Impacto Social Generado por el Insuficiente Marco Normativo Penal	38
-------	---	----

CAPÍTULO III. 43

4. METODOLOGÍA..... 43

4.1	Unidad de análisis.....	43
4.2	Métodos.....	43
4.3	Enfoque de investigación.....	44
4.4	Tipo de investigación	44
4.5	Diseño de investigación.....	45
4.6	Población y muestra.....	45
4.7	Técnicas e instrumentos de investigación	46
4.8	Técnicas para el tratamiento de información	46

CAPÍTULO IV. 47

5. RESULTADOS Y DISCUSIÓN 47

5.1	Resultados	47
	Resultados de la entrevista por expertos.....	47
5.1.1	Resultados pregunta 1	47
5.1.2	Respuesta pregunta 2.....	48
5.1.3	Respuesta pregunta 3.....	49
5.1.4	Respuesta pregunta 4.....	50
5.1.5	Respuesta pregunta 5.....	50
5.1.6	Respuesta pregunta 6.....	52
5.1.7	Respuesta pregunta 7.....	53
5.2	Análisis y discusión de resultados	53
5.2.1	Percepción y conocimiento del deepfake como mecanismo de suplantación de identidad.	54
5.2.2	Insuficiencia del marco jurídico ecuatoriano frente la suplantación de identidad mediante inteligencia artificial	55
5.2.3	Determinación de la responsabilidad penal en delitos cometidos mediante deepfake.....	56

5.2.4	Limitaciones frente a los delitos cometidos mediante inteligencia artificial	57
5.2.5	Responsabilidad del Estado y necesidad de fortalecimiento del marco jurídico	58
CAPÍTULO V.....		59
6.	CONCLUSIONES Y RECOMENDACIONES	59
6.1	Conclusiones	59
6.2	Recomendaciones	60
BIBLIOGRAFÍA		61
ANEXOS		65

ÍNDICE DE TABLAS

Tabla 1 48

Tabla 2 49

Tabla 3 49

Tabla 4 50

Tabla 5 51

Tabla 6 52

Tabla 7 53

RESUMEN

La presente investigación “La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal”, estudia la rápida evolución tecnológica y el desarrollo del ciberespacio como fuente de nuevas formas y un nuevo espacio delictivo. La finalidad de esta investigación es el estudio de la suplantación de identidad con IA desde una perspectiva jurídica, penal, para demostrar las anomalías en la normativa y la necesidad de la elevación de la identidad digital a bien jurídico protegido susceptible de tutela estricta. La metodología utilizada es cualitativa, de tipo inductivo y jurídico-analítico, mediante el análisis documental, bibliográfico, normas nacionales e internacionales y doctrina. Los estudios realizados revelan que la legislación penal ecuatoriana es insuficiente, evidencia la existencia de retos probatorios y anomalías permitiendo que estos delitos queden en impunidad. Se concluye que la legislación penal actual muestra la ausencia de una regulación jurídica específica, es inminente que el avance tecnológico ha generado un vacío normativo legal.

Palabras claves: suplantación de identidad, inteligencia artificial, insuficiencia, marco normativo, deepfake.

ABSTRACT

This study, titled “Identity Theft via Artificial Intelligence and the Inadequacy of the Criminal Legal Framework,” examines rapid technological advancements and the evolution of cyberspace as a source of new forms of crime and a new criminal arena. The purpose of this research is to examine AI-related identity theft from legal and criminal perspectives, to highlight gaps in the law, and to demonstrate the need to elevate digital identity to the status of a legally protected right deserving of strict safeguards. The methodology employed is qualitative, inductive, and legal-analytical, involving the analysis of documents, literature, national and international regulations, and legal doctrine. Studies have shown that Ecuador’s criminal law is inadequate, highlighting evidentiary challenges and legal loopholes that allow these crimes to go unpunished. It is concluded that current criminal law lacks specific regulations and that technological advances have created a legal vacuum.

Keywords: identity theft, artificial intelligence, insufficiency, regulatory framework, deepfake.



Reviewed by:

Mgs. Jessica María Guaranga Lema

ENGLISH PROFESSOR

C.C. 0606012607

CAPÍTULO I.

2. INTRODUCCIÓN.

La presente investigación estudia el tema la suplantación de identidad mediante inteligencia artificial denominada la insuficiencia del marco jurídico penal, una problemática que surge a partir de la era digital y, se posiciona como delito en distintos lugares del mundo como La Union Europea y Estados Unidos, los cuales han desarrollado propuestas de ley para combatir esta creciente amenaza digital, por esta razón la ausencia de regulación específica sancionatoria en el Ecuador ante el evidente incremento tecnológico para el cometimiento de delitos,

La problemática de la investigación refiere a como la Inteligencia artificial actúa como limitante para proteger el bien jurídico, debido a que, la IA es capaz de crear rostros y voces para imitar a otras personas sin poder identificar su autenticidad. En el Estado ecuatoriano este tipo de prácticas, se han inmiscuido en redes sociales y medios digitales lo que causa una alerta en los ciudadanos y una desconfianza en el sistema judicial por la ausencia de normativa sancionatoria en caso de una vulneración de derechos contra la intimidad de las personas, por esta razón, es ineludible analizar el marco jurídico ecuatoriano para evidenciar las anomalías normativas.

El uso de las herramientas digitales ha transformado una sociedad y un cambio de era, y junto con el desarrollo de la sociedad el derecho cambia, para garantizar la protección de derechos dentro de un mundo cibernético donde las personas son vulnerables a todo tipo de ataques dejándolos en estado de indefensión, por lo cual el objetivo de esta investigación es analizar como la suplantación de identidad mediante inteligencia artificial es creciente en la sociedad, es así que se evidencia la insuficiencia del marco jurídico Penal en el Ecuador.

En cuanto a la metodología, se basa en un enfoque cualitativo y descriptivo con la ayuda de revisión documental, doctrina, legislaciones nacionales e internacionales y artículos sobre la inteligencia artificial, el deepfake, y el derecho digital. El interés de la investigación busca adecuar el marco jurídico a las nuevas necesidades de la sociedad ecuatoriana, para promover la efectividad del sistema jurídico dentro del territorio y evitar la vulneración del derecho a la identidad, a la intimidad, al honor, buen nombre y la seguridad jurídica.

La siguiente tesis contiene cinco capítulos: el primero encierra la introducción al tema de investigación junto con el problema planteado, el segundo desarrolla el marco teórico en referencia a la insuficiencia de la norma y los paradigmas establecidos; el tercer capítulo contiene el esquema metodológico, los instrumentos y herramientas utilizadas; el cuarto capítulo análisis de resultados de la investigación y el capítulo 5 conclusiones y recomendaciones conseguidas en la investigación. Además, se estructura de la siguiente manera; portada; introducción; planteamiento del problema; objetivos: general y específicos; estado del arte, marco teórico; metodología; presupuesto y cronograma del trabajo investigativo; referencias bibliográficas; anexos; y, visto bueno del tutor.

2.1 Planteamiento del problema

La constante evolución de la inteligencia artificial ha dado paso a que varias aplicaciones o herramientas sean fuente para crear imágenes, audios y videos hiperrealistas, hoy por hoy llamados deepfakes, donde, se modifican voces y rostros con una precisión real, casi imposible de distinguir su veracidad. Estos avances han dado lugar al uso indebido de tales herramientas, lo que facilita las prácticas ilícitas como la suplantación de identidad.

Los términos conocidos como “deepfake” y “Phishing” causan confusión en el argot jurídico, por lo cual es menester diferenciarlos. Autores como Ben Gebremeskel (2025) mencionan que el Phishing, se basa en el uso y envío de correos electrónicos genéricos con múltiples errores o virus y enlaces no seguros o sospechosos para ingresar a la información personal de las personas, por otro lado, el deepfake es la creación de imágenes, videos y audios para imitar la apariencia y voz de las personas y así suplantar su identidad, lo que asegura evitar la seguridad biométrica.

En el Ecuador este tipo de prácticas, se han presentado en diferentes ámbitos como redes sociales, campañas políticas y medios digitales. La falta de una normativa específica que regule el uso y sanción de estas conductas ocasionan un estado de indefensión para las víctimas. Una de las principales causas de este problema es la ausencia de normativa legal que sancione la suplantación de identidad con IA o denominado deepfake, si bien existe una normativa que protege los datos personales como lo es la Ley Orgánica de Protección de Datos Personales (2021), esta ley establece solo una sanción administrativa que regula el tratamiento de datos personales, pero no regula la aplicación de nuevas tecnologías e IA.

En la actualidad en el Ecuador el uso de la inteligencia artificial para el cometimiento de delitos ha incrementado lo cual genera alarma en la población, debido a que todos los ciudadanos son víctimas de estos lamentables sucesos. La utilización del deepfake es clave para que las personas suplanten la identidad de otra y por medio de esto ocasionen delitos como la estafa o la suplantación de identidad, por esta situación ciertas instituciones han tomado medidas para que la población conozca de este tipo de delitos y tenga el cuidado necesario con la información proporcionada hacia entidades públicas, privadas o redes sociales.

La suplantación de identidad mediante inteligencia artificial, como los deepfakes, al no estar tipificada genera un problema jurídico, porque al no existir una sanción penal, las autoridades competentes proporcionarán respuestas que dejan estos actos en impunidad. Existen desafíos aun mas grandes junto con este acto al no esclarecer la autoría, la intención y el daño real causado, por lo cual es necesario que prevalezca la protección de la identidad y la dignidad humana, solo así, se previene la vulneración de los derechos fundamentales garantizados en la Constitución.

El problema para investigar surge a partir del avance tecnológico y la nueva era digital creciente en el mundo, que ha llegado a arraigarse en distintos países y Ecuador no es la excepción, por ello muchas personas con analfabetismo tecnológico son más vulnerables a este tipo de ataques. Frente a este escenario, resulta indispensable analizar los nuevos tipos penales identificados por los avances tecnológicos y con esta necesidad generar conciencia para que se fortalezcan los sistemas jurídicos.

Según la agenda 2030 para el desarrollo sostenible establecida en la Asamblea General de Naciones Unidas, esta investigación sobre la suplantación de identidad mediante inteligencia artificial se vincula principalmente con el ODS 16, al promover un enfoque de justicia y fortalecimiento institucional frente a nuevas vulneraciones de derechos. También, se relaciona con el ODS 9, al analizar el impacto de la innovación tecnológica y la necesidad de una regulación responsable de la IA. De manera complementaria, aporta al ODS 10, al advertir que una normativa desproporcionada profundiza desigualdades. Así, la investigación contribuye a un desarrollo tecnológico orientado a la dignidad humana y la justicia social.

En concreto, esta investigación busca analizar el sistema penal y sus normas adyacentes, para procurar evidenciar cómo la normativa penal ecuatoriana no sanciona el uso e implementación de nuevas tecnologías como lo son la inteligencia artificial, para la comisión de ciberdelitos entre ellos el deepfake. Explicada la problemática la pregunta de investigación es la siguiente ¿La inteligencia artificial puede ser un limitante en la protección de los bienes jurídicos protegidos por el Estado?

2.2 Justificación

La presente investigación, se fundamenta en el enfoque sociológico y crítico del derecho con un paradigma basado en el realismo-jurídico y post-positivismo, debido a que busca comprender el avance tecnológico, como lo es la inteligencia artificial y la digitalización que transforma al sistema jurídico tradicional en un campo completamente desconocido. Desde una perspectiva epistemología y hermenéutica entendemos que el derecho es dinámico, porque debe adaptarse a los nuevos contextos de la sociedad, y garantizar una protección efectiva de los derechos en los nuevos entornos digitales.

El autor Miró Linares sostiene que el cibercrimen no tiene una modalidad de criminalidad específica, el delincuente tiene una gama de variedad criminal en el ciberespacio, semejante a la delincuencia tradicional en el espacio físico, sin embargo, la criminalidad en el área tangible se encuentra regulada y sancionada mientras que en el área digital carece de regulación.

Los paradigmas de este estudio demuestran que la suplantación de identidad mediante deepfake se integran a la sociedad, lo que transforma, manipula y convierte la información digital encontrada en el ciberespacio para afectar bienes jurídicos como lo son la honra y la seguridad jurídica de las personas, se insta a una transformación del derecho penal tradicional a un derecho adaptativo y dinámico.

Este estudio pretende visibilizar los vacíos legales existentes que impiden sancionar las conductas delictivas en el ciberespacio o ámbito digital y con esto demostrar la necesidad de la creación de una normativa específica que regule los ciberdelitos en especial la suplantación de la identidad por medios tecnológicos, garantizan una seguridad jurídica digital, y se fortalece la política criminal frente a las nuevas amenazas crecientes por el uso de las tecnologías. Los resultados de esta investigación son útiles para el conocimiento de estudiantes, abogados, jueces, fiscales y legisladores en el reconocimiento de nuevas formas de tipos penales vinculadas a la inteligencia artificial y a la criminalidad en espacios digitales

intangibles. Así mismo, procura promover la colaboración institucional en el ámbito penal y tecnológico, se busca sensibilizar a las autoridades y a la sociedad sobre la importancia de la alfabetización y seguridad digitales, para prevenir este tipo de delitos.

La investigación, se lleva bajo un enfoque cualitativo y descriptivo, de tipo crítico interpretativo, este enfoque permite ir un paso más allá de un estudio normativo formal, incorporado múltiples ámbitos como el social y el tecnológico. También, se utiliza métodos de análisis documental, doctrinal, para poner en evidencia la falta de normativa para los ciberdelitos (deepfakes) en el Ecuador. Es menester poner en evidencia con esta investigación el déficit del sistema jurídico con relación a la innovación tecnológica frente al uso indebido de la inteligencia artificial, y con esta necesidad el sistema judicial fortalece la norma y genera confianza en el entorno digital para los ciudadanos. Es importante mencionar que esta investigación beneficiara a las posibles víctimas, pero también a la sociedad en general.

2.3 Objetivos

Objetivo General

Analizar la incidencia de la inteligencia artificial en el tipo penal de suplantación de identidad y determinar de qué manera esta tecnología genera insuficiencia del marco normativo penal ecuatoriano a través de la interpretación de la norma y el análisis crítico doctrinario para visibilizar el vacío legal vigente frente a los nuevos desafíos tecnológicos.

Objetivos Específicos

- Identificar los conceptos básicos y técnicos del deepfake y el uso de las herramientas digitales con fines delictivos para comprobar su conexión con la suplantación de identidad.
- Examinar el marco jurídico normativo ecuatoriano actual relacionado con el delito de suplantación de identidad para identificar las anomalías existentes en cuanto al uso de inteligencia artificial - deepfake.
- Determinar el impacto social ocasionado por la necesidad de tipificar el uso de la IA - deepfake, dentro del Derecho Penal ecuatoriano, con el fin de evidenciar el vacío legal existente.

CAPÍTULO II.

3. MARCO TEÓRICO

3.1 Estado del arte

Taco y Sánchez publicaron en 2025 el artículo científico Delitos de contenido íntimo generado mediante inteligencia artificial: análisis de la necesidad de una regulación especial en Ecuador. En este trabajo se analizan los riesgos legales que surgen al crear y difundir contenidos íntimos falsos mediante el uso de deepfakes. En su análisis realizan un estudio doctrinal y comparado: revisan leyes de otros países y la normativa ecuatoriana, además llegan a la conclusión, de que los delitos de contenido íntimo no consentido hechos con inteligencia artificial no están tipificados. Según ellos, esta ausencia deja desprotegidos derechos tan importantes como la honra y la intimidad, porque las normas actuales del COIP no consideran la manipulación tecnológica como parte del delito. Por eso proponen crear un tipo penal específico que castigue tanto la producción como la difusión de deepfakes íntimos, y además incluir medidas procesales rápidas para sacar ese contenido de circulación y reparar de forma integral el daño a las víctimas.

Este artículo alude en el marco teórico la falta de tipificación penal para contenido fraudulento generado con inteligencia artificial. También demuestra que la manipulación tecnológica o contenido generado con IA no está contemplada en los tipos penales del COIP, lo que refuerza el argumento de que el marco jurídico actual no es suficiente. Este trabajo exhibe propuestas concretas de un delito específico y medidas urgentes que dan un respaldo muy sólido a la idea de insuficiencia del marco jurídico, que se plantea.

Carlos Fredi Jumbo, en su artículo La suplantación de identidad digital en el COIP: análisis de aplicación y obstáculos (2025), engloba la eficiencia de la normativa penal cuando hay suplantación de identidad digital. Realizó un estudio documental y comparativo entre el derecho ecuatoriano y el de otros países de la región, y encontró que el COIP no tiene reglas claras para regular la manipulación de imágenes, voces o videos creados con inteligencia artificial. Se vuelve complejo la identificación de los responsables en esta clase de actos. Es claro que persiste ausencia de procedimientos técnicos para conservar y autenticar pruebas digitales durante el proceso penal. Fredi concluye que es necesario incorporar parámetros de autenticación tecnológica y capacitar mejor a los operadores de justicia en delitos informáticos para que la ley se aplique correctamente.

El porte de Jumbo muestra en detalle las complicaciones reales que tiene el COIP para lidiar con la suplantación de identidad digital, menciona una normativa relevante donde la idea de capacitar a los entes de justicia en delitos informáticos encaja perfecto con las recomendaciones institucionales que se aplicara en el presente trabajo.

Geovanny Sinaluisa Sagñay en 2024 presentó su tesis Deepfakes, dificultades probatorias y su incidencia en la vulneración al derecho de intimidad. La idea principal era observar cómo la creación de contenidos falsos a través de IA afecta el derecho a la intimidad y qué problemas probatorios generan dentro de los procesos penales ecuatorianos. Es así que, con un enfoque cualitativo, revisó doctrina, jurisprudencia y artículos del Código Orgánico Integral Penal, y concluyó que la legislación penal no tiene una tipificación

específica para sancionar la creación o difusión de material deepfake. También dejó claro que hay serias carencias técnicas a la hora de valorar pruebas digitales, por lo que, se hace énfasis en la falta de peritos especializados en inteligencia artificial. Según sus conclusiones, estos vacíos normativos y técnicos impiden proteger realmente a las víctimas, por lo que recomienda reformas legales y fortalecer la pericia digital en el sistema judicial.

Este trabajo aporta al marco teórico un análisis bastante profundo sobre el impacto de los deepfakes en derechos fundamentales y confirma la ausencia de regulación específica. Refuerza la justificación de mi investigación al mostrar cómo los contenidos falsos afectan derechos básicos, y su parte sobre las dificultades probatorias es muy útil para explicar los problemas procesales que existen, como la falta de peritos especializados, que también produce complicaciones en los casos de suplantación de identidad digital.

Nelly Lizeth Arévalo Fernández en el 2024 publicó su tesis “La omisión del delito de deepfake en el código orgánico integral Penal en Ecuador”. En esta investigación se da prevalece el cuestionamiento de si el marco jurídico actual protege la identidad en casos de suplantación de identidad digital. Su investigación es de enfoque cualitativo en donde se realizó entrevistas a juristas y un análisis comparativo con legislaciones de países latinoamericanos, sus hallazgos muestran que el COIP tiene figuras dispersas relacionadas con la suplantación, pero ninguna que mencione expresamente el uso de inteligencia artificial o deepfakes, permitiendo la omisión de muchas conductas delictivas sin castigo. En su conclusión, la investigadora alude que es urgente la reforma del COIP para incluir como tipo penal la suplantación de identidad digital con inteligencia artificial además menciona que se debe crear mecanismos procesales que garanticen la persecución y la reparación rápida para las víctimas.

La importancia de esta investigación en nuestro trabajo se encuentra en la problemática puesto que busca resolver si la ley protege lo suficiente los derechos fundamentales en delitos cometidos con inteligencia artificial. Los resultados de este trabajo fundamentan la necesidad de reformar el COIP ante la falta de un tipo penal autónomo responda bien a los delitos con inteligencia artificial.

Cristopher Stalyn Aleman publicó en 2024 el artículo La inteligencia artificial, un nuevo desafío para el Derecho Penal ecuatoriano. Este artículo examina las herramientas de IA en donde se configura los delitos al nuevo dinamismo tecnológico. El enfoque cualitativo utilizado es descriptivo y teórico, porque analiza casos que aparecieron en medios nacionales y revisa la doctrina Penal ecuatoriana. A su vez, en sus resultados indica que el uso de IA aumenta la suplantación de identidad en un espacio digital porque crea anomias en el tratamiento penal. Concluye que el sistema penal ecuatoriano necesita modernizarse e incorporar elementos tecnológicos que determinen para que reconozcan la responsabilidad penal digital.

Este artículo provee una base para desarrollar el capítulo III de nuestra investigación, debido a que combina distintos métodos y técnicas para obtener resultados favorables. En los resultados obtenidos se demuestra que existe riesgo en el uso de la IA y se considera que es insuficiente el marco jurídico actual.

3.2 Aspecto teórico

3.2.1 UNIDAD I: SUPLANTACIÓN DE IDENTIDAD

3.2.1.1 Conceptos referenciales

3.2.1.1.1 Suplantación

Este vocablo también conocido como robo de identidad, se ha convertido en una variante moderna de los delitos tradicionales, incorporándose como una acción penalmente relevante enmarcada en el ámbito tecnológico dentro del contexto actual.

El término suplantar se define como “Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba” (Real Academia Española, 2025). Por su parte, la palabra “suplantación se considera un delito, pues se trata de alguien que finge ser quien no es para poder conseguir algún beneficio” (González, 2015, s/p).

En otras palabras, este tipo penal es constituido como una conducta dolosa usada deliberadamente para causar engaño, debido a, que se utiliza ilegítimamente el lugar de una persona con el fin de obtener un lucro o causar un perjuicio. En este sentido, dicha práctica asume relevancia jurídica, puesto que con este hecho se vulnera la identidad de la persona y sus derechos fundamentales.

3.2.1.1.2 Identidad

El término identidad es una forma de comprender como las personas se perciben así mismas y como se reconocen dentro de un determinado contexto histórico. Maldonado ha conceptualizado este término con la finalidad de describir el yo dentro de la sociedad humana, por lo que en su obra: Los bárbaros jurídicos: Identidad, derecho comparado moderno y el Sur global, establece la identidad como:

El “yo” quisiera siempre tener control sobre quien es, sobre su historia, sobre cómo se conectan los hechos que se presentan como entrelazados con su cuerpo. Quisiera, además que la historia que cuenta sobre sí mismo coincidiera con la historia que los otros cuentan sobre quien es. Quisiera persuadir al otro de que ella es quien dice ser (Maldonado, 2020, s/p).

Para Maldonado podemos decir que la identidad es la existencia de un individuo, el cual no existe sin la validación de otro, el individuo es identificado por otro a causa de su ser y su esencia.

“La Identidad es la construcción de sentido, atendiendo a uno o varios atributos culturales, priorizándolos del resto de atributos, que se construye por el individuo y representa su autodefinición” (Noriega y Medina, 2012, p. 273). Esta permite al individuo construir su sentido y personalidad, le permite comprender quien es y en quien se convertirá según las decisiones que este tome durante toda su vida.

“La "identidad" entraña una lucha simultánea contra la disolución y la fragmentación; una intención de devorar y, al mismo tiempo, una resuelta negativa a ser comido” (Bauman, 2005, p. 164). Contrario a este comentario Castells menciona que “Las identidades son fuentes de sentido para los propios actores y por ellos mismos son

construidas mediante un proceso de individualización” (Castells, 2001, p. 29). Al fragmentar las identidades nos aseguramos de no ser consumidos por la sociedad, porque la identidad es el sentido de individualización, si la sociedad nos consume entonces perdemos nuestra esencia.

La identidad es la fuente de sentido y experiencia para la gente. Como escribe Calhoun:

No conocemos gente sin nombre, ni lenguas o culturas en las que no se establezcan de alguna manera distinciones entre yo y el otro, nosotros y ellos. [...] El conocimiento de uno mismo —siempre una construcción pese a que se considere un descubrimiento— nunca es completamente separable de las exigencias de ser conocido por los otros de modos específicos (Calhoun, 1994, citado en Castells, 2001, p. 28).

El término mencionado, es un derecho innato del ser humano es el propio ser, su autodefinición, su característica y personalidad, el simple hecho de arrebatarlo para otros fines lo convierte en la pérdida de la existencia de uno mismo, sin identidad perdemos lo que somos, lo que fuimos y lo que seremos dentro de una sociedad donde la identidad es lo único que nos hace humanos.

Los autores mencionados anteriormente manifiestan la importancia de la identidad, es por esta razón que se encuentra tipificada en la constitución como un derecho fundamental, es un bien jurídico protegido que garantiza el Estado su cumplimiento. Si la suplantación de identidad vulnera la identidad entonces se transgrede un derecho fundamental que el Estado debe proteger.

3.2.1.1.3 Suplantación de identidad

Comprendidos los términos suplantación e identidad de forma individual, es necesario abordarlos de manera conjunta. La interrelación de estos términos nos permite entender esta conducta típica sobre la usurpación de identidad, que se convierte en un delito según lo estipulado en el artículo 212 del Código Orgánico Integral Penal (COIP). La suplantación de identidad se convierte en una afección a la persona, vulnera significativamente sus derechos en su esfera personal, tales como la honra, la intimidad y privacidad.

Según Martínez la suplantación de identidad se caracteriza por la apropiación de la identidad de una persona, haciéndose pasar por ella y se lleva a cabo a través de la pérdida, robo o fotocopiado del DNI. También lo hacen con datos personales que obtienen de distintos lugares. En forma virtual se usan las técnicas de la ingeniería social o la introducción de software malicioso en la computadora de la víctima (citado en Anónimo, 2018).

Martínez manifiesta que la identidad no es solo un documento físico, en la actualidad la identidad evoluciona y profundiza su concepto en base a las nuevas tecnologías que regularizan los nuevos hechos delictivos.

La suplantación de identidad, también conocida como robo de identidad, se define como el acto de usurpar la identidad de otra persona con el fin de cometer fraude, robo o cualquier otra actividad delictiva. Por ende, esta práctica se lleva a

cabo a través de medios digitales, como el robo de información personal en línea o la creación de perfiles falsos en redes sociales (Anonimo, 2018).

Macías Lara y otros concuerdan con Martínez al mencionar que la suplantación es una práctica que se da normalmente en redes sociales, un espacio digital donde la identidad digital se ve desprotegida.

La suplantación de identidad se produce cuando alguien finge ser otra persona con el propósito de engañar a otros. Es como si alguien se pusiera una máscara o un disfraz para hacerse pasar por otra persona, con el fin de obtener información, algún beneficio, difamar o cometer acciones ilegales en nombre de esa persona (INCEBE, s.f.).

Los autores en su concepto concuerdan en que la suplantación de identidad es una forma de fingir la identidad, a través de documentos perdidos, fotos en línea y redes sociales, con la finalidad de obtener un beneficio. La suplantación de identidad no solo se da de forma física, usualmente se usa el robo de identidad digital para cometer fraudes económicos y perjuicios al honor y al buen nombre.

3.2.1.1.4 Identidad digital

La identidad digital, se considera un término insólito y desconocido, si bien hemos logrado comprender la identidad como un derecho innato del ser humano que recae en su característica al ser y a su autodeterminación. En una sociedad dinámica que crece de la mano con la tecnología, lleva a los juristas a contemplarse incógnitas con relación a considerar si la misma se emplea como un derecho el cual no está tutelado, lo que incrementa las nuevas formas de criminalidad en una era digital.

La realidad es que la identidad digital todavía no es un concepto jurídico admitido o reconocido como tal por la doctrina, ni tan siquiera el uso de la expresión se ha generalizado en los textos jurídicos, sino que, antes al contrario, por ser un concepto que no se ha perfilado ni concretado, necesariamente está sujeto a controversia (Caletrío, 2022, p. 956).

Caletrío establece un concepto sobre este término desconocido y menciona que “La identidad digital debe ser entendida como la manifestación de la identidad física y de la identidad intelectual o moral (o ideal, como se designa en Italia) del individuo en el entorno digital, ni más ni menos que esto” (Caletrío, 2022, p. 958). Con ambos conceptos del autor, podemos decir que la identidad digital es un conjunto de todos los datos de la persona para identificarla en la red, estos ayudaran a identificarla e individualizarla, manifiesta que otras personas buscan ampliar este término en sentido de proteger todos los datos de las personas que existan en internet, tanto los creados por ella misma o los que son generados por terceros.

Según F. Georges, la identidad digital está constituida por diferentes tipos de datos según el usuario tenga o no la intención de revelarlos, lo que da lugar a una identidad declarada, compuesta por aquella información que revela expresamente la persona, otra identidad actuante, según las acciones que esta lleva a cabo, y otra calculada o inferida según el análisis de las acciones que realiza la persona. Toda esta información puede ser utilizada para configurar una idea de quien es y que le gusta a una persona determinada (citado en Fundación Telefónica, 2013).

Al contrario que los comentarios de los autores anteriores Ernesto Liceda (2011) manifiesta que no existe un Identidad Digital debido a 3 aspectos claves, el primero establece que existe identidad digital para mantener correspondencia, solo así con datos de la red y de una persona real se establece una identidad digital. Segundo, una persona crea varias identidades digitales en la red, lo cual conlleva a que no todas estas identidades son de su total identificación. Tercero existe la posibilidad de encontrar identidades digitales vacías, porque las personas que crean estas identidades dejan de usarlas físicamente. Georges y Liceda concuerdan en que la identidad digital permite que el individuo tenga una personalidad que solo existe en el ciberespacio.

3.2.1.2 Evolución histórica de la Inteligencia artificial

La evolución tecnológica comienza a partir de la industrialización, debido a la mecanización de las labores agrícolas y movilización de personas, estas causales son el inicio de un mundo que avanza y se dinamiza con cada década. La Industrialización trajo consigo las migraciones masivas del campo a la ciudad, dándonos un ejemplo de cómo la inteligencia artificial nos adapta a una nueva realidad tecnológica existente (Valera, 2025)..

Fue en el año 1950, que se da inicio al desarrollo de métodos y algoritmos de la inteligencia artificial. En 1970, se desarrollan los algoritmos necesarios para estos sistemas y es en la década de 1990 aparece el aprendizaje automático con el super computador Deep Blu de IBM, esta máquina es uno de los principales inicios y salidas de la IA al mundo, este permite su ingreso en la cotidianidad de laboratorios, empresas y personas (Dirección de Ciberdelitos Ministerio del Interior, 2024).

En la actualidad la tecnología y la inteligencia artificial se ha vuelto parte de la vida diaria de las personas, y en consecuencia surgen nuevos delitos, mientras que, otros se adaptan a las nuevas tecnologías para poder obtener distintos fines, que se convierten en conductas típicas. Gustavo Sain establece que la vinculación dentro el delito y la tecnología comienza en el siglo XIX con la creación del telégrafo en donde se interceptaban comunicaciones para transmitir información falsa y con ello obtener un beneficio económico (Llinares, 2012).

En la década de los 60 era común boicotear el financiamiento de la guerra de vietnam, a través de uso del servicio gratuito de telefonía, utilizaban cajas azules para reproducir sonidos grabados idénticos a los de Bell Corporation. En los años 70 con el desarrollo y creación de las computadoras existieron distintas actividades ilícitas con finalidad de lucro dentro de los cuales se destacaban la piratería de software, sabotaje de datos, espionaje y extorsión. Ya en la década de los 80 surgen otro tipo de delitos como la alteración de archivos y manipulación de las facturas de pagos de salarios. En Norteamérica en los años 90 la incidencia de delitos informáticos se vuelve trascendental al existir distintas formas de criminalidad dentro de las empresas hasta el área artística, la música y el cine, orillándoles a crear leyes como el Copyright. Lo más peligroso de esta época fue el rebrote de pedofilia y pornografía infantil en la red (Anónimo, 2018).

3.2.1.3 Cibercrimen y la cbersuplantación de identidad

El término cibercrimen para referirnos a un comportamiento concreto que reúne una serie de características criminológicas (también podrían ser legales) relacionadas con el ciberespacio (sentido tipológico), o para tratar de identificar un tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas en el ciberespacio que afectan a bienes jurídicos dignos de protección (sentido normativo) (Miro Llinares, 2012, p. 40).

Se entiende como cibercrimen a la forma de describir y sistematizar las formas de afectación de los bienes jurídicos dentro de las tecnologías de información y comunicación también denominadas (TIC), es decir, determina el tipo penal del comportamiento criminal en el ciberespacio, no obstante, “para que estemos ante un cibercrimen no bastará con que se utilicen las TIC para realizar el comportamiento criminal, sino que se exigirá que tal uso tenga que ver con algún elemento esencial del delito” (Miro Linares, 2012, p.41).

Miro en su obra, explica las generalidades del ciberespacio lo refiere como aquel lugar en la red que rompe la distancia para la comunicación en donde le sujeto interactúa y tiene una identidad digital. Antes era necesario un lugar físico para poder ingresar al ciberespacio, puesto que, solo se podía ingresar de determinados lugares, no obstante, a partir de la creación de los smartphone y el wifi podemos acceder a este lugar desde cualquier parte del mundo y esto gracias a la aceleración subjetiva del tiempo.

Como establece Gustavo Sain en su obra La estrategia gubernamental frente al cibercrimen; los delitos informáticos son aquellos delitos convencionales, que se adaptan a las nuevas tecnologías, se reinicia su forma de criminalidad mediante el uso y a aplicación de los dispositivos electrónicos y servicios informáticos.

La suplantación de identidad es uno de estos delitos que sin ser nuevos adquieren una dimensión en el ciberespacio, lo que permite el logro de un sin número de ciberataques, es por ello que, dentro de la cibercriminalidad, se entiende a la suplantación de identidad como la adquisición de los datos de un sujeto en el ciberespacio para luego usarlos a su conveniencia como si le pertenecieran, hay que tener en cuenta que la suplantación de identidad es el primer paso para la ejecución de un delito más elaborado, en especial para cualquier tipo de fraude informático.

3.2.1.4 Tipos de suplantación de identidad Deepfake, Spoofing e Identity Theft

3.2.1.4.1 Deepfake

Dentro de la suplantación de identidad digital o a través de inteligencia artificial encontramos distintos tipos y términos que tienen el mismo tipo penal, pero son diferentes el uno del otro por sus características. El denominado deepfake uno de los puntos de inicio y de inflexión en la investigación, “hace referencia a contenidos audiovisuales —principalmente videos, imágenes y audios— generados o alterados mediante técnicas de aprendizaje profundo (*deep learning*), que permiten simular con gran realismo la apariencia, voz o acciones de una persona” (Chesney & Citron, 2019, citado en Atencio, 2025).

“El objetivo de tales videos es entonces poder realizar copias digitalizadas de cualquier personaje público o privado para poder hacer que esta copia haga o diga lo que el

autor o autores de esta creación se les ocurra” (Oliva, 2022, s/p). Los autores mencionan que el deepfake funciona como un titiritero, a través de esta aplicación tecnológica su marioneta hará lo que desee, refieren que usar deepfake es sumamente sencillo, porque para crear este tipo de imágenes generativas el sujeto debe hacerlo a través de aplicaciones software generativas con el cual, crean un clon perfecto en base a su víctima.

La primera aparición del deepfake no fue en los videos de política para reprochar las acciones del gobierno, al contrario, este término aparece en las plataformas de contenido pornográfico, en donde tomaban las imágenes de las actrices de contenido sexual, usan su cuerpo como base física de las imágenes o videos públicos de sus famosos favoritos. El deepfake se divide en distintos tipos, dentro los cuales, se destacan el deepfake pornográfico, deepfake psicosocial.

3.2.1.4.2 Spoofing

El spoofing, se diferencia del deepfake porque “se utiliza la ingeniería informática para lograr los distintos mecanismos existentes para la identificación de los sistemas que actúan en el ciberespacio” (Miro Llinares, 2012, p. 80). Es decir, mientras el deepfake se considera más fácil y accesible por su tipo de acción y aplicación, el spoofing es más complejo, requiere de ingeniería informática para ingresarse en el software y suplantar la identidad. Según Miro existen cinco formas de spoofing. 1) IP spoofing, se utiliza técnicas y programas para sustraer la dirección IP original por otra. 2) ARP spoofing, se falsean las tablas ARP (Address Resolution Protocol, actúa como guía telefónica para enviar datos directamente) para que envíen al atacante los paquetes hosts en lugar de su propia dirección. 3) DNS spoofing. (Sistema de Nombre de Dominio) Esta busca modificar el nombre de la IP de un servidor para poder ingresar a el mismo, se hace esto si existe algún tipo de falla en el sistema, es lo que realiza prácticamente el pharming 4) Web spoofing, es el más usado por los atacantes, puesto que por medio de links falsos haciéndose pasar por otras páginas sustraen información. 5) mail spoofing, suplanta la dirección de correo electrónico para enviar spam, así inicia el ataque del phishing.

3.2.1.4.3 Identity Theft

Miro Llinares dentro de su libro crea un glosario de términos en donde explica mejor el significado de las nuevas palabras utilizadas en los ciberdelitos, que son de desconocimiento para la ciudadanía y a causa de esta falta de conocimiento el individuo se encuentra más propenso a ser una víctima del cibercrimen.

cuando se habla de *identity theft* se suele utilizar presuponiendo el futuro uso delictivo de la suplantación, esto es, como la utilización o explicación de los datos de identificación personal u otro tipo de información de la persona como el nombre, el número de DNI, etc., para cometer fraude o participar en otras actividades ilegales (Miro Llinares, 2012, p. 79).

Los términos analizados anteriormente son parte de la misma rama del tipo penal de suplantación de identidad, sin embargo, cada uno engloba un mundo tecnológico distinto, el deepfake suplanta la identidad de una persona a través de la inteligencia artificial, utiliza técnicas de aplicaciones generativas que replican voces o que se incorpora como propia una

imagen o video adulterado pero con un alto grado de realismo. Dentro de esta investigación nos enfocamos específicamente en el deepfake, debido a que esta conducta implica un riesgo para la imagen e identidad del ciudadano, que al ser vulnerado causa una deshonra a su persona.

3.2.2 UNIDAD II: MARCO NORMATIVO Y ANÁLISIS DEL DERECHO PENAL ECUATORIANO

3.2.2.1 La suplantación de identidad mediante inteligencia artificial un análisis de la norma y del Código Orgánico Integral Penal.

3.2.2.1.1 La identidad digital un bien jurídico protegido

En capítulos anteriores, se especifica la definición de identidad digital, sin embargo, en este apartado entenderemos a la identidad digital, desde un punto de vista jurídico, porque, se convierte en un bien donde el estado deberá protegerlo y tutelarlos. La identidad hoy ha cambiado y adopta a un ambiente tecnológico en una dimensión distinta la cual la denominaremos RED o ciberespacio, el producto de este dinamismo provoca la creación de un nuevo derecho como sería el derecho a la identidad digital, un término que a pesar de no ser acuñado en los juristas acrecienta en la sociedad. Fernández Burgueño (2012) concuerda al decir que “en la era de la información existe un nuevo derecho a la identidad digital, que no se limita a los datos físicos o registrales de una persona, sino que abarca también su presencia, reputación e interacción dentro del ciberespacio” (citado en Guaycha, 2025).

El entorno digital permite a las personas desarrollar relaciones sociales, laborales, académicas y comerciales que pueden verse severamente afectadas por actos de suplantación, produciendo daños no solo a su imagen, sino también a su credibilidad, acceso a servicios, relaciones y oportunidades profesionales (Guaycha, 2025).

El bien jurídico protegido de la identidad va más allá de la integridad o seguridad en tecnologías, este bien, abarca a la identidad como personal proyectándola y construyéndola en el ciberespacio, por lo que, la suplantación de identidad adquiere un nuevo riesgo al identificar que el tipo penal tiene distintas propiedades y características cuando se trata del ciberespacio.

Otras de las causales para definir a la identidad digital como un bien jurídico protegido es la complejidad en la prueba, se necesitará de distintas técnicas, conocimientos en informática forense y ciberseguridad que solo obtendrá por el Estado para una correcta recolección de pruebas y atribución de responsabilidades, también por medio de la ayuda del gobierno junto con la colaboración internacional, se detendrán a los victimarios que se esconden detrás de una pantalla, y a quienes ocultan su identidad con ingeniería avanzada exhumándose de toda culpa.

3.2.2.1.2 Principio de legalidad

La Constitución de la República del Ecuador, se constituye como un Estado de derecho, regido por un principio de legalidad, debido a que toda actuación debe encontrarse autorizada por la ley. El art 226 de la CRE menciona “las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley” (Constitución de la República del Ecuador [CRE], 2008). Con el crecimiento de las tecnologías y la transformación digital este principio adquiere complejidades al momento de ser efectuado, se dejaría nuevamente en impunidad todas las actuaciones delictivas cometidas por medios digitales.

3.2.2.1.3 Derecho a la identidad (Art 66 N.28, CRE)

El artículo 66 numeral 28 de la CRE reconoce a la identidad como un derecho personal y colectivo. Por su parte, la Corte Constitucional en su sentencia No. 732-18-JP/20, menciona que todos los atributos del artículo 11 numeral 2 de la constitución en relación con la nacionalidad, origen, etnia, nombres, etc, son elementos que integran la identidad y los mismos son garantizados por la Constitución (López, 2024, s/p).

En cuanto a los atributos de la identidad, estos pueden ser clasificados en tres categorías. En primer lugar, los atributos inherentes, dicho de otra forma, biológicos o de comportamiento, como es el iris, el rostro, la retina, la huella dactilar o de voz, patrones al redactar un correo o mensaje de texto, tono de voz, inicios de sesión esperados, entre otros datos biométricos. En segundo lugar, los atributos asignados, por ejemplo, el nombre y apellido de una persona, su lugar de nacimiento o domicilio, su número de teléfono y número de la cédula de ciudadanía. En tercer lugar, se encuentran los atributos acumulados, y como ejemplo clásico se puede enunciar el historial médico, pero también puede ser el historial crediticio o incluso las preferencias contenidas dentro de la meta data de un teléfono. (López, 2024, s/p)

Dentro de la categoría establecida por López, el artículo 66 numeral 28 de la CRE, entra en el segundo atributo de identidad, el Estado reconoce a la identidad como el nombre, nacimiento o domicilio, sin embargo, como la autora mismo comenta no solo existe este tipo de identidad, existen otras categorías que, no se encuentran protegidas y tuteladas por el Estado.

El artículo 75 de Constitución del Ecuador manifiesta que todas las personas tenemos derecho al acceso gratuito a la justicia sujetándose a los principios de inmediación y celeridad, establece que en ningún caso un acto que vulnere un derecho fundamental queda en la indefensión, la norma mismo menciona que el incumplimiento de esta será sancionado por la ley. No obstante, el artículo 75 no tutela el bien jurídico de la identidad si es digital, lo que instaura una anomia claramente visible, sobre todo en la suplantación de identidad mediante inteligencia artificial.

3.2.2.1.4 Análisis del artículo 11 de la Convención Americana de Derechos Humanos

El artículo 11 de la Convención Americana de Derechos Humanos consagra el derecho a la honra y el reconocimiento a su dignidad, este establece que las personas gozarán

de la protección de injerencias arbitrarias o abusos en su vida privada, familiar, o en su domicilio según como corresponda su reputación (Convención Americana sobre Derechos Humanos [CADH], 1969). Es así como, este precepto constituye una garantía base para la protección del ambiente personal del ser humano frente a injerencias ya sea de una manera estatal o de manera particular.

Entendemos que el numeral primero instaura en general el respeto a la honra y a la dignidad humana, entendiéndose que son derechos inherentes al ser humano solo por el hecho de serlo, comprendemos que la honra se enlaza directamente con la estigmatización social, así mismo con la reputación que los individuos poseen, en tanto la dignidad, se conjuga con el valor intrínseco del ser humano y esa autonomía moral que posee (Convención Americana sobre Derechos Humanos, 1969). En los casos de suplantación de identidad mediante inteligencia artificial, como la creación de perfiles falsos, deepfakes, o la utilización de datos personales para aparentar la identidad de una persona, se entiende que estos bienes jurídicos son vulnerados, porque modifican artificialmente la apreciación social de la persona, además de utilizar su identidad sin su consentimiento.

La suplantación de identidad mediante inteligencia artificial tiene una naturaleza injusta y no persigue ningún fin legítimo que sea compatible con los derechos humanos y además genera un daño desproporcionado en los derechos personales de las víctimas. Más allá de una simple prohibición el numeral segundo y tercero de la normativa impone al Estado una obligación positiva de ofrecer una protección legal que sea realmente efectiva. No es suficiente con que el Estado se limite a no vulnerar estos derechos por su propia cuenta su deber es actuar y adoptar medidas legislativas, administrativas y judiciales para prevenir, investigar, sancionar y reparar estas violaciones.

En la era de la inteligencia artificial este compromiso es crítico. En la actualidad muchos ordenamientos jurídicos especialmente en el ámbito penal no detallan estas conductas de forma expresa, esta carencia crea vacíos normativos y serias dificultades probatorias que, lamentablemente, suelen terminar en la impunidad.

El artículo 11 de la CADH se convierte en el fundamento circunstancial para exigir a los Estados la modernización de sus marcos normativos. Además, se considera inminente fortalecer las leyes ante las nuevas amenazas que ha creado la IA frente los derechos como la honra, la dignidad y la privacidad. El sistema penal no puede sancionar la suplantación de identidad por IA porque no está tipificado como delito, sin embargo, en los estatutos internacionales se interpreta como un incumplimiento de las obligaciones internacionales la vulneración de estos derechos, debido a que el Estado ha asumido su responsabilidad en materia de derechos humanos (Convención Americana sobre Derechos Humanos, 1969).

3.2.2.1.5 Generalidades sobre la identidad según la Declaración Universal sobre Bioética y Derechos Humanos

La Declaración Universal sobre Bioética y Derechos Humanos adoptada por la UNESCO en 2005, se impone en la actualidad como un pilar normativo internacional esencial para comprender los límites éticos del desarrollo científico a pesar de que este instrumento no fue diseñado originalmente para regular la identidad digital o la suplantación mediante la inteligencia artificial, sus principios fundamentales ofrecen un mapa general

sólido para la protección de la identidad. Bajo esta idea la identidad, no se reduce a un simple registro de datos, sino, que se reconoce como la manifestación más profunda y esencial de la dignidad humana en el contexto tecnológico.

Entendemos la identidad como ese complemento de características biológicas, psicológicas, sociales, culturales y jurídicas que permiten reconocer a cada una de las personas y distinguirlas de las demás. Desde la Declaración Universal sobre Bioética y Derechos Humanos, la identidad está intrínsecamente ligada a la autonomía y la integridad personal. Por ello, estos principios constituyen un fundamento ético irrenunciable de cualquier regulación sobre el uso de tecnologías emergentes que tengan el potencial de afectar o alterar la individualidad humana.

Bajo esta percepción, el artículo tercero, establece el respeto a la dignidad humana, los derechos humanos y las libertades fundamentales como el principio rector de todo avance tecnológico (Declaración Universal sobre Bioética y Derechos Humanos [UNESCO], 2005). Este reconocimiento implica que ninguna herramienta, incluida la inteligencia artificial, es justificable ante la alteración de la identidad de una persona sin su consentimiento.

Asimismo, el artículo quinto pone en el centro el respeto a la autonomía y la responsabilidad individual, lo cual otorga a cada persona el derecho soberano a decidir sobre el uso de sus datos personales, su imagen, su voz y cualquier otro elemento que la represente (UNESCO, 2005). Cuando la inteligencia artificial se utiliza para suplantar la identidad de un individuo, se produce una violación de este principio y se trata de una apropiación ilegítima de elementos de identidad para crear representaciones falsas que no reflejan la voluntad ni la realidad de la persona afectada.

Para mejorar esta protección, el artículo sexto, habla sobre el consentimiento informado, exige que toda intervención sobre la persona o su información relevante cuente con una autorización previa, libre y expresa. En los escenarios de suplantación de identidad digital, la ausencia total de este consentimiento convierte a estas prácticas no solo en un fallo técnico, sino en conductas éticamente rechazables y jurídicamente inaceptables que requieren una atención especial por parte de los órganos de justicia.

El artículo octavo alude al reconocimiento de la tecnología como fuente inseguridad en los individuos. El uso de la inteligencia artificial para la creación de contenido como los deepfakes o la clonación de voz, incrementa los daños reputacionales, psicológicos y jurídicos y con esta realidad el derecho debe ofrecer una respuesta que reconozca y mitigue estas nuevas formas de exhibición digital.

El artículo noveno protege la privacidad y la confidencialidad de la información personal, que resulta el punto de partida para la identidad en su dimensión digital. Se conoce que actualmente el perfil se construye a través de datos informáticos. Su adquisición, tratamiento y reutilización sin consentimiento constituye una violación a la privacidad y una forma de vulnerabilidad al derecho intrínseco del ser humano.

La Declaración no habla expresamente de la suplantación mediante inteligencia artificial, deepfakes, sus principios permiten afirmar que la identidad es un bien jurídico protegido de la dignidad humana, el cual será garantizado ante los riesgos tecnológicos. La actual ausencia de una regulación penal específica frente a estos fenómenos revela una vacío entre los principios bioéticos internacionalmente reconocidos y la actual normativa. Esto

justifica la necesidad urgente de revisar y fortalecer el marco jurídico penal para asegurar una tutela efectiva de la identidad humana en la era digital y evitar que estos ataques queden en la impunidad.

3.2.2.1.6 Anomias del artículo 212 del COIP

Según el Código Orgánico Integral Penal del Ecuador la suplantación de identidad se encuentra tipificada en el artículo 212. Este artículo estipula que quien suplante la identidad de otra persona para obtener un beneficio personal o para un tercero, provoca un perjuicio, por lo que, será sancionado con una pena privativa de libertad que va desde uno hasta tres años (Código Orgánico Integral Penal [COIP], 2014).

Pese a que la redacción del tipo penal es extensa y, en teoría, podría incluir comportamientos llevados a cabo con medios digitales, tiene serias restricciones cuando se refiere a las modalidades promovidas por inteligencia artificial.

Uno de los principales obstáculos es el tipo penal porque no menciona explícitamente la suplantación realizada por medio de tecnologías, algoritmos o alteración biométrica. El tipo penal que se encuentra tipificado en el 212 establece un principio bajo una lógica de reemplazo tradicional de manera física o documental, mas no digital, lo que provoca graves dificultades en la práctica judicial en especial en el auge de los ciberdelitos. Contrario a esto, el deepfake es una forma de suplantación que se realiza a través de un espacio digital donde el autor no tiene contacto con la víctima ni con terceros, sino que a través de un artefacto digital disuelve los límites tradicionales de la responsabilidad penal.

El artículo 212 del (COIP, 2014) establece, que existe simultáneamente un beneficio para el autor o un tercero y un daño para la víctima, lo que constituye un delito de resultado. En el artículo mencionado, se excluye la tipificación de numerosas acciones que son muy perjudiciales, como la propagación de un deepfake que dañe el honor, la reputación o la paz emocional de alguien, pero que no genere una ganancia económica demostrable. La complejidad para comprobar esta clase de hechos en contextos digitales da como resultado un aumento en la impunidad, se deja a los afectados sin una protección real ante ataques directos a su identidad.

Por otro lado, el marco legal vigente no abarca de manera específica prácticas como la alteración facial automatizada, la clonación de voz, la manipulación de datos biométricos o la creación de identidades falsas que parecen reales, pese a que estas acciones afectan de manera negativa a los bienes jurídicos protegidos como la honra, la privacidad y la integridad personal. El hecho de, que no se tipifiquen explícitamente demuestra una importante desproporción entre el acelerado avance tecnológico y la capacidad estatal para responder. La ausencia de precisión provoca que la protección de los derechos ciudadanos se debilite, y también obstaculiza el trabajo de jueces y fiscales al perseguir y castigar estas nuevas formas de delincuencia.

En este contexto, es esencial incluir un tipo penal específico que controle el empleo malintencionado del deepfake como una forma independiente de suplantación de identidad. Una reforma al Art. 212 del (COIP, 2014) que abarque la suplantación de identidad mediante IA donde defina los elementos constitutivos, medios tecnológicos, que se encuentren involucrados y un rango de sanciones acorde al daño causado. No se busca sancionar el

desarrollo o la utilización legítima de la inteligencia artificial, sino más bien castigar de manera eficaz y disuasoria su uso perjudicial, para adecuar el derecho penal a los riesgos específicos de la era digital.

La normativa penal ecuatoriana no es suficiente para afrontar los retos que se presentan en la suplantación de identidad mediante inteligencia artificial. El Artículo 212 del (COIP, 2014) establece una forma de protección de la identidad ante suplantación, sin embargo, esta no es suficiente ante la complejidad de conductas como el deepfake, lo que enciende con urgencia la necesidad de una reforma penal que considere las realidades y termino tecnológico que aseguren el derecho a la identidad.

3.2.2.1.7 Delito contra la integridad personal

El derecho a la integridad personal es uno de los derechos humanos fundamentales que ampara integralmente la vida física, psíquica y moral de toda persona, contra cualquier agresión lesión de particulares o del Estado, aun si ésta sea culposa.

Desde la óptica de los derechos humanos, esta protección, no se limita al cuidado del cuerpo; incluye con la misma fuerza la mente y la dimensión moral de la persona. Es defender a la persona de todo maltrato, tortura, trato cruel, inhumano o degradante que viole su dignidad. En esa línea, el artículo 5 de la Convención Americana de Derechos Humanos es tajante, toda persona tiene derecho a que se respete su integridad en estas tres dimensiones y está prohibido cualquier acto que las viole (Convención Americana sobre Derechos Humanos, 1969).

Esta tutela integral adquiere hoy mayor importancia, compromete al Estado y al ordenamiento jurídico a un análisis preventivo y a una tutela efectiva ante el desarrollo de nuevas tecnologías, como la inteligencia artificial, que abren la posibilidad a agresiones hasta hace poco inimaginables (Constitución de la República del Ecuador, 2008).

En el ordenamiento jurídico ecuatoriano, el (COIP, 2014) sanciona los delitos en contra de la integridad personal, protege la salud y el equilibrio emocional. Las figuras delictivas clásicas tortura, lesiones, etc., se pensaron para castigar agresiones directas, localizables, al cuerpo o a la mente. El cambio de paradigma ante la tecnología nos exige pensar en cómo salvaguardar la integridad en un mundo en donde el daño ya no se manifiesta en cicatrices físicas, sino en el daño profundo y a menudo devastador, que inflige en el ámbito digital y social de la víctima.

Una de las formas más preocupantes de estas nuevas amenazas es la suplantación de identidad con IA, especialmente a través de deepfakes. Estas herramientas crean imágenes, videos y audios hiperrealistas que ponen a la gente en momentos o en conversaciones que no tuvieron o en momentos que no estuvieron, lo que causa un daño grave a su integridad mental y moral.

Las consecuencias para la víctima suelen ser devastadoras: cuadros severos y prolongados de angustia, estrés crónico, humillación pública masiva y daño al honor y la imagen social, en muchos casos, irreparable. Pero, a pesar de su gravedad, estos ataques no encajan en las figuras clásicas de delitos contra la integridad que recoge el (COIP, 2014), porque, no se imaginaron mecanismos tecnológicos tan sofisticados.

3.2.2.1.8 Delitos informáticos

Los delitos informáticos o ciberdelitos son todas aquellas acciones delictivas, que se llevan a cabo mediante el uso de sistemas informáticos, redes digitales o tecnologías de la información, y que atentan contra bienes jurídicos protegidos, tanto individuales como colectivos. Más que una nueva categoría, la ciberdelincuencia es una mutación de los delitos de siempre como fraude, extorsión, robo de identidad, violación de la intimidad, ahora ampliados por la tecnología digital y, sobre todo, por la inteligencia artificial. En este nuevo escenario, la IA es un agente disruptivo que no solo potencia la capacidad de hacer daño y automatiza los ataques, sino que además dificulta su atribución, lo que abre paso a serios problemas técnicos, probatorios y éticos para el derecho penal (CHILAN & PÁRRAGA, 2020).

Con la llegada de la IA como los deepfakes, los deepnudes o la clonación de voz (deepfake voice), se han creado nuevas formas de criminalidad que afectan directamente a la identidad, la reputación o la salud mental de las personas. Estas tecnologías crean videos y audios falsos tan realistas que hacen que cualquiera crea que alguien hizo o dijo algo que nunca sucedió, por lo que abre la puerta a extorsiones, acoso, chantaje y manipulación emocional. Como indican los estudios, la facilidad de acceso a estas herramientas y lo difícil que resulta descubrir su falsedad han aumentado su uso para fines delictivos, y son los grupos vulnerables, como niños, niñas y adolescentes, los más afectados, sin embargo, ya afecta a toda la sociedad (Anónimo, 2021).

Desde otra perspectiva los delitos generados con inteligencia artificial muestran ciertos límites ante la facilidad del uso de plataformas digitales que promueven el anonimato, la falsificación y fácil distribución, lo que demuestra que las evidencias digitales podrían ser destruidas inmediatamente o incluso alteradas. La rapidez de evolución tecnológica y la respuesta del Estado demuestra la necesidad de una actualización legislativa que incluya expresamente estas nuevas formas de delincuencia, como la suplantación de identidad automatizada y el uso perverso de algoritmos de aprendizaje profundo.

En suma, los delitos informáticos no son simples delitos técnicos cometidos a través de computadoras: son violaciones modernas de derechos humanos como la identidad, la dignidad y la integridad. En el caso específico de la suplantación de identidad a través de la IA, la ciberdelincuencia evidencia la insuficiencia de la legislación vigente. Para garantizar la protección de los ciudadanos en el mundo digital, el ordenamiento jurídico tendrá que reconocer, prevenir y sancionar estos nuevos riesgos, y no permitir que el avance tecnológico cree un espacio de impunidad para la violación de los derechos (Atencio, 2025)

3.2.2.2 Anomías y problemas de tipicidad penal frente al deepfake, spoofing o identity theft

La aparición de la inteligencia artificial en el mundo delictivo ha dejado al descubierto un desfase del Derecho Penal ecuatoriano frente a la realidad tecnológica que crea un vacío cada vez mayor entre la realidad y la ley. Mientras que el legislador pensó el Código Orgánico Integral Penal desde una perspectiva de criminalidad material o documental, tecnologías como el deepfake, el spoofing o la suplantación de identidad, se mueven en un

plano inmaterial que desafía las categorías clásicas del delito. Y ello implica admitir que hoy el Derecho vive un momento de transición con un evidente desfase tecnológico legislativo. El informe base de esta investigación, elaborado por Tipanguano Chicaiza y otras investigadoras de la Universidad Regional Autónoma de los Andes, advierte que, hay primeros intentos para regular fenómenos particulares como la pornografía infantil deepfake, el Ecuador todavía carece de una legislación integral y preventiva en esta área. Esta ausencia de regulación sistemática no solo crea inseguridad jurídica, sino que deja al ciudadano en una situación de indefensión, y quedan sus derechos fundamentales a expensas de interpretaciones judiciales limitadas por el principio de legalidad penal (Tipanguano-Chicaiza, et. al, 2024).

Desde el punto de vista de la dogmática penal, para que una conducta sea punible debe subsumirse perfectamente en un tipo penal previamente definido por la ley. Pero el Art. 212 del (COIP, 2014), sobre suplantación de identidad, se queda corto ante los escenarios generados por la IA. El primer problema lo halla en la mutación de la acción ordinaria: mientras que la norma piensa en que el victimario "toma el lugar" de otro, el deepfake hace posible generar una identidad sintética que no suplanta al sujeto, sino que lo replica. Esta distancia entre el autor y la acción dificulta la imputación objetiva de la conducta. A lo anterior, se añade que el delito requiere de un beneficio para el autor o un tercero y un perjuicio para la víctima. Pero muchas agresiones con IA no buscan un beneficio económico, sino destruir la reputación, causar daño moral o la "muerte social" de la víctima, conductas que quedan fuera del tipo penal por no encajar en los moldes patrimonialistas clásicos.

En la perspectiva constitucional la suplantación de identidad mediante inteligencia artificial vulnera lo establecido en el artículo 66 numeral 88 de la constitución, el cual menciona la garantía de protección de la identidad en todas sus expresiones. El art. 178 del COIP establece la violación a la intimidad en donde se sanciona el acceso y difusión de información sin contar con el consentimiento o autorización del individuo, es decir se sanciona el acceso y difusión mas no la creación de contenido falso y su divulgación, esta omisión crea un vacío legal que abre la puerta a casos de impunidad para los usuarios de plataformas digitales que inconscientemente dejan su información en un espacio digital que no es completamente seguro.

A ello, se añade el spoofing o suplantación técnica, que dificulta la imputación penal por los problemas de anonimato y transnacionalidad característicos del ciberespacio. El documento de base indica que la falta de capacitación especializada de los operadores de justicia es una debilidad institucional importante en esta área. La insuficiencia del marco legal no es solo de contenido, sino también procesal. En el juicio penal la carga de la prueba la tiene la fiscalía, pero las actuales tecnologías de IA son tan sofisticadas que el fraude se vuelve indetectable al ojo humano. En el Ecuador no existen laboratorios forenses especializados ni protocolos de cadena de custodia para la evidencia digital sintética, lo que causa incertidumbre tecnológica (Tipanguano-Chicaiza, et. al, 2024).

3.2.2.3 La existencia de dificultades probatorias en delitos informáticos generados con IA

El análisis de los crímenes informáticos por medio de la IA en Ecuador muestra una crisis en el sistema punitivo, donde la prueba se convierte en el principal impedimento para hacer efectiva la justicia. La aparición de nuevas herramientas tecnológicas como los deepfakes y otros mecanismos de generación artificial han vulnerado la capacidad de obtener pruebas digitales, se da paso al debate jurídico acerca de la existencia de los datos, su autenticidad y veracidad. En el ordenamiento jurídico vigente, la criminalización del deepfake sería un primer paso relevante en la tutela efectiva de los derechos fundamentales, pero la escasez de una fuerza probatoria y la inexistencia de un marco regulatorio integral transforman estas figuras delictivas en materia de compleja aplicación práctica, lo que permite que las víctimas desamparadas ante la ley.

Esta situación, se agrava por la ausencia de una normativa con precisión respecto a la cadena de custodia y la evaluación de la evidencia digital producida por algoritmos. La modernización de estas herramientas de manipulación hiperrealista crea un muro de difícil acceso para el sistema judicial, los medios convencionales de peritaje informáticos son incapaces de diferenciar con certeza entre un registro verídico y una simulación algorítmica de alta fidelidad. La ausencia de protocolos periciales estandarizados para detectar material creado por medio de la IA impide que los jueces tengan la certeza moral para condenar y el principio de presunción de inocencia choca con la incertidumbre tecnológica (Tipanguano-Chicaiza, et. al, 2024).

Una de las debilidades institucionales de los operadores de justicia es la baja capacitación técnica, la incorrecta interpretación de las pruebas en los delitos informáticos al presentar la prueba sin tener el conocimiento del funcionamiento de las herramientas autorizadas. Es necesario que el Estado establezca laboratorios forenses de alta gama para equilibrar la balanza procesal, además que con la aplicación de estas nuevas herramientas ningún delito informático quedaría en impunidad. La modernización de las normas y la capacitación de los operadores de justicia asegurará la eficiencia judicial (Tipanguano-Chicaiza, et. al, 2024).

3.2.2.4 Sanciones según la Ley Orgánica de Protección de Datos Personales

Desde su vigencia en mayo de 2021, la (Ley Orgánica de Protección de Datos Personales [LOPD], 2021) se ha convertido en la base para proteger el derecho a la privacidad en Ecuador. Más que un código, este cuerpo normativo crea un régimen administrativo sancionatorio para protegerse contra tratamientos ilegales o abusivos. En el mundo hiperconectado actual, esta salvaguarda se vuelve esencial ante riesgos como el robo de identidad con IA, que básicamente alimenta del uso indebido de la información más personal: los datos biométricos, la voz, los rasgos físicos.

Para hacer efectiva esta protección, el capítulo XI de la LOPDP en el artículo 65 al 74, la norma estructura su régimen sancionador en una escala de proporcionalidad, donde distingue entre infracciones leves, graves y muy graves. Cuando nos referimos al responsable del tratamiento, las faltas leves generalmente son fallos en la estructura

organizativa, como no responder en plazo a las solicitudes de un ciudadano o no contar con políticas internas de protección. A pesar de que, estas violaciones parecen solo superficiales, abren la primera brecha en el muro de seguridad; un sistema debilitado es el terreno perfecto para que datos personales caigan en manos de algoritmos de IA sin control. (Ley Orgánica de Protección de Datos Personales, 2021)

La sanción se agrava en caso de infracciones graves. La ley castiga la transgresión de las reglas fundamentales del uso de la información para diferentes fines a los autorizados o compartir datos personales sin el consentimiento de su titular. Pero la LOPDP no habla sobre los deepfakes y las simulaciones desarrolladas con herramientas tecnológicas, en específico. A pesar de, se entiende que crear un perfil falso o un video por medio de IA, evidencia una desnaturalización del derecho a la identidad y de la finalidad inicial de los datos causa la vulnerabilidad del principio de licitud, y rompe totalmente la confianza en el mundo online.

En este contexto, el responsable de estos casos en muchas ocasiones plataformas tecnológicas o proveedores de servicios de IA, se convierte en una figura clave. La ley les impone una obligación de estricta confidencialidad y protección de la información. Si un responsable no informa de una violación de seguridad o permite un uso indebido de los datos, la ley da poder a la autoridad para intervenir con mano dura. Desde el punto de vista económico, la LOPDP en su artículo 72 establece sanciones con fines disuasivos: en el sector público las multas van de 1 a 20 Salarios Básicos Unificados (SBU), en tanto que en el privado se calcula sobre la base del volumen de negocios del año anterior, hasta el 1% (Ley Orgánica de Protección de Datos Personales, 2021).

Pero la ley no solamente tiende a reprimir, sino a reparar. Para analizar la gravedad de las sanciones, se consideran elementos humanos y técnicos como la intencionalidad, la reiteración y el perjuicio efectivo al honor o la intimidad del titular. Así mismo, la autoridad de Protección de Datos Personales tiene la facultad de ordenar medidas inmediatas, como la suspensión o eliminación definitiva del tratamiento. Estas capacidades son críticas ante una tecnología tan rápida como la IA, donde un error de reputación se hace viral e imposible de revertir en cuestión de segundos.

El alcance de la LOPDP adolece de un defecto ante los ciberdelitos, debido a que esta normativa es administrativa y no penal. Si bien la LOPDP se sanciona con altas multas y medidas correctivas técnicas, no logra dar una respuesta proporcional a la magnitud de una suplantación de identidad mediante inteligencia artificial, lo que destruye la seguridad jurídica de una persona. Y esto reafirma que el actual marco legal penal ecuatoriano, creado para la era física y de papel, se queda corto ante la ciberdelincuencia.

En definitiva, la LOPD es un gran paso para los derechos digitales en Ecuador, pero no es la solución. La distancia entre una multa administrativa y el daño que hace una IA mal utilizada nos dice que necesitamos una reforma urgente. Solo a través de la articulación del derecho administrativo, la regulación de elementos tecnológicos y un derecho penal renovado podremos asegurar que la identidad de los ciudadanos esté realmente protegida en la era digital

3.2.3 UNIDAD III: Impacto Social Generado por el Insuficiente Marco Normativo Penal

3.2.3.1 Impacto social de la suplantación de identidad mediante IA en Ecuador

La suplantación de identidad con IA se ha convertido en una de las formas más disruptivas de cibercrimen en la actualidad, no solo por su sofisticación tecnológica, sino por el daño que causa a la estructura de la sociedad. Y esto va más allá de lo legal y tecnológico, para impactar en la confianza ciudadana, en la seguridad y en la noción de la verdad en línea. En Ecuador, donde el mundo de la informática avanza a pasos agigantados, los impactos de esta forma delictiva se sienten con especial sensibilidad, porque convierten el riesgo tecnológico en vulnerabilidad humana.

Como ya reconoce el Boletín de Análisis de la Ciberdelincuencia del Ministerio del Interior, la inteligencia artificial ha dado a los ciberataques un nuevo grado de sofisticación. Los estafadores ya no requieren cercanía física para estafar; ahora utilizan métodos automatizados y personalizados que dificultan su detección y permiten una estafa masiva. En este nuevo mundo, la verosimilitud tecnológica de los deepfakes, la clonación de voz y la creación de imágenes falsas hace que el fraude sea prácticamente imposible de detectar, permite que el ciudadano quede indefenso ante un fraude de apariencia completamente real (Dirección de Ciberdelitos Ministerio del Interior, 2024).

Esta erosión de la confianza no solo perjudica a la persona, sino que socava la base de la convivencia. La sobreabundancia de material falsificado crea lo que varios estudios sobre deepfakes llaman una pérdida de realidad compartida. Cuando, no se diferencia una declaración real de una manipulada digitalmente, se rompe la confianza en las autoridades, los medios y el discurso público, se abre la puerta a una manipulación de la opinión pública que amenaza la democracia.

En el caso ecuatoriano, este hecho se da con los más débiles. Las estafas dirigidas tienen éxito entre, adultos mayores y personas con baja alfabetización digital. El daño aquí es doble: primero, el perjuicio económico directo y, segundo, el aumento del temor a relacionarse en línea, este retraimiento imposibilita cualquier capacidad de ejercer los derechos de comunicación y el acceso a oportunidades; ahonda el vacío social al transformar la tecnología en objeto de sospecha en vez de en palanca de progreso. (Dirección de Ciberdelitos Ministerio del Interior, 2024)

Pero el daño más profundo es el que no se ve. Los estudios en observatorios de deepfakes muestran que el daño moral y psicológico es el más común de los efectos de un ataque de deepfake, por encima de las pérdidas económicas. El acto de compartir una imagen o un audio manipulados genera ansiedad, aislamiento y estigma que destruye reputaciones y vidas en segundos. Esta manera de victimización psicológica es especialmente preocupante si las víctimas son niños, niñas y adolescentes. Ya se han viralizado casos en Ecuador donde niños usan la IA para crear deepfakes sexuales de sus compañeros, lo cual no solo es ciberacoso y pornografía infantil, sino que crea una alerta social comprensible sobre la seguridad en los espacios educativos. (Fernandes, Fernández, Molero y Pérez, 2025)

A esto, se añade la peligrosa difusión de estos productos digitales. Los algoritmos de las redes sociales, que se suelen utilizar para mostrar las reacciones emocionales fuertes, se convierten en cómplices involuntarios de la desinformación. Un deepfake, se viraliza y se convierte una suplantación aislada en un linchamiento público o un pánico moral colectivo, con independencia de su veracidad.

Finalmente, este panorama nos invita a pensar en la cultura digital y la necesidad de una educación integral. El desconocimiento de los riesgos de la IA nos hace más vulnerables y deja indefensos a aquellos que no tienen cómo detectarlos. En definitiva, la suplantación de identidad con IA en Ecuador no es solo una cuestión de líneas de código o de artículos de ley; es una revolución que redefine el daño, el peligro y la victimización en la sociedad. Esto refuerza la necesidad de que el sistema penal se adapte, porque no es suficiente castigar la conducta si el daño social y humano ya es irreversible.

3.2.3.2 Riesgos para la integridad personal, reputación y seguridad digital

Es preciso reconocer que esta tecnología no solo plantea nuevos desafíos legales, sino que afecta directamente aspectos fundamentales de la persona, como la integridad, la reputación y la seguridad informática. La IA generativa ha sustituido la noción clásica de identidad anclada en lo físico y documental por un mundo de datos, perfiles y representaciones sintéticas donde el sujeto pierde, en muchos casos, el control sobre su imagen, su voz y su presencia pública. Ahora la integridad personal no solo se refiere a la integridad corporal, sino también a la integridad moral, psíquica y simbólica de la persona, que también es parte de la personalidad jurídica. Cuando la huella digital de una persona es capturada, manipulada o replicada sin consentimiento a través de la IA, se genera un tipo de daño que no deja marcas físicas, pero viola la dignidad humana (Dirección de Ciberdelitos Ministerio del Interior, 2024).

La generación de material sintético no consentido en especial de naturaleza sexual, abusiva o degradante es una forma moderna de violencia simbólica que somete a la víctima a eventos que nunca sucedieron, pero que la sociedad considera que sí. La habilidad de la tecnología de simular la realidad de manera muy convincente deja a la víctima en una situación de indefensión, tiene que probar que lo que la gente ve como real es falso.

El honor y la propia imagen, que jurídicamente constituyen la reputación, hoy están amenazadas como nunca. La suplantación con IA no busca sólo el engaño instrumental, sino sustituir al sujeto en el espacio social, destruye su credibilidad, su reputación, su imagen pública. A diferencia de la difamación o la injuria convencionales, el daño a la reputación de los deepfakes, se distingue por su perdurabilidad, su reproducibilidad y su viralización. Una vez que una información falsa se viraliza en redes sociales o medios digitales, el derecho a la rectificación se ve seriamente comprometido por causas técnicas y sociales que están fuera del control del afectado.

En este sentido, la identidad digital se ha convertido en parte inherente de la persona jurídica. Ya no es solamente una información, ha evolucionado y ahora es la manera de ser, de presentarse y de ser reconocido en el mundo actual. Cuando un individuo ajeno se apropia de esa identidad a través de algoritmos no solo incurre en un delito, sino que le roba a la persona la capacidad de autodeterminarse en su representación, un estigma que anticipa

cualquier resolución judicial posterior. Es aquí donde se hace más evidente la insuficiencia del marco penal actual, con sus categorías tradicionales, para aprehender un daño que es masivo, automatizado y mundial.

Al mismo tiempo, la seguridad informática se ve afectada por la identidad, debido a que, deja de ser una figura confiable y se transforma en un conjunto de datos vulnerable y explotable. El uso de datos biométricos, imágenes, grabaciones de voz y demás informaciones personales para entrenar sistemas de IA para suplantación viola la confianza que sirve de base para las relaciones jurídicas, económicas y sociales en el mundo digital. La vulnerabilidad no está solo en el uso de herramientas tecnológicas, sino en la facilidad con la que se recopilan, procesan y reutilizan datos personales para fines ilícitos, casi siempre sin que el propietario sea consciente ni alcance a evitarlo.

En este aspecto la seguridad informática no limita a contraseñas o claves de acceso, sino al nivel de seguridad de la información que define la identidad de las personas en el ciberespacio. La capacidad de los cibercriminales para adaptarse es mucho más rápida que la capacidad de los marcos legales e instituciones de control que cambian una sensación de inseguridad jurídica y desprotección que erosiona la confianza ciudadanía en el derecho y el Estado.

Los peligros para la integridad, la reputación y la seguridad cibernética que implica la suplantación de identidad a través de IA, no son puras casualidades tecnológicas, sino violaciones de los principios de la personalidad que el derecho está llamado a garantizar. Entendemos que el desarrollo constante de la IA basándonos en los deepfakes y la clonación de voz, ha hecho que el derecho neto de identidad se vuelva muy vulnerable, donde todo lo creado con la tecnología llega a confundirse con la realidad. Es así como, estos escenarios requieren que el Derecho Penal Ecuatoriano salga de una lógica responsiva y desarrolle una mirada más atenta al daño que las herramientas tecnológicas causan en la actualidad, se entiende que violar el ciberespacio es violar la condición humana. Mientras la ley no evolucione para cubrir los vacíos de esta realidad, no solo habrá impunidad para ciertas conductas, que se comentan mediante Inteligencia Artificial, sino, que se agudizará la indefensión de las víctimas, atrapadas en un terreno donde su imagen, voz y honor son manipulados por algoritmos que el derecho aún no alcanza a regular ni sancionar con eficacia y eficiencia (Dirección de Ciberdelitos Ministerio del Interior, 2024).

3.2.3.3 Comparación con marcos normativos internacionales (Unión Europea y Estados Unidos)

La regulación de la suplantación de identidad con inteligencia artificial se ha convertido en un tema espinoso que los diferentes marcos legales internacionales han abordado desde perspectivas opuestas. Mientras que algunos países han desarrollado marcos preventivos y de controles ante esto, otros han preferido soluciones sectoriales y esencialmente reactivas. En este contexto, la comparación de los modelos europeo y estadounidense no es un ejercicio teórico, sino una necesidad para analizar si el actual marco penal ecuatoriano es suficiente para proteger la identidad de sus ciudadanos.

Basándose en la dignidad humana, la Unión Europea se ha concentrado en un enfoque sistémico y preventivo ante los riesgos generados por la IA, sobre todo ante la

manipulación de la identidad y la creación de deepfakes. Con su Reglamento de IA, Europa gradúa estos sistemas en función del riesgo, exige mucho más a las tecnologías susceptibles de violar derechos fundamentales como la dignidad, la vida privada o la identidad. En este contexto, los sistemas capaces de crear medios sintéticos realistas (imágenes, audios, videos falsos) se consideran de alto impacto social. Por eso la ley exige total transparencia sobre la naturaleza artificial del contenido y establece medidas para evitar usos fraudulentos, que impliquen tanto al usuario como al proveedor y al desarrollador del sistema (Ferreiro, 2025).

Este modelo normativo no actúa de manera aislada, sino que se coordina con el Reglamento General de Protección de Datos y la Carta de Derechos Fundamentales de la Unión Europea. Con ello se reafirma que la identidad digital es una extensión del núcleo de la personalidad jurídica. De este modo, la normativa europea no espera a castigar la conducta delictiva, sino que busca prevenir el daño antes de que ocurra. Los daños de una suplantación digital propagan de forma inmediata, viral y, en muchos casos, irreversible. Y en eso el Derecho concentra con exigencias de diseño responsable, evaluaciones continuas de riesgo y un fuerte control institucional.

A diferencia de varios países europeos en Estados Unidos no existe una ley federal, que se enfoque en la inteligencia artificial o los contenidos creados por herramientas tecnológicas. La legislación en Estados Unidos está dividida entre leyes estatales, sectoriales y el uso de figuras clásicas del derecho penal y civil. En algunos estados se ha legislado sobre deepfakes en casos específicos como elecciones o pornografía no consentida. A nivel federal se han propuesto leyes como la Take It Down Act para facilitar la eliminación de cualquier contenido creado con IA.

El modelo americano da prioridad a la libertad de expresión y confía en la reacción posterior del sistema judicial para reparar los daños causados, la reacción penal generalmente se pone en evidencia una vez que el daño ya se ha producido, a través de los tipos penales clásicos de fraude, extorsión, difamación o delitos informáticos. Al recaer la responsabilidad sobre todo en el individuo que abusa y nada en los creadores de la tecnología, el sistema pierde capacidad de anticiparse y controlar los riesgos de la suplantación automatizada de identidad.

Esta diferencia de miradas es muy reveladora para el caso ecuatoriano. En el contexto actual, Ecuador se encuentra más en el modelo reactivo que en el preventivo, y peor aún, carece de la capacidad institucional, tecnológica y legal para hacer frente a los impactos de la IA en la identidad. El Código Orgánico Integral Penal, se estructuró bajo una concepción de criminalidad material o documental, lo que dificulta su aplicación a conductas automatizadas y masivas que no encajan exactamente en las categorías clásicas de falsificación, suplantación o fraude (Ferreiro, 2025).

La falta de norma en cuanto a la suplantación de identidad por medio de deepfakes crea zonas grises en términos procesales y materiales, como la imputación penal, la prueba, y la atribución de responsabilidad si se habla de sanciones para dichos casos. Esta brecha entre la realidad tecnológica y la respuesta jurídica actual genera un vacío para los derechos fundamentales. En definitiva, la comparación entre la Unión Europea y los Estados Unidos muestra que la suplantación de identidad con IA necesita una respuesta regulatoria que vaya más allá de las sanciones. Para Ecuador, esta comparación hace evidente la necesidad de

reformular el Derecho Penal, incluye criterios de prevención y responsabilidad tecnológica para proteger mejor la identidad en el mundo virtual.

CAPÍTULO III.

4. METODOLOGÍA.

“Metodología jurídica es una disciplina que estudia la aplicación de los métodos de conocimiento a los diferentes ámbitos del derecho” (Durán, 2002, p.177).

4.1 Unidad de análisis

La unidad de análisis (o nivel de análisis) hace referencia, por lo tanto, a lo que será estudiado. En el área de las ciencias sociales, la unidad de análisis más común es el individuo. Pero la unidad de análisis puede ser un agregado de individuos (p.e. un municipio), un grupo-organización-institución (de modo que los datos son recogidos a nivel colectivo), un acontecimiento (p.e. un proceso electoral) o un producto cultural (p.e. un resultado escrito de los medios de comunicación) (Navarro, 2023, p. 14).

En vista de ello, la unidad de análisis de esta investigación se centra en la normativa penal ecuatoriana vigente, y la doctrina encontrada durante la investigación, este estudio se ubica en el territorio ecuatoriano, se analiza las limitaciones del marco penal actual frente al crecimiento acelerado de estas tecnologías y la aparición de ciberdelitos.

4.2 Métodos

Método inductivo: Ruiz-~~(2011)~~ menciona que “A diferencia del deductivo, el método inductivo determina o establece una ley general a partir de fenómenos particulares, es decir, va de lo particular a lo general” ~~221~~(Ruiz, 2011, p. 221). Este método inductivo nos permitió desarrollar la investigación a profundidad, porque se analiza cada vacío legal existente para con el tipo penal de la suplantación de identidad y como el incremento de las tecnologías como el deepfake abren puertas a la vulneración de derechos que ya han ocurrido en Ecuador y en otros países. También, nos permite observar hechos reales, examinar denuncias, evidenciar la dificultad de peritajes digitales, dictámenes fiscales y situaciones probatorias que demuestran que la legislación actual es insuficiente, lo que conduce a la necesidad de replantear el tratamiento jurídico de estas conductas emergentes.

Método jurídico-analítico: El método jurídico-analítico “consiste en dividir un todo abstracto o concreto en sus elementos integrantes a fin de investigar la naturaleza y efectos de cada uno de ellos; el análisis implica resolver el todo a través de las diferentes partes que lo integran” (Ruiz, 2011). Este método fue empleado para realizar un examen detallado de la normativa penal vigente, se desglosará su estructura, su alcance y sus limitaciones. La investigación requiere un análisis minucioso de aquellos artículos que parecen relacionados con la suplantación de identidad, sin embargo, no alcanzan a cubrir la sofisticación tecnológica del deepfake ni sus implicaciones en el ámbito probatorio y procesal. A través de este método, se logró comprender por qué las categorías jurídicas tradicionales son insuficientes frente al impacto de la inteligencia artificial en la construcción, manipulación y falsificación de identidades digitales.

Método dogmático: Para Odar “La dogmática jurídica es la encargada de estudiar a fondo las instituciones jurídicas, pero de modo abstracto, es decir sin verificar su materialización en la realidad” (Odar, 2016,p. 4). La aplicación de este método es necesaria porque la investigación no solo pretende describir normas, sino interpretarlas de manera sistemática, crítica y teleológica. Este método permitió analizar doctrina especializada en ciberdelitos, identidad digital, responsabilidad penal y protección de datos, así como revisar jurisprudencia relevante y principios generales del Derecho penal. La dogmática jurídica ofreció un marco conceptual riguroso que permitió reflexionar sobre aspectos como la tipicidad, antijuridicidad e imputación en casos de deepfakes criminales, y facilita la construcción de argumentos científicos que respalden la necesidad de una reforma legislativa.

Método jurídico-comparativo:

Según Tantaleán Odar en su obra Tipología de las investigaciones jurídicas menciona que el método jurídico-comparativo es:

En este tipo de estudio se parte de un ordenamiento jurídico “madre ” (que suele ser el nacional y que es aquel que se conoce meridianamente), para luego establecer semejanzas y diferencias con otro ordenamiento jurídico, y culminar con una propuesta de mejora del derecho, resultado de evaluar las bondades y defectos de cada uno de ellos, así como de verificar la factibilidad de aplicación de la propuesta. (Odar, 2016, p. 18).

Este análisis comparado permitió identificar aquellos modelos normativos acerca del dinamismo tecnológico y el incremento de la IA en los delitos tradicionales. Esta aplicación normativa sancionatoria es de carácter útil y aplicable en los países como la Union europea y Estados Unidos, los cuales son de apoyo en la creación de nuevas legislaciones en nuestro país. Gracias a este método, se demostró que la legislación nacional se encuentra rezagada frente a estándares internacionales, lo que reafirma la urgencia de incorporar regulaciones específicas para combatir la suplantación de identidad mediante inteligencia artificial.

4.3 Enfoque de investigación

Por las características de la investigación, se asumió un enfoque cualitativo, debido a que, al paradigma a desarrollar es el realismo-jurídico y post-positivismo con un enfoque sociológico y crítico del derecho, además, se realizó la revisión bibliográfica y la aplicación de una guía de entrevistas estructurada, con el fin de explorar las diversas opiniones y percepciones de expertos en ciencias jurídicas sobre la realidad normativa en base a el tema.

4.4 Tipo de investigación

La investigación es principalmente de carácter dogmático, porque se orienta al análisis lógico, sistemático e interpretativo del Derecho positivo. En este contexto, se estudia el contenido y alcance de las normas penales ecuatorianas relacionadas con la protección de la identidad, la falsedad y los delitos informáticos, evalúa su validez y pertinencia frente al fenómeno de la suplantación mediante inteligencia artificial. La dogmática jurídica permite identificar si el COIP responde adecuadamente a las exigencias actuales o si, por el contrario, presenta vacíos que comprometen la tutela de derechos fundamentales y favorecen

escenarios de impunidad. Este enfoque es indispensable para comprender la estructura normativa del problema y fundamentar la necesidad de una reforma penal.

La investigación también se clasifica como explorativa, el uso de deepfakes con fines delictivos es un fenómeno novedoso en Ecuador y aún poco desarrollado en la doctrina y jurisprudencia nacionales. El ordenamiento jurídico ecuatoriano no cuenta con un tipo penal específico que regule la suplantación digital mediante IA, que se examina fuentes preliminares, revisa casos aislados y analiza disposiciones generales que podrían relacionarse indirectamente con esta conducta. Debido a que existe escasa producción académica y normativa sobre el tema, la investigación explorativa permite abrir camino para futuras indagaciones y generar nuevos aportes teóricos y jurídicos.

De igual manera, la investigación posee un componente descriptivo, es necesario caracterizar el fenómeno de la suplantación de identidad mediante inteligencia artificial, para explicar sus elementos tecnológicos, su funcionamiento, sus riesgos y sus efectos en el ámbito jurídico penal. Este tipo de investigación permite detallar cómo operan los deepfakes, cuáles son sus principales usos ilícitos, qué impacto generan en la confiabilidad de la evidencia digital y cómo afectan a la víctima. La descripción rigurosa del fenómeno posibilita comprender por qué esta conducta desborda las categorías jurídicas tradicionales y evidencia la necesidad de un análisis más profundo del marco normativo.

4.5 Diseño de investigación

Según Sampieri “el investigador utiliza sus diseños para analizar la certeza de las hipótesis formuladas en un contexto en particular o para aportar evidencias respecto de los lineamientos de la investigación” (Sampieri, 2014, p.161). En otras palabras, el diseño de investigación es el plan o estrategia para confirmar si es viable la investigación a realizar

Dentro de esta tesis el diseño de investigación adoptado es de carácter no experimental debido a que no es posible manipular las variables que intervienen en el fenómeno estudiado. En el ámbito jurídico, especialmente cuando se examinan normas, principios, conductas delictivas y efectos sociales, los hechos deben analizarse tal como ocurren en la realidad, sin intervenir directamente en su desarrollo. Por esta razón, el estudio se basa en la observación, análisis documental, interpretación normativa y revisión de casos, sin modificar las condiciones del entorno jurídico o tecnológico.

4.6 Población y muestra

Universo o Población son expresiones equivalentes para referirse al conjunto total de elementos que constituyen el ámbito de interés analítico y sobre el que queremos inferir las conclusiones del análisis, conclusiones de naturaleza estadística y también sustantiva o teórica (López-Roldán y Fachelli, 2015).

La población de este estudio incluye a dos abogados especialistas en Derecho Penal un funcionario de la Fiscalía General del Estado, un servidor de la Fuerza Pública del Departamento de Ciberseguridad y un perito especializado en perfilación criminal y documentos jurídicos relevantes, todos ellos permiten comprender el fenómeno desde dimensiones técnicas, institucionales, personales y normativas. Debido a que este grupo no supera los 100 actores consultables y la investigación requiere información cualitativa de

alto valor, no se aplicó una muestra estadística, sino un muestreo probabilístico por conveniencia de participantes claves, cuyo conocimiento o experiencia aporte datos sustanciales para analizar la insuficiencia del marco jurídico penal frente a la suplantación de identidad digital mediante deepfakes.

4.7 Técnicas e instrumentos de investigación

Las técnicas de investigación “Es un método sistemático utilizado para recopilar y analizar información, con el fin de responder a una pregunta o resolver un problema específico.” (Romero, y otros, 2023, p.12). Es decir que es un procedimiento que es utilizado para recopilar y analizar un problema con el fin de resolverlo.

Para alcanzar los objetivos del estudio, se empleó técnicas cualitativas como la entrevista a expertos en Derecho penal y tecnologías digitales, y la observación documental de normas y jurisprudencia, complementándose opcionalmente con una encuesta para obtener datos cuantitativos sobre la percepción del marco penal vigente. Los instrumentos correspondientes a la investigación fueron en base a una guía de entrevista con preguntas abiertas dirigidas a profesionales, permite obtener información organizada y pertinente sobre la regulación y los efectos de la suplantación de identidad mediante IA.

4.8 Técnicas para el tratamiento de información

Para recopilar la información en esta investigación es necesario analizar el contenido temático, con el fin de obtener percepciones y valoraciones de los profesionales del derecho especializados en Derecho Penal, estudiantes en formación para abogados y funcionarios de Fiscalía. Dentro de las técnicas de investigación utilizaremos las siguientes:

- Elaboración del instrumento de investigación: se diseñó una guía de entrevista la cual nos ayudó a recopilar información.
- Tabulación de datos: la información recopilada se organizó en tablas para una mejor explicación de la información obtenida.
- Procesamiento de los datos e información: se clasificó las repuestas de cada pregunta en base a lo que manifestaron los entrevistados
- Interpretación o análisis de resultados: una vez obtenida la información se interpretó las mismas con un análisis crítico.
- Discusión de resultados: la discusión de los resultados permitió evaluar hasta qué punto hemos podido evidenciar ya respaldar la hipótesis.

CAPÍTULO IV.

5. RESULTADOS Y DISCUSIÓN

5.1 Resultados

En este capítulo, se ha recopilado la información a través de técnicas de investigación conocidas como entrevistas. La población, se encuentra conformada por Fiscales, abogados y fuerza pública, actores fundamentales por su conocimiento y experiencia respecto al tema de investigación planteado. A continuación, se presenta el perfil de cada entrevistado.

Entrevistado 001: Abogado/a especializado en Derecho Penal

Entrevistado 002: Agente Fiscal

Entrevistado 003: Abogado/a especializado en Derecho Penal

Entrevistado 004: Cabo Primero de Comunicaciones/Comando de Ciberdefensa.

Entrevistado 005: Perito magíster en psicología forense con especialidad en perfilación criminal.

Resultados de la entrevista por expertos

5.1.1 Resultados pregunta 1

¿Usted ha evidenciado contenido realizado con inteligencia artificial que le parezca hiperrealista? Si conoce un caso menciónelo.

En base a los resultados obtenidos en la pregunta 1 en la entrevista elaborada, 4 de 5 entrevistados afirman haber evidenciado contenido realizado con inteligencia artificial, mencionan, que se les ha hecho hiperrealista e incluso han realizado con su propia efigie videos e imágenes con IA. El entrevistado 001 expuso el caso de un allegado que fue víctima de suplantación de identidad mediante deepfake, en donde su imagen es modificada para y con ella creaba contenido que afectaba la reputación del implicado. El entrevistado 002 refirió un caso que se encuentra en investigación por una presunta suplantación de identidad para adquirir una firma electrónica, en la investigación se esclarece que utilizaron una fotografía en Facebook y la modificaron con inteligencia artificial para poder obtener este documento, a través del trámite que se realiza por la web, sin embargo, fiscalía considera, que no se sanciona el delito por suplantación, si no por falsificación y uso de documento falso. Por su parte, el entrevistado 004 reporta haber sido participe dentro de la investigación por suplantación de identidad, en donde la víctima fue el Ministro de Economía y Finanzas, dentro de esta investigación se logra determinar que clonaron su voz con inteligencia artificial y por medio de esta los autores del delito mediante extorción obtuvieron más de 10 000 dólares. Por último, el entrevistado 005 señala que el caso de suplantación de identidad que conoce refiere en cuanto a redes sociales, en donde uno de los implicados compartió su contraseña con su pareja y la misma suplanta su identidad a través de vía digital para amedrentar a sus amigos en línea. Contrario a lo manifestado por los entrevistados anteriores, el entrevistado 003 refiere no haber experimentado o conocido un caso de este tipo.

Tabla 1*Percepción de Hiperrealismo y casos de suplantación de identidad*

Entrevistado	Percepción de Hiperrealismo	Caso expuesto	Tecnología o Recurso usado
Sujeto 001	Si	Suplantación de Identidad de un allegado para afectar su reputación.	Modificación de imagen o deepfake.
Sujeto 002	Si	Obtención de forma fraudulenta de firma electrónica.	Uso de IA en fotos obtenidas de redes sociales para suplantar.
Sujeto 003	No	Sin conocimiento de casos.	Ninguna
Sujeto 004	Si	Extorsión al Ministro de Economía y Finanzas.	Clonación de voz con IA.
Sujeto 005	Si	Suplantación de identidad en redes sociales con finalidad de hostigamiento.	Acceso indebido a credenciales y suplantación de redes sociales.

Fuente: Elaborado por García. L. y Gavilanes. J.**5.1.2 Respuesta pregunta 2**

Desde su criterio profesional, ¿Considera usted que debería modificarse el artículo 212 del COIP en el cual versa la Suplantación de Identidad Expandiendo dicho artículo a los delitos generados por medio de la Inteligencia Artificial Deepfake?

En unanimidad, los entrevistados concuerdan en la modificación de artículo 212 del Código Orgánico Integral Penal. El entrevistado 001 refiere que el incremento de las nuevas tecnologías y su uso indebido permite el cometimiento de delitos. El entrevistado 002 menciona que muchos delitos van a reformarse debido al avance tecnológico, sin embargo, en referencia a la suplantación de identidad es ineludible incluir distintos numerales derivados a la inteligencia artificial y la tecnología como deepfake, después del inciso 212 para establecer una sanción mayor. Por otra parte, el entrevistado 003 establece que es necesario que se logre ampliar el marco normativo ante el contenido generado por IA. Según el entrevistado 004, es imprescindible la reforma del artículo 212 del COIP, refiere que la norma es insuficiente, lo que provoca impunidad ante el cometimiento de estos delitos. Por último, el entrevistado 005 indica que existe facilidad en el acceso a la información de las

personas y esto permite que se encuentren vulnerables, también señala que existe poco control respecto a la información personal.

Tabla 2

Criterios sobre la modificación del Art. 212 del COIP

Entrevistados	Postura ante la modificación del artículo 212 del COIP	Argumento
001	A favor	El incremento tecnológico facilita el cometimiento de nuevos delitos.
002	A favor	Incluir numerales agravantes derivados de la IA y tecnología.
003	A favor	Ampliación del marco normativo.
004	A favor	La norma es insuficiente lo que provoca impunidad ante los delitos con IA.
005	A favor	Existe poco control para proteger la información personal.

Fuente: Elaborado por García. L. y Gavilanes. J.

5.1.3 Respuesta pregunta 3

¿Considera que la responsabilidad penal debería recaer únicamente en el autor material del deepfake, o también en quienes, financian o facilitan la suplantación? ¿Por qué?

Respecto a esta interrogante, se identifican posturas diferentes por parte de los consultados. Los entrevistados 001, 003 y 005 concuerdan que la responsabilidad penal debe recaer en autor, coautor, cómplice y en quien financia y facilita el hecho. Por el contrario, los entrevistados 002 y 004 sostienen que en este tipo de delitos las investigaciones requieren personal especializado, además señalan que actualmente el personal ecuatoriano no se encuentra capacitado lo suficiente, por lo que consideran necesaria la cooperación internacional para determinar la autoría de este tipo de delitos.

Tabla 3

Responsabilidad Penal y desafíos

Descripción	Entrevistados	Afirmación
-------------	---------------	------------

Responsabilidad Penal	001,003 y 005	La responsabilidad recae en todo autor, coautor, cómplice o facilitador que realice o permita que el hecho se promueva.
Desafíos	002 y 004	Para determinar la autoría se necesita de investigaciones con personal especializado junto con la cooperación internacional.

Fuente: Elaborado por García. L. y Gavilanes. J.

5.1.4 Respuesta pregunta 4

¿Conoce usted si existen mecanismos legales, administrativos o tecnológicos que puedan complementar al sistema penal en este tipo de casos? Fundamente su respuesta.

Con respecto a la pregunta 4 los entrevistados presentan posturas divididas, por su parte el entrevistado 001 manifiesta que no conoce si existe algún tipo de normativa específica o de apoyo para este tipo de situaciones. Los entrevistados 002,003 y 005 coinciden en su respuesta y mencionan que la policía tiene un departamento de ciberdelitos y con ello un manual que fue elaborado junto con otras instituciones, también aluden que fiscalía está desarrollando un modelo para actuar en los casos de delitos informáticos. El entrevistado 004 establece que existen distintas normativas como La ley Orgánica de Protección de Datos, La ley establecida por el ARCOTEL, también menciona el uso del Código Civil, el cual permite acciones por daño moral.

Tabla 4

Mecanismos legales, administrativos o tecnológicos

Entrevistados	Instrumentos	Tipo de mecanismo
001	Ninguno	Desconocimiento
002,003,005	Manual de ciberdelitos	Policial
	Modelos de actuación fiscal	Fiscal
004	Ley de Protección de Datos Personales	Normativo
004	Acciones por daño moral (Código Civil)	Civil

Fuente: Elaborado por García. L. y Gavilanes. J.

5.1.5 Respuesta pregunta 5

¿Considera usted que la insuficiencia del marco jurídico penal influye en el incremento de la suplantación de identidad mediante inteligencia artificial deepfake en el Ecuador?

En referencia a la pregunta 5 los entrevistados concuerdan en unanimidad que existe insuficiencia en el marco jurídico penal en cuanto a los delitos cometidos con las nuevas tecnologías e inteligencia artificial, no obstante, cada entrevistado fundamenta sus respuestas con distintas razones. El entrevistado 001 menciona que mientras no exista norma no hay sanción, también refiere que los delincuentes tienen conocimiento de la norma y actúan en base a su conocimiento. El entrevistado 002 refiere que no existe una normativa legal que genere prevención ante estos tipos de delitos. El entrevistado 003 sostiene que existe falta de regulación penal específica y sobre todo actualiza frente a los delitos cometidos mediante inteligencia artificial. El consultado 004 indica que se están creando mesas técnicas para poder levantar un marco legal frente a los ciberdelitos. A su vez, el consultado 005 menciona que un tipo de delito se va develando y va abriendo un amplio espectro de diferentes líneas de investigación en relación con el hecho, porque no es individual, siempre va a tener otro tipo de diferentes connotaciones.

Tabla 5

Impacto de la insuficiencia normativa en el incremento de la suplantación con inteligencia artificial

Entrevistado	Percepción sobre insuficiencia normativa	Hallazgo	Factor de impacto
001	A favor	Los infractores se benefician de los vacíos legales y la ausencia de tipificación impide sancionar esto en base al principio de legalidad.	Impunidad
002	A favor	El sistema legal vigente no promueve la prevención y disuasión jurídica.	Ausencia de prevención
003	A favor	Normativa desactualizada ante la sofisticación nuevos delitos tecnológicos.	Vacio Normativo
004	A favor	Implementación de mesas técnicas encaminadas al desarrollo de un marco normativo en materia de ciberdelitos.	Respuesta del Estado
005	A favor	El derecho es dinámico y genera distintas líneas de investigación que la ley no abarca	Líneas de investigación diferentes

Fuente: Elaborado por García. L. y Gavilanes. J.

5.1.6 Respuesta pregunta 6

En el caso de que no se identifique al creador del deepfake o que este opere desde el extranjero, ¿qué nivel de responsabilidad podría tener el Estado por la falta de mecanismos regulatorios, de prevención o de ciberseguridad?

Los entrevistados en sus respuestas ante esta pregunta presentan posturas divergentes en sus contestaciones, por su parte, el consultado 001 menciona que la tecnología permite interconectarte con el mundo sin tener el control de lo que se publica o se crea en páginas sociales, dentro de otros aspectos menciona que la competencia es un factor importante, alude que si el autor material del hecho es identificado en el país de Colombia se debería aplicar su legislación, el entrevistado concluye que la responsabilidad no recae en el Estado. El entrevistado 002 menciona que este tipo de delitos cibernéticos no generan efectos jurídicos consecuentes al Estado, refiere que la entidad estatal vela por la consecuencia del delito de suplantación de identidad y no con el tipo penal, el consultado recalca que existen límites para que los fiscales determinen la autoría de una persona frente a un delito realizado con inteligencia artificial. El entrevistado 003 señala que el Estado si tiene la responsabilidad de fortalecer todos aquellos mecanismos necesarios para la correcta investigación en aspectos de delitos tecnológicos, junto con la cooperación internacional. El entrevistado 004 menciona que el Estado tendría responsabilidad internacional al no cumplir los tratados de los Derechos Humanos y las obligaciones del Pacto de San José, tiene responsabilidad constitucional para hacer cumplir la norma y responsabilidad administrativa por la insuficiencia de políticas frente delitos tecnológicos y ausencia de alfabetización digital. A su vez el consultado indica que desde su experiencia hasta el año pasado el Ecuador contaba con la existencia de un solo fiscal especializado en ciberseguridad y ciberdelitos. El consultado 005 mencionan que el Estado si tiene responsabilidad refiere que con ayuda internacional junto con los recursos estatales se podría investigar adecuadamente el hecho y establecer una sanción para la misma.

Tabla 6

Responsabilidad Estatal ante delitos con IA anónimos o transfronterizos

Entrevistado	Postura sobre la responsabilidad estatal	Argumento aplicado
001	En contra	La ausencia de control sobre las redes sociales y la competencia impiden atribuir responsabilidad estatal.
002	En contra	Los delitos cibernéticos no generan perjuicio al estado, condenan la consecuencia mas no el acto.
003 y 005	A favor	El estado tiene el deber de fortalecer los mecanismos de investigación y solicitar la cooperación internacional.
004	A favor	La limitación operativa, insuficiencia de recursos y la omisión de la norma produce responsabilidad estatal.

Fuente: Elaborado por García. L. y Gavilanes. J.

5.1.7 Respuesta pregunta 7

¿Cuál considera que es el principal reto probatorio para demostrar que una suplantación mediante IA ha generado un daño real y atribuible a una persona específica, tomando en cuenta la facilidad de alteración de contenidos y la falta de normativa procesal y penal clara?

En respuesta a la pregunta el entrevistado 001 manifiesta que sin reforma no hay delito alude que es necesario equipar a la fiscalía y al consejo de la judicatura para que personas especializadas en la materia puedan hacer un trabajo que combata este tipo de contenidos, indica que la falta de especialización técnica limita la eficacia para combatir este tipo de conductas. El entrevistado 002 menciona que el mayor reto es el presupuesto del Estado para invertir en capacitación a peritos y adquirir las herramientas necesarias para la correcta investigación. Para el entrevistado 003 el principal reto es contar con una pericia técnica que nos permita determinar o atribuir de manera específica al autor del cometimiento de este tipo de delitos. El entrevistado 004 señala que existen distintos retos probatorios como la autenticidad y alteración, necesidad de peritos especializados en análisis forense digital con certificaciones internacional, dificultad para establecer cadena de custodia digital que garantice integridad a la evidencia e insuficiencia de la norma. El entrevistado 005 alude que el reto probatorio principal es identificar el autor material del hecho.

Tabla 7

Desafíos probatorios de la suplantación de identidad mediante inteligencia artificial

Entrevistado	Reto probatorio	Ámbitos
001	Escasa especialización y formación de los funcionarios públicos.	Ámbito institucional
002	Brecha económica que dificulta la adquisición de software forense y capacitación de peritos.	Ámbito económico
003 y 005	Dificultad para identificar el autor material del hecho.	Responsabilidad penal
004	Riesgos de alteración en las pruebas por la debilidad en la cadena de custodia.	Forense digital

Fuente: Elaborado por García. L. y Gavilanes. J.

5.2 Análisis y discusión de resultados

Los resultados obtenidos en esta investigación nos permiten evidenciar aspectos relevantes en torno al fenómeno de la suplantación de identidad mediante inteligencia artificial deepfake. Las respuestas y criterios recogidos reflejan la trascendencia del problema dentro del ámbito jurídico. Los profesionales entrevistados, entre ellos, fiscales, abogados y fuerza

pública, expresan sus posturas acerca de las limitaciones existentes ante la insuficiencia de la norma frente los delitos cometidos mediante el uso de las nuevas tecnologías.

5.2.1 Percepción y conocimiento del deepfake como mecanismo de suplantación de identidad.

En la entrevista realizada, la primera pregunta refiere acerca del conocimiento y percepción del uso del deepfakes en el delito de suplantación de identidad, en la cual se evidencia que los hallazgos del estudio realizado reconocen a esta tecnología como una herramienta para clonar y modificar voces, imágenes y videos. Cuatro de los cinco entrevistados manifiestan haber observado este tipo de contenido reconociendo su carácter hiperrealista, Tabla 1, este resultado permite inferir que el deepfake no se mantiene en hipótesis o una posibilidad teórica, sino que se ha convertido en una realidad que vulnera al contexto social y jurídico actual.

El levantamiento de la información dentro de esta pregunta identifica que 4 de los 5 entrevistados señalan conocer casos en donde se ha suplantado la identidad a través del uso de inteligencia artificial. El caso reportado por el entrevistado 002 menciona que se abre un proceso por suplantación de identidad, un caso que, a pesar de ser cometido con el uso de inteligencia artificial, el tipo penal fue cambiado por falsificación y uso de documento falso. El entrevistado 002 en la entrevista menciona que la suplantación de identidad es el medio para llegar a un fin, por lo cual, es solo un delito menor que tiene por consecuencia un delito mayor, es decir, se ejerce el delito de suplantación de identidad para cometer una estafa, y en este caso se sanciona la estafa mas no el delito inicial.

En contraste al consultado 002, el entrevistado 004 menciona que estos casos se incrementan a nivel exponencial y el hecho de no proteger la identidad digital como un bien jurídico protegido, provoca impunidad en las victimas. Con su testimonio establece un punto crítico sobre la falta de protección a los derechos individuales y también el incremento de la brecha al acceso a la justicia, porque según la experiencia de este profesional alude que la identificación de la responsabilidad penal ante estos hechos suele depender de los recursos económicos y técnicos que tienen a su alcance cada persona, como el testimonio que refiere anteriormente donde se ve involucrado un funcionario público.

En la perspectiva doctrinaria la IA tiene la facilidad de replicar rasgos biográficos con precisión y con el deepfake esta tiene la capacidad para expropiarse digitalmente de la efigie de una persona, lo que la constituye como una forma avanzada de suplantación de identidad. Autores como Chesney y Citron (2019) sostienen que el deepfake es una nueva forma de manipulación digital que realiza representaciones falsas, donde engañan a personas e instituciones, se confirma este tipo de hechos con el caso mencionado por el sujeto 002 porque los suplantadores lograron engañar a la institución para obtener la firma electrónica.

La Constitución en su artículo 66 numeral 28 garantiza el derecho a la identidad, constituyéndola como un atributo esencial de la personalidad, se considera su protección indispensable para garantizar el respeto a la dignidad humana. El uso del deepfake como mecanismo de suplantación de identidad constituye una vulneración directa al derecho fundamental y genera consecuencias jurídicas que afectan la vida y la honra de las personas, además refleja un vacío normativo respecto a identidad digital.

Los hallazgos encontrados, ocasionan un impacto en la investigación, puesto que, se corrobora que el contenido generado con inteligencia artificial es una realidad fáctica, demuestra que existen anomalías e insuficiencia en el marco jurídico, porque, no se protege como tal la identidad de la persona, ni mucho menos se protege su privacidad y sus derechos que son fundamentales, esto evidencia el potencial que tiene la inteligencia artificial o deepfake para ser un instrumento útil en la comisión de delitos y este produce un incremento del mismo.

5.2.2 Insuficiencia del marco jurídico ecuatoriano frente la suplantación de identidad mediante inteligencia artificial

Dentro de la segunda y quinta pregunta, los entrevistados manifiestan y coinciden que el artículo 212 del Código Orgánico Integral Penal es insuficiente para regular los delitos de suplantación de identidad que son generados y cometidos mediante inteligencia artificial, en razón a esta premisa los profesionales manifiestan que deberían estipularse o expandirse el artículo a través de numerales que especifiquen y tipifiquen los delitos que podrán ser cometidos por inteligencia artificial o el uso de nuevas tecnologías.

La necesidad de modificar el artículo 212 del COIP, se vuelve fundamental, debido a que surge un nuevo término, identidad digital, así lo menciona Calterio (2022) que la identidad digital es una nueva forma de identificación, que a pesar de no estar admitida como un término jurídico la función del Estado es protegerla, así el derecho de identidad estipulado en la Constitución en su artículo 66 numeral 28 no recae solamente en la cultura, grupo social o etnia, sino también el ciberespacio, un lugar sin tipificación de norma y con libertad para delinquir. La Constitución de la República del Ecuador del 2008 en su artículo 76 numeral 3 menciona que nadie podrá ser juzgado ni sancionado si no se encuentra tipificada la acción como infracción penal o delito. Este principio estipulado en la norma es una garantía fundamental para limitar el poder punitivo del Estado y garantizar la seguridad jurídica de los ciudadanos, no obstante, un punto medular de la investigación realizada en base a las entrevistas, si revisamos la Tabla 2, observamos que la norma vigente padece una atipicidad relativa, esto en razón de que la descripción típica del delito no contempla la manipulación digital de los datos biográficos, por lo que los operadores de justicia deben subsumir a otros tipos penales análogos y esta práctica contravine el principio de legalidad y el principio de tipicidad que se encuentran establecidos en la Constitución.

Miro linares (2012) en su libro menciona las distintas formas de criminalidad en el ciberespacio y como cada una de estas se posiciona en el mundo digital, lo que motiva a los Estados a tomar medidas. Sin embargo, el resultado obtenido en la Tabla 5 sobre los impactos que genera la insuficiencia del marco legal refleja que los factores que producen un incremento en la criminalidad se encuentra la impunidad, la ausencia de prevención, desactualización normativa, vacío normativo y diferentes líneas de investigación. En ese sentido, la insuficiencia de la norma limita la capacidad penal para sancionar las conductas.

5.2.3 Determinación de la responsabilidad penal en delitos cometidos mediante deepfake

La determinación de la responsabilidad del delito es fundamental para llevar a cabo el proceso de juzgamiento, por lo cual el autor material del hecho será sancionado por el acto doloso cometido. Dicho esto, los entrevistados en cuanto a la pregunta que refiere acerca de la responsabilidad penal, Tabla 3, que tendrán los actores, cómplices, coautores, quienes financian o difunden el contenido realizado con inteligencia artificial que vulnera los derechos de una persona, concuerdan que la responsabilidad penal recae en todos no solo en el autor material, esta debe extenderse a quienes son partícipes de la planificación, creación, financiamiento o facilitación del delito.

No obstante, por los resultado obtenidos en la Tabla 7, identificamos obstáculos que frenan las investigaciones al momento de determinar la responsabilidad penal de los creadores del contenido, especialmente cuando utilizan herramientas especiales y tecnológicamente avanzadas en donde modifican y suplantán la identidad de las mismas computadoras a través del hackeo de los IP de los ordenadores para que no sea posible determinar su dirección, esto es lo que menciona el entrevistado 004 experto en ciberdefensa del ejército ecuatoriano y concuerda con Miro Linares (2012), el autor señala que la deslocalización en cibercrimen es una de las principales características para no encontrar al autor material del hecho, y con ello dificulta la determinación de la jurisdicción y competencia para sancionar el acto.

En base a la responsabilidad penal, determina que los artículos 41, 42 y 43 de Código Orgánico Integral Penal (2014), se establece el grado de participación que tendrían las personas al momento de cometer un delito, en el caso de la suplantación de identidad por el simple hecho de ser partícipe conlleva una responsabilidad penal, dentro de la misma existe el autor y el coautor, la norma establece, que no se afectará a los demás partícipes si existen condiciones que limiten o agravan la responsabilidad, sin embargo, no se dispensa de la misma. El artículo 43 del (COIP, 2014) manifiesta, que se considera cómplice a toda persona que participe de forma dolosa, faciliten o cooperen en el acto, es decir, que todos aquellos que financian o facilitan el contenido realizado con Inteligencia artificial se vuelve cómplice del autor material del hecho. La ley es expresa el desconocimiento de la ley no exime de la responsabilidad ni justifica su incumplimiento.

Por su parte, en el ámbito constitucional en el artículo 75 de la Constitución de la Republica del Ecuador, se reconoce el derecho a la tutela judicial efectiva en donde el estado garantiza que las personas acceden a los mecanismos necesarios para protección de sus derechos, a pesar de ello, el estado no cuenta con los medios efectivos para investigar a cabalidad los hechos y sancionar a los partícipes del delito. En razón a este tipo de circunstancias, tanto fiscales como profesionales expertos en el tema de ciberdefensa refieren que es necesaria la ayuda internacional para poder lograr un avance en cuanto a las nuevas tecnologías, así también, se podrá capacitar a los operadores de justicia para que ejerzan su función de manera adecuada y asegurar la protección del ciudadano en un entorno digital.

5.2.4 Limitaciones frente a los delitos cometidos mediante inteligencia artificial

La Tabla 4 y 7 muestran los resultados obtenidos durante las entrevistas realizadas, las mismas esclarecen importantes hechos dentro del sistema jurídico ecuatoriano, debido a, que se desglosan diversas limitaciones normativas, institucionales y probatorias frente a los delitos que son cometidos mediante el uso de nuevas tecnologías o inteligencia artificial.

Dentro de la Tabla 4 podemos ver ciertos mecanismos que tienen las instituciones para actuar en casos de delitos cibernéticos, de los cuales se encuentran el Departamento de Ciberdelitos de la Policía, La Ley de Protección de Datos Personales, daño moral según el código Civil art. 2232, sin embargo, se identifica un desconocimiento parcial de los profesionales acerca la normativa legal vigente en relación a los ciberdelitos, si bien nos mencionan regulación específica como lo es la Ley Orgánica de Protección de Datos personales y mecanismos utilizados dentro de las instituciones de la Policía Nacional, estos resultan ser ineficientes para abordar de manera integral el delito de suplantación de identidad mediante inteligencia artificial deepfake desde una perspectiva sancionatoria.

En el desglose de la investigación, se reconoce distintos tipos de norma que consagra la dignidad del ciudadano ante las nuevas tecnologías, uno de estos es la Convención Americana de Derechos Humanos, el cual, en su artículo 11 reconoce el derecho a la honra y la protección de injerencia o arbitraje por parte del Estado, este funciona como fundamento para exigir la modernización de los marcos normativos penales, concuerda con Sánchez, quien en su libro Aproximación al Derecho Penal, manifiesta que, para un mejor desarrollo del derecho penal, se tendrá una perspectiva resocializadora, en donde, se protege a la sociedad mediante la prevención de delitos, que se podrán cometer a futuro (Sánchez, 1992).

Por otra parte, La Declaración Universal de Derechos Humanos refiere acerca de los límites éticos del desarrollo científico, si bien esta normativa no fue creada para regular la identidad digital ni mucho menos para regular la suplantación de identidad mediante inteligencia artificial, la misma ofrece una guía para proteger la identidad y los derechos ante el incremento de la tecnología.

La Ley Orgánica de Protección de Datos Personales es la base para proteger el derecho a la privacidad en el país, sin embargo, la misma protege los datos personales, que se encuentran en las instituciones públicas o privadas, es decir, esta ley protege el dato mas no la identidad. En el caso del deepfake se vulnera la identidad y a pesar de la existencia de esta ley no es suficiente para tartar la suplantación, en cuanto a sus sanciones son de carácter administrativo mas no penales. En consecuencia, esta normativa no proporciona una respuesta adecuada para un tratamiento penal ante las nuevas formas de criminalidad tecnológica, lo que evidencia la necesidad de una norma específica, que se derive del artículo 212 del COIP.

A su vez, dentro de las limitaciones presentadas por parte de los entrevistados mencionan, la falta de recursos por parte del Estado para invertir en nuevas tecnologías que identifiquen este tipo de hechos y permitan una investigación clara y precisa, así mismo, las instituciones públicas como fiscalía no tiene los instrumentos necesarios. La infraestructura y los profesionales especializados para resolver el hecho presentado como un delito que, a

pesar de, que no se encuentre tipificado en la norma afecta a la sociedad y vulnera sus derechos fundamentales establecidos legamente en la constitución.

A causa de las limitaciones, se distinguen distintos retos probatorios al momento de demostrar la autenticidad del contenido digital para establecer una responsabilidad específica, porque los contenidos digitales son modificados, esto menciona uno de los entrevistados en Tabla 7 en base a la pregunta acerca de los retos probatorios que trae consigo el incremento de la tecnología y su aplicabilidad en la forma de delinquir, lo que concuerda con la investigación realizada en este trabajo.

5.2.5 Responsabilidad del Estado y necesidad de fortalecimiento del marco jurídico

El estudio realizado en las entrevistas y en base a la Tabla 6 de los resultados, 2 entrevistados refieren que el Estado no podría asumir responsabilidad porque no existe una norma tipificada, consideran que es necesaria la reforma o modificación de la misma ante el aumento acelerado de la tecnología y el uso de nuevos instrumentos como la inteligencia artificial, no obstante, manifiestan que la posición del Estado no es la adecuada para poder dar solución. Sostienen que a pesar de esta ley y de la reforma del artículo 212 del COIP, se necesitaran insumos, infraestructura y recursos que el Estado no solventa en este momento, la idea de reformar las nuevas tecnologías debería basarse en la realidad del país, y tomar medidas en crecimiento para fortalecer poco a poco al sistema jurídico ecuatoriano.

Uno de los entrevistados menciona que este tipo de delitos quedaran solo en una recepción de denuncia y se archivara la causa, en casos más graves podrá llevarse a cabo bajo un procedimiento abreviado o también dadas las circunstancias, para evitar cualquier tipo de situación donde se perjudique la honra mutuamente, lo usual es llegar a un acuerdo entre las partes y dar por concluida la causa, en otra palabras, no hay proceso ni tampoco el Estado tendría una responsabilidad ante este tipo de situaciones.

Contrario a lo mencionado anteriormente, en el artículo 11 numeral 9 de la Constitución de la Republica del Ecuador manifiesta, que el Estado tendrá el deber de respetar y hacer respetar los derechos garantizados en la constitución, mientras que en su inciso 3 refiere que el Estado será responsable por cualquier violación, retardo, error judicial, inadecuada administración, entre otros. En síntesis, la responsabilidad del estado es proteger y hacer cumplir los derechos, al existir un dinamismo en la sociedad y un acelerado crecimiento tecnológico donde los delincuentes han visto un punto de inflexión para introducir un nuevo tipo de criminalidad, el Estado al no intervenir genera anomias en su norma.

En este sentido, la responsabilidad del Estado frente a los ciudadanos que son víctimas de estos tipos de delitos es proteger al bien jurídico, su deber es tutelar el goce efectivo de los derechos de las personas, sin embargo, se evidencia que el Estado enfrenta limitantes para cumplir eficazmente con su función.

Finalmente, estos enfoques analizados y discutidos se desarrollaron en base al paradigma del realismo-jurídico y post-positivismo, debido a que el tema investigado es un tema que afecta a la sociedad actual.

CAPÍTULO V.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

El deepfake es una forma de edición digital que trasciende de modalidad al punto de realizar una apropiación biométrica clonando con precisión la efigie y la voz humana, el hiperrealismo de esta tecnología compromete la identidad del ser humano creando versiones sintéticas de una persona capaces de engañar a instituciones como a personas naturales, por tanto evidenciamos que su conexión con la suplantación de identidad es intrínseca y directa, debido a que el deepfake funciona como instrumento para usurpar la personalidad en el ciberespacio vulnerando el derecho fundamental de la identidad consagrado en la constitución.

Los elementos de nuestra investigación nos permite concluir en que el artículo 212 dentro del marco jurídico penal ecuatoriano está incompleto, esto en razón de que la actual tipificación no contempla el componente tecnológico de la inteligencia artificial provocando una atipicidad relativa, esta laguna legal permite que los operadores de justicia tomen decisiones análogas, diluyendo la gravedad de la afectación a la identidad y limita al poder punitivo del Estado frente las nuevas formas de criminalidad.

En conclusión, el impacto social que genera la necesidad de tipificar el uso de IA en el cometimiento de delitos radica en las experiencias de las víctimas al no recibir una ayuda oportuna por parte de la justicia, esto en razón al evidente vacío legal de la norma y ante las brechas económicas existentes por parte del Estado, así mismo, la evidente ausencia de mecanismos procesales claros vulnera el derecho de las personas privándoles de su derecho a la integridad y su honra.

Finalmente, la investigación a profundidad realizada revela en sus resultados que la insuficiencia del marco jurídico penal contribuye de manera significativa al aumento de los casos de suplantación de identidad mediante inteligencia artificial en el país. Este problema se manifiesta a través de anomias que crean un entorno propicio para estas conductas, al minimizar la percepción del riesgo por parte de la población, debido a la falta de sanciones específicas previstas en el Código Orgánico Integral Penal. La ausencia de una tipificación precisa no solo debilita el efecto preventivo del derecho penal, sino que también obstaculiza la labor de investigación y persecución de la Fiscalía y la Policía Nacional. El resultado es un sistema de protección insuficiente que favorece el desarrollo de la ciberdelincuencia, alimentado por el retraso y la escasa adaptación del sistema jurídico ante los avances tecnológicos.

6.2 Recomendaciones

Se recomienda integrar en la normativa penal y constitucional apartados específicos que reconozcan el deepfake como problema creciente que afecta a la identidad y a la honra los cuales son bienes jurídicos protegidos por el Estado. Y con ello evitar la vulneración de los derechos fundamentales y la disminución de riesgo ante las nuevas amenazas presentadas por la Inteligencia Artificial

Se recomienda realizar un proceso de reforma al artículo 212 del COIP, en el cual se establezcan numerales específicos que sancionen la suplantación de identidad mediante Inteligencia artificial, Deepfake o cualquier otro mecanismo tecnológico, así también que sugiere establecer agravantes constitutivos de la infracción, cuando el delito sea en contra de grupos de atención prioritaria, extorción y fraude bancario.

Se recomienda al Ministerio de Telecomunicaciones hacer campañas de alfabetización digital y ciberseguridad para que tanto niños, jóvenes y adultos identifiquen riesgos del uso compartido de datos biométricos, comprendiendo que el deepfake es de carácter hiperrealista, el cual clona la biometría de las imágenes que subimos a redes sociales para comprometer nuestra identidad, nuestra honra y nuestros datos ante un público desconocido.

Se recomienda a la Fiscalía General del Estado y al Consejo de la Judicatura la creación y fortalecimiento de las unidades periciales con profesionales forenses digitales, además es necesario asignar un presupuesto específico con la finalidad de capacitar constantemente a los investigadores. Además realizar capacitaciones con el cuerpo legislativo nacional e internacional en contra de la ciberdelincuencia, siendo así sus principales capacitados fiscalía, y fortalecer los tratados de asistencia mutua, fomentar una colaboración para que los contenidos falsos sean detectados y eliminados rápidamente, así se fortalecerá nuestra resiliencia como sociedad, pero para obtener resultados deseados se tendrá que concientizar a la comunidad y explicar que es, de qué forma puede afectar a las personas el deepfake, y cuales los límites que este contempla.

BIBLIOGRAFÍA

- Anónimo. (2018). *CIBERCRIMEN Y DELITOS: Los nuevos tipos penales en la era de internet / compilado por Ricardo Antonio*. Ciudad Autónoma de Buenos Aires: Erreius.
- Anónimo. (2021). *SISTEMATIZACIÓN DEL CURSO VIRTUAL CIBERDELINCUENCIA/ CURSO LA CIBERDELINCUENCIA: TRATAMIENTO PREVENTIVO, PROCESAL Y SUSTANTIVO DESDE UNA PERSPECTIVA INTERNACIONAL*.
- Atencio, A. B. (2025). Inteligencia artificial y ciberdelincuencia: amenazas emergentes para la infancia y adolescencia en la era de los deepfakes? *Brújula. Semilleros de Investigación*, Volumen 13, Número 25, enero-junio, pp. 16-33.
- Bauman, Z. (2005). *Identidad*. Buenos Aires, Argentina : Editorial Losada, J. Sarasola, Daniel, trad. II. Título CDD 190.
- CALETRÍO, A. B. (2022). El Derecho a la identidad y la identidad digital. *Estudios Monográficos*, ADC, tomo LXXV, 2022, fasc. III (julio-septiembre), pp. 923-986.
- Castells, M. (2001). *LA ERA DE LA INFORMACION: Economía, sociedad y Cultura Volumen II: El poder de la identidad*. Buenos Aires Argentina : siglo xxi editores, s.a. de c.v - tercera edición en español, 2001.
- CHILAN, K. B., & PÁRRAGA, A. I. (2020). *LA SUPLANTACIÓN DE IDENTIDAD ELECTRÓNICA A TRAVÉS DE SITIOS WEB COMO DELITO INFORMÁTICO EN EL ECUADOR*.
- Código Orgánico Integral Penal. (2014). *[COIP] Registro Oficial Suplemento No. 180*.
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). *Asamblea Nacional Constituyente* .
Registro Oficial No. 449.
- Convención Americana sobre Derechos Humanos. (1969). *CADH*. Obtenido de https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf
- Declaración Universal sobre Bioética y Derechos Humanos. (2005). *UNESCO. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura*.
Obtenido de <https://rionegro.gov.ar/download/archivos/00007497.pdf>
- Dirección de Ciberdelitos Ministerio del Interior. (diciembre de 2024). *Boletín de Análisis de la Ciberdelincuencia: La nueva era de la ciberdelincuencia, el lado oscuro de la*

- Inteligencia Artificial*. Obtenido de <https://www.ministeriodelinterior.gob.ec/wp-content/uploads/downloads/2025/07/Boletin-La-nueva-era-de-la-ciberdelincuencia-el-lado-oscuro-de-la-Inteligencia-Artificial.pdf>
- Durán, R. L. (2002). *Metodología jurídica*. México: IURE Editores.
- Fernandes, A., Fernández, D., Molero, D., & Pérez, M. Á. (2025). *DEEPFAKES: RIESGOS, CASOS REALES Y DESAFÍOS EN LA ERA DE LA IA*. Obtenido de ISMS FORUM: <https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf>
- Fundación Telefónica. (2013). *Identidad Digital: El nuevo usuario en el mundo digital*. Barcelona España: © Editorial Ariel, S.A.
- Gebremeskel, B. (20 de june de 2025). *Deepfakes and Phishing in the AI Age*. Obtenido de TeckPath: <https://teckpath.com/deepfakes-phishing-ai-threats-2025/>
- González, S. C. (9 de febrero de 2015). *Castellano Actual*. Obtenido de Suplir y suplantar: <https://www.udep.edu.pe/castellanoactual/suplir-y-suplantar/>
- Guaycha, C. F. (2025). La Suplantación de Identidad Digital en el COIP: Análisis Jurídico de las Dificultades de Aplicación y su Impacto en el Derecho a la Tutela Judicial Efectiva de las Víctimas en Ecuador. *Polo del Conocimiento Ciencias Sociales y Políticas Artículo de Investigación* , Pol. Con. (Edición núm. 111) Vol. 10, No 10 Octubre 2025, pp. 264-284.
- Guerrero, D. A. (2025). *La Inteligencia Artificial utilizada como herramienta en el delito de suplantación de identidad: Consideraciones para su tipificación dentro del Derecho Penal en el Ecuador*. Obtenido de file:///C:/Users/user/Downloads/FJCPS-CD-DAVID%20ALEJANDRO%20ROSERO%20GUERRERO.pdf
- INCEBE. (s.f.). *Suplantación de identidad*. Obtenido de Instituto Nacional de Ciberseguridad: <https://www.incibe.es/ciudadania/tematicas/virus-amenazas/suplantacion-de-identidad>
- Karla, P. M. (2023). *SUPLANTACIÓN DE IDENTIDAD EN LAS REDES SOCIALES EN LA CIUDAD DE BABAHOYO EN 2023*. Obtenido de file:///C:/Users/user/OneDrive%20-%20Universidad%20Nacional%20de%20Chimborazo/Escritorio/titulacion/tesis/U A-DER-PDI-017-2023.pdf
- content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
- Ley Orgánica de Protección de Datos Personales. (2021). *Asamblea Nacional*. Registro Oficial Suplemento No. 459.

- Liceda, E. (2011). La identidad digital. *ANALES N° 41 - Facultad de Cs. Jurídicas y Sociales. U.n.l.p.*, 296-304.
- Llinares, F. M. (2012). *El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Ediciones jurídicas y sociales, s. a.
- López, I. R. (30 de abril de 2024). *IDENTIDAD DIGITAL DESCENTRALIZADA: ¿LEAPFROGGING DIGITAL EN ECUADOR?* Obtenido de <https://www.usfq.edu.ec/sites/default/files/2024-04/identidad-digital-descentralizada-leapfrogging-digital-en-ecuador-comp.pdf?itok=dZLA0jnqBz>
- López-Roldán, P., & Fachelli, S. (2015). *METODOLOGÍA DE LA INVESTIGACIÓN SOCIAL CUANTITATIVA*. Barcelona - España: Edición digital: <http://ddd.uab.cat/record/129382>.
- Macías-Lara, R. A., Bedoya-Benavides, J. O., Orbea, J. C., Vivero, G. N., & Angulo, R. M. (2014). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales. *Revista Científica Multidisciplinar G-NERANDO*, V°5 (N°1), 544 -561.
- Maldonado, D. B. (2020). *Los bárbaros jurídicos: Identidad, derecho comparado moderno y el Sur global*. Siglo del Hombre Editores.
- Miro Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología*. San Sotero Madrid: marcial pons ediciones jurídicas y sociales, s. a.
- Navarro, M. (2023). *LOS CONCEPTOS, LAS VARIABLES Y LA MEDICIÓN EN LA INVESTIGACIÓN SOCIAL CUANTITATIVA*. Obtenido de ORKESTRA WORKING PAPER SERIES IN TERRITORIAL COMPETITIVENESS: <https://www.orquestra.deusto.es/images/investigacion/publicaciones/articulos-cientificos/orkestra-working-papers/230054-conceptos-variables-medicion-investigacion-social-cuantitativa.pdf>
- Noriega, J. Á., & Medina, J. E. (2012). El concepto de identidad como recurso para el estudio de transiciones. *Psicología e Sociedade*, 11.
- Odar, R. M. (2016). TIPOLOGÍA DE LAS INVESTIGACIONES JURÍDICAS. *Derecho y Cambio Social*, 4-18.
- Oliva, M. L. (2022). Deepfake: Cuando la inteligencia artificial amenaza el Derecho y la Democracia. *Lawgic Tec - Revista de Derecho y Tecnología*, 84-95.
- Real Academia Española. (2025). *Diccionario de la lengua española*. 23.^a ed., [versión 23.8.1 en línea]. <<https://dle.rae.es>.

- ROMERO, M. M., LEÓN, R. R., HOCES, W. B., CARRASCO, R. L., CARRANZA, C. M., & ACOBO, R. C. (2023). *Metodología de la investigación: Técnicas e instrumentos de investigación*. Puno-Perú: Editorial: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.
- Ruiz, J. F. (2011). *Derecho administrativo y administración pública*. México: Porrúa .
- Sampieri, R. H. (2014). *Metodología de la Investigación* . Santa Fe: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.
- Sánchez, J.-M. S. (1992). *Aproximación al derecho penal contemporáneo*. Barcelona: Jose Maria Bosch, <https://es.scribd.com/document/333584145/Aproximacion-Al-Derecho-Penal-Contemporaneo-Jesus-Maria-Silva-Sanchez>.
- Singh, S. S. (2024). *SIGNIFICADO DE LA HIPÓTESIS EN LA INVESTIGACIÓN JURÍDICA*. Obtenido de Revista Internacional de Investigación Avanzada (IJAR): <https://www.journalijar.com/article/49065/significance-of-hypothesis-in-legal-research/>
- Tipanguano-Chicaiza, L. G., Barreno-Sailema, S. N., Mejía-Toscano, N. d., & Urrutia-Guevara, J. A. (2024). La Inteligencia Artificial en el Ecuador, tipificación, desafíos y perspectivas. *Revista Arbitrada de Ciencias Jurídicas y Sociales*, 259-265.
- Torres, K. N., & Ruiz, J. E. (2024). *UNIVERSIDAD ECOTEC*. Obtenido de file:///C:/Users/user/OneDrive%20-%20Universidad%20Nacional%20de%20Chimborazo/Escritorio/titulacion/tesis/CE DE%C3%91O%20TORRES-%20RUIZ%20RUIZ.pdf
- Valera, V. (23 de May de 2025). *La evolución de la Inteligencia Artificial (IA)*. Obtenido de RQR: <https://www.rqrcom.com/la-evolucion-de-la-inteligencia-artificial-ia/>
- Vega Noriega, J., & Valenzuela Medina, J. (2012). EL CONCEPTO DE IDENTIDAD COMO RECURSO PARA EL ESTUDIO DE TRANSICIONES. *Psicología & Sociedad* , 24 (2), 272-282.
- VELOZ, T. M., & NARANJO, V. H. (2025). *Delitos informáticos: un análisis jurídico integral de las amenazas en el entorno digital*. Obtenido de file:///C:/Users/user/OneDrive%20-%20Universidad%20Nacional%20de%20Chimborazo/Escritorio/titulacion/tesis/UP S-GT006266.pdf

ANEXOS



Dirección
Académica
VICERRECTORADO ACADÉMICO



UNACH-RGF-01-04-08.04
VERSIÓN 01: 06-09-2021



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de Investigación: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco normativo penal en Ecuador.

Investigadoras: Leslie Estefanía García Mosquera y Joselyn Jemima Gavilanes Viteri

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se le invita cordialmente a participar como informante en una entrevista realizada en el marco de un proyecto académico sobre la respuesta del sistema penal ecuatoriano ante los casos de suplantación de identidad digital generada mediante tecnologías de inteligencia artificial (IA), especialmente deepfakes. El propósito de este estudio es obtener criterios profesionales y empíricos sobre la eficacia, limitaciones y vacíos existentes en la normativa penal actual para enfrentar este tipo de ciberdelitos emergentes.

- La entrevista podrá ser grabada únicamente con fines de análisis académico.
- Toda la información proporcionada será tratada con estricta confidencialidad y solo se utilizará para los fines de esta investigación.
- Su participación es completamente voluntaria y puede retirarse en cualquier momento sin consecuencia alguna.
- Los resultados se emplearán exclusivamente con fines investigativos y académicos.

Declaro que he sido informado/a adecuada y claramente sobre los objetivos y condiciones del estudio, y doy mi consentimiento libre para participar en esta entrevista.

Firma:

Nombre del entrevistado:

ANA CALDERON MACHADO

Fecha: 26 ENERO 2020.



Dirección
Académica
VICERRECTORADO ACADÉMICO

en movimiento



UNACH-RGF-01-04-08.04
VERSIÓN 01: 06-09-2021



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal.

Investigadoras: Leslie Estefanía García Mosquera y Joselyn Jemima Gavilanes Viteri

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se le invita cordialmente a participar como informante en una entrevista realizada en el marco de un proyecto académico sobre la respuesta del sistema penal ecuatoriano ante los casos de suplantación de identidad digital generada mediante tecnologías de inteligencia artificial (IA), especialmente deepfakes. El propósito de este estudio es obtener criterios profesionales y empíricos sobre la eficacia, limitaciones y vacíos existentes en la normativa penal actual para enfrentar este tipo de ciberdelitos emergentes.

- La entrevista podrá ser grabada únicamente con fines de análisis académico.
- Toda la información proporcionada será tratada con estricta confidencialidad y solo se utilizará para los fines de esta investigación.
- Su participación es completamente voluntaria y puede retirarse en cualquier momento sin consecuencia alguna.
- Los resultados se emplearán exclusivamente con fines investigativos y académicos.

Declaro que he sido informado/a adecuada y claramente sobre los objetivos y condiciones del estudio, y doy mi consentimiento libre para participar en esta entrevista.

Firma:

Nombre del entrevistado: SILVANA VALERIA DONOSO ESTRADA

Fecha: 22/ENERO/2026



Dirección
Académica
VICERRECTORADO ACADÉMICO



UNACH-RGF-01-04-08.04
VERSIÓN 01: 06-09-2021



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco jurídico Penal.

Investigadoras: Leslie Estefanía García Mosquera y Joselyn Jemima Gavilanes Viteri

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se le invita cordialmente a participar como informante en una entrevista realizada en el marco de un proyecto académico sobre la respuesta del sistema penal ecuatoriano ante los casos de suplantación de identidad digital generada mediante tecnologías de inteligencia artificial (IA), especialmente deepfakes. El propósito de este estudio es obtener criterios profesionales y empíricos sobre la eficacia, limitaciones y vacíos existentes en la normativa penal actual para enfrentar este tipo de ciberdelitos emergentes.

- La entrevista podrá ser grabada únicamente con fines de análisis académico.
- Toda la información proporcionada será tratada con estricta confidencialidad y solo se utilizará para los fines de esta investigación.
- Su participación es completamente voluntaria y puede retirarse en cualquier momento sin consecuencia alguna.
- Los resultados se emplearán exclusivamente con fines investigativos y académicos.

Declaro que he sido informado/a adecuada y claramente sobre los objetivos y condiciones del estudio, y doy mi consentimiento libre para participar en esta entrevista.

Firma: 
Nombre del entrevistado: 
Fecha: 22 / 01 / 2026



Dirección
Académica
VICERRECTORADO ACADÉMICO

en movimiento



UNACH-RGF-01-04-08.04
VERSIÓN 01: 06-09-2021



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de investigación: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco normativo penal en Ecuador.

Investigadoras: Leslie Estefanía García Mosquera y Joselyn Jemima Gavilanes Viteri

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se le invita cordialmente a participar como informante en una entrevista realizada en el marco de un proyecto académico sobre la respuesta del sistema penal ecuatoriano ante los casos de suplantación de identidad digital generada mediante tecnologías de inteligencia artificial (IA), especialmente deepfakes. El propósito de este estudio es obtener criterios profesionales y empíricos sobre la eficacia, limitaciones y vacíos existentes en la normativa penal actual para enfrentar este tipo de ciberdelitos emergentes.

- La entrevista podrá ser grabada únicamente con fines de análisis académico.
- Toda la información proporcionada será tratada con estricta confidencialidad y solo se utilizará para los fines de esta investigación.
- Su participación es completamente voluntaria y puede retirarse en cualquier momento sin consecuencia alguna.
- Los resultados se emplearán exclusivamente con fines investigativos y académicos.

Declaro que he sido informado/a adecuada y claramente sobre los objetivos y condiciones del estudio, y doy mi consentimiento libre para participar en esta entrevista.

Firma:

Firma manuscrita

Nombre del entrevistado:

Friedel Delgado

Fecha: 16-01-2026



Dirección
Académica
VICERRECTORADO ACADÉMICO

en movimiento



UNACH-RGF-01-04-08.04
VERSIÓN 01: 06-09-2021



CONSENTIMIENTO INFORMADO

UNIVERSIDAD NACIONAL DE CHIMBORAZO – CARRERA DE DERECHO

Proyecto de Investigación: La suplantación de identidad mediante inteligencia artificial y la insuficiencia del marco normativo penal en Ecuador.

Investigadoras: Leslie Estefanía García Mosquera y Joselyn Jemima Gavilanes Viteri

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES

Se le invita cordialmente a participar como informante en una entrevista realizada en el marco de un proyecto académico sobre la respuesta del sistema penal ecuatoriano ante los casos de suplantación de identidad digital generada mediante tecnologías de inteligencia artificial (IA), especialmente deepfakes. El propósito de este estudio es obtener criterios profesionales y empíricos sobre la eficacia, limitaciones y vacíos existentes en la normativa penal actual para enfrentar este tipo de ciberdelitos emergentes.

- La entrevista podrá ser grabada únicamente con fines de análisis académico.
- Toda la información proporcionada será tratada con estricta confidencialidad y solo se utilizará para los fines de esta investigación.
- Su participación es completamente voluntaria y puede retirarse en cualquier momento sin consecuencia alguna.
- Los resultados se emplearán exclusivamente con fines investigativos y académicos.

Declaro que he sido informado/a adecuada y claramente sobre los objetivos y condiciones del estudio, y doy mi consentimiento libre para participar en esta entrevista.

Firma:

Nombre del entrevistado:

Fecha:

[Firma manuscrita]
Graciela Guerrero Jiménez
16 de enero 2026

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: Wendy Romero

Especialidad: Derecho Penal y Procesal Penal

Título de la investigación: La suplantación de identidad mediante Inteligencia Artificial y la Insuficiencia del Marco Jurídico Penal

Objetivo del instrumento (Que pretende medir): Analizar la incidencia de la inteligencia artificial en el tipo penal de suplantación de identidad y determinar de qué manera esta tecnología genera insuficiencia del marco normativo penal ecuatoriano a través de la interpretación de la norma y el análisis crítico doctrinario.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún ítem)
	SI	No	SI	No	SI	No	SI	No	Esencial	Util pero no esencial	No importante	
1	✓		✓			✓		✓	✓			
2	✓		✓			✓		✓	✓			
3	✓		✓			✓		✓	✓			
4	✓		✓			✓		✓	✓			
5	✓		✓			✓		✓	✓			
6	✓		✓			✓		✓	✓			
7	✓		✓			✓		✓	✓			

Firma de Validador

Nombre: Wendy Romero

Cédula: 0604453569

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: *Nelson Fari*

Especialidad: *Decido Penal y Criminología*

Título de la investigación: La suplantación de Identidad mediante Inteligencia Artificial y la Insuficiencia del Marco Jurídico Penal

Objetivo del instrumento (Que pretende medir): Analizar la incidencia de la inteligencia artificial en el tipo penal de suplantación de identidad y determinar de qué manera esta tecnología genera insuficiencia del marco normativo penal ecuatoriano a través de la interpretación de la norma y el análisis crítico doctrinario.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún ítem)
	Si	No	Si	No	Si	No	Si	No	Esencial	Util pero no esencial	No Importante	
1	☒						☒		☒			
2	☒						☒		☒			
3	☒						☒		☒			
4	☒						☒		☒			
5	☒						☒		☒			
6	☒						☒		☒			
7	☒						☒		☒			

Firma de Validador: *[Firma]*

Nombre: *Franz Fari*

Cédula: *0602469991*

MATRIZ DE VALIDACION DE INSTRUMENTOS POR ESPECIALISTAS

Nombre de Especialista Validador: ROSITA CARRUZZANO

Especialidad: Derecho Penal

Título de la investigación: La suplantación de Identidad mediante Inteligencia Artificial y la Insuficiencia del Marco Jurídico Penal

Objetivo del instrumento (Que pretende medir): Analizar la incidencia de la inteligencia artificial en el tipo penal de suplantación de identidad y determinar de qué manera esta tecnología genera insuficiencia del marco normativo penal ecuatoriano a través de la interpretación de la norma y el análisis crítico doctrinario.

Preguntas	Claridad en la redacción		Coherencia interna		Introducción a la respuesta (Sesgo)		Pertinencia		Calificación de las preguntas			Observaciones (Por favor indique si debe eliminarse o modificar algún ítem)
	Si	No	Si	No	Si	No	Si	No	Esencial	Útil pero no esencial	No Importante	
1	/		/			/	/		/			
2	/		/			/	/		/			
3	/		/			/	/		/			
4	/		/			/	/		/			
5	/		/			/	/		/			
6	/		/			/	/		/			
7	/		/			/	/		/			

Firma de Validador

Nombre: ROSITA CARRUZZANO

Cédula: 0602523805

Link de audios de entrevistas:

<https://drive.google.com/drive/folders/1uS7GPR87ohdrzT4YuN30GEso6TBDM6GP?usp=sharing>