

UNIVERSIDAD ESTATAL DE BOLÍVAR

Facultad de Jurisprudencia, Ciencias Sociales y Políticas

Carrera de Derecho

Trabajo de investigación previo a la obtención del título de Abogada

Título

La ausencia de una tipificación específica en el código orgánico integral penal sobre la desprotección de las víctimas de delitos de contenido falso, o "deepfakes"

Autora

Kherly Zamantha Saltos García

Tutor

Dr. Marco Vinicio Chávez Taco MSc.

Guaranda – Ecuador

CERTIFICACIÓN DE APROBACIÓN

En mi calidad de Tutora del Trabajo de Integración Curricular, presentado por la señorita Kherly Zamantha Saltos García previo a la obtención del grado de Abogada, titulado La Ausencia de una tipificación específica en el Código Orgánico Integral Penal sobre la desprotección de las víctimas de delitos de contenido falso, o "Deepfakes", certifico que dicho trabajo cumple con los requisitos académicos, metodológicos y formales exigidos, y reúne los méritos suficientes para ser sometido a la presentación pública y evaluación por parte del tribunal examinador que se designe.


Dr. Marco Vinicio Chávez Taco MSc

Tutor

DECLARACIÓN JURAMENTADA DE AUTORÍA

Yo, Kherly Zamantha Saltos García, portadora de la cédula No 0202189019-8, egresada de la carrera de Derecho de la Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad Estatal de Bolívar, bajo juramento declaro en forma libre y voluntaria que el presente trabajo de investigación titulado: LA AUSENCIA DE UNA TIPIFICACIÓN ESPECÍFICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL SOBRE LA DESPROTECCIÓN DE LAS VÍCTIMAS DE DELITOS DE CONTENIDO FALSO, O "DEEPFAKES", ha sido realizado íntegramente por mi persona con la dirección del tutor Dr. Marco Vinicio Chávez Taco, docente de la carrera antes mencionada; por lo tanto, es de mi exclusiva autoría. En tal virtud, dejo constancia que las ideas, criterios y expresiones vertidas en el desarrollo del presente documento han sido elaboradas a partir de la recopilación y análisis de fuentes bibliográficas, tales como libros, revistas, publicaciones académicas, medios de comunicación, y demás fuentes pertinentes y necesarias para la elaboración de esta investigación.



Kherly Zamantha Saltos García

AUTORA

Se otorgó ante mí y en fe de ello
confiero ésta primera copia
certificada, firmada y sellada en
Guaranda, 10 de junio del 2026

Dr. Hernán Cristóbal Arcos
NOTARIO SEGUNDO DEL CANTÓN GUARANDA



20260201002P00828

DECLARACION JURAMENTADA
OTORGA: KHERLY ZAMANTHA SALTOS GARCÍA
CUANTIA: INDETERMINADA
DI 2 COPIAS



En la ciudad de Guaranda, provincia Bolívar, República del Ecuador, hoy día miércoles diez de junio de dos mil veintiséis, ante mí DOCTOR HERNÁN RAMIRO CRIOLLO ARCOS, NOTARIO SEGUNDO DE ESTE CANTÓN, comparece la señorita Kherly Zamantha Saltos García, por sus propios derechos. La compareciente es de nacionalidad ecuatoriana, mayor de edad, de estado civil soltera, domiciliada en el cantón San José de Chimbo, provincia de Bolívar y de tránsito por este lugar, con celular número: cero nueve ocho cinco nueve cuatro siete cero tres uno, correo electrónico: zamysaltos12@gmail.com; a quien de conocerla doy fe en virtud de haberme exhibido su cédula de ciudadanía en base a la que procedo a obtener su certificado electrónico de datos de identidad ciudadana, del Registro Civil, mismo que agrego a esta escritura como documento habilitante; bien instruida por mí el Notario en el objeto y resultados de esta escritura de Declaración Juramentada que a celebrarlo procede, libre y voluntariamente.- En efecto juramentado que fue en legal forma previa las advertencias de la gravedad del juramento, de las penas de perjurio y de la obligación que tiene de decir la verdad con claridad y exactitud, declara lo siguiente: "Que previo a la obtención del Título de Abogada en la Facultad de Jurisprudencia Ciencias Sociales y Políticas, otorgado por la Universidad Estatal de Bolívar, manifiesto que los criterios e ideas emitidas en el presente Trabajo de Investigación, titulado: **"LA AUSENCIA DE UNA TIPIFICACIÓN ESPECÍFICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL SOBRE LA DESPROTECCIÓN DE LAS VÍCTIMAS DE DELITOS DE CONTENIDO FALSO O "DEEPPFAKES"**; es de mi exclusiva responsabilidad en calidad de autora, además autorizo a la Universidad Estatal de Bolívar hacer uso de todos los contenidos que me pertenece a parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Es todo cuanto tengo que decir en honor a la verdad". Hasta aquí la declaración juramentada que junto con los documentos anexos y habilitantes que se incorpora queda elevada a escritura pública con todo el valor legal, y que la compareciente acepta en todas y cada una de sus partes, para la celebración de la presente escritura se observaron los preceptos y requisitos previstos en la Ley Notarial; y, leída que le fue a la compareciente por mí el Notario, se ratifica y firma conmigo en unidad de acto quedando incorporada en el Protocolo de esta Notaría, de todo cuanto DOY FE.

Kherly Zamantha Saltos García
C.C. 0202189098

DR. HERNÁN RAMIRO CRIOLLO ARCOS
NOTARIO SEGUNDO DE CANTÓN GUARANDA

DERECHOS DE AUTOR

Yo: Kherly Zamantha Saltos García, portador de la Cédula de Identidad No **0202189098**, en calidad de autor titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Tema: La ausencia de una tipificación específica en el código orgánico integral penal sobre la desprotección de las víctimas de delitos de contenido falso, o "deepfakes**, modalidad Proyecto de Investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo/autorizamos a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El (los) autor (es) declara (n) que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.



Kherly Zamantha Saltos García

Autora

DEDICATORIA

Esta tesis le dedico a Dios, a mi Señor de la Divina Justicia y a San José, por guiarme siempre con su infinita bondad y mantenerme de pie pese a las adversidades.

A mis amados padres: William Saltos y Martha Garcia; mis dos pilares quienes me sostienen día a día, mi fuerza, y mi mayor inspiración, por su amor incondicional, su sacrificio silencioso, su apoyo, su bendición, por ser un gran ejemplo para mí, por formarme con valores y principios dignos de ser su hija. Mi padre, muestra de fuerza incansable, trabajador, talentoso, y mi madre, reflejo de valentía, empoderada, maravillosa, ambos con cualidades hermosas, principios y valores que los hacen únicos y especiales.

A mis hermanas: Karina y Jheyemi; por ser mi compañía en este camino, por sus consejos, por sus palabras de aliento, por no dejarme caer, por su cariño y por confiar en mí.

A mis sobrinos: James, Evan y mi angelito Eizhan; mis pequeños, por llenar mi vida de luz, ternura, y felicidad.

Pero también le dedico a mi niña interior, aquella que creía que no lo lograría y sintió que no podía continuar, aquí estamos, eres fuerte, eres valiente pequeña Zam.

Kherly Zamantha Saltos García

AGRADECIMIENTO

Quiero agradecer en primer lugar a Dios, a mi Señor de la Divina Justicia y San José, por iluminar mi camino, guiarme, protegerme y escucharme siempre.

Agradezco profundamente a los dos seres más importantes de mi vida, mi padre William Saltos y mi madre Martha García. Quienes me enseñaron a ser resiliente pese a cada dificultad, quienes han sanado mis heridas y jamás han soltado mi mano, quienes han cuidado tanto de mí, quienes me enseñaron a como sobrellevar hasta las situaciones más difíciles. Crecer bajo la guía de ustedes significó forjar mi vida en la fe, reconociendo en Dios la fuente inagotable de fortaleza y esperanza, quienes creyeron en mí, y jamás dudaron de lo lejos que yo podía llegar, y de todo lo que yo podía lograr, siempre con la bendición de Dios. Gracias por enseñarme a levantarme y por cada abrazo que me llenó de amor y fortaleza. Papitos los adoro, admiro, respeto y amo inmensamente. Hoy se cosecha frutos de lo que sembraron con amor.

A mis hermanas: Karina, quien pese a nuestras diferencias siempre ha visto por mí, me ha defendido cuando más indefensa me he sentido, me ha aconsejado cuando más lo he necesitado, me ha enseñado a ser un poco más dura y menos frágil, quien me dió dos hermosos sobrinos, James y Evan, mis pequeños, quienes alegran hasta mis días más tristes, con sus sonrisas, sus besos, abrazos. No son solos mis sobrinos, son mis hijos, mi sangre. Mi cuñado Edgar, quien ha aportado sus conocimientos en mi formación académica, y me ha brindado su ayuda.

Jheymi, mi gordita, quien, a pesar de su carácter fuerte, siempre supo cuando más necesitaba un abrazo, quien siempre tuvo las palabras correctas para poder animarme, quien con su amor y cariño me ha transmitido tanta fuerza en momentos en los que me quería rendir, quien también me dió un precioso sobrino Eizhan, un angelito; aquel pequeño que, a pesar de que estuvo pocos días en este mundo, me llenó de felicidad. Mi cuñado Stalin, el más acolitador, bromista, gracioso y un poquito loco, quien jamás ha dudado en extender su mano y brindarme su apoyo.

A mi tutor, Doctor Marco Chávez, por su invaluable guía, paciencia, y compromiso durante este proceso, por su orientación académica y por su confianza en mí. Su experiencia, conocimientos y su dedicación fueron esenciales para poder llegar hasta aquí. Fue un gran honor aprender de usted.

Pero también te agradezco a ti, mi pequeña Zam, aquella niña indefensa, que no tenía ganas ni fuerzas para seguir, gracias por ser fuerte, por no rendirte, por resistir, por continuar aún con miedo. Hoy la Zamantha de 22 años te dice; lo logramos, no desmayes, tenemos muchos propósitos que cumplir, mucho que soñar y demasiado por vivir, este sueño también es tuyo.

Kherly Zamantha Saltos García

ÍNDICE GENERAL

CERTIFICACIÓN DE APROBACIÓN	I
DECLARACIÓN JURAMENTADA DE AUTORÍA	II
DEDICATORIA.....	IV
AGRADECIMIENTO	II
CAPÍTULO I: PROBLEMA.....	1
1. Título.....	1
1.1. Resumen.....	2
1.2. Abstract	3
1.3. Introducción	4
1.4. Planteamiento del problema.....	5
1.5. Formulación del problema	6
1.6. Hipótesis o supuesto	7
1.7. Variables.....	7
1.7.1. Variable independiente.....	7
1.7.2. Variable dependiente.....	7
1.8. Objetivos.....	7
1.8.1. Objetivo general.....	7
1.8.2. Objetivos específicos	7

1.9. Justificación	8
2. CAPÍTULO II. MARCOS	10
2.1. Marco histórico	10
2.1.1. Reconocimiento constitucional de derechos comprometidos por la representación sintética en Ecuador	10
2.1.2. Consolidación del principio de legalidad y tipicidad estricta en el COIP	11
2.1.3. El problema de la cobertura típica frente a nuevas formas de manipulación sintética	12
2.1.4. Expansión de la tutela de datos e identidad digital con la Ley Orgánica de Protección de Datos Personales	12
2.1.5. Consentimiento, licitud del tratamiento y persistencia del vacío penal.....	13
2.1.6. Colombia y la evolución desde la protección penal de datos hacia la suplantación mediante inteligencia artificial.....	14
2.1.7. Chile y la transición hacia respuestas más cercanas a las imitaciones sintéticas	15
2.1.8. Balance histórico del vacío típico en Ecuador frente al desarrollo regional	16
2.2. Marco teórico.....	16
2.2.1. Derechos Fundamentales	17
2.2.2. Derecho a la privacidad e intimidad	18
2.2.3. Delito de calumnia	21
2.2.4. Bien jurídico protegido del delito de calumnia.....	22

2.2.5. Código Orgánico Integral Penal y tipos penales próximos.....	23
2.2.6. Contenido falso como delito	24
2.2.7. Poder punitivo del Estado	26
2.2.8. Principio de lesividad en el COIP	27
2.2.9. Principio de legalidad	28
2.2.10. Deepfake	29
2.2.11. Violencia digital	30
3. CAPÍTULO III. METODOLOGÍA	32
3.1. Método	32
3.1.1. Método documental	32
3.1.2. Método interpretativo	32
3.1.3. Método de análisis jurídico	33
3.2. Tipo de investigación	33
3.2.1. Investigación descriptiva	33
3.2.2. Investigación exploratoria.....	33
3.3. Técnicas e instrumentos de investigación.....	34
3.3.1. Técnica de revisión documental.....	34
3.4. Técnica de entrevista.....	35
3.5. Criterios de inclusión y criterios de exclusión.....	35

3.5.1. Criterios de inclusión	35
3.5.2. Criterios de exclusión	37
3.6. Población y muestra.....	38
3.7. Localización geográfica del estudio	38
4. CAPITULO IV – RESULTADOS Y DISCUSIÓN	40
4.1. Resultados del análisis documental	40
4.1.1. Insuficiencia del Código Orgánico Integral Penal frente a la creación de deepfakes.....	40
4.1.2. Limitaciones del artículo 178 del COIP frente a los deepfakes	44
4.1.3. Bienes jurídicos comprometidos por los deepfakes.....	46
4.1.4. Aportes del derecho comparado: Colombia y Chile	49
4.1.5. Necesidad de una tipificación penal en Ecuador	52
4.2. RESULTADOS DE LAS ENTREVISTAS.....	55
4.2.1. Criterios sobre la insuficiencia normativa y la aplicabilidad de los tipos penales vigentes	55
4.2.2. Dificultades probatorias, de autoría y de afectación a bienes jurídicos	57
4.2.3. Criterios sobre reforma normativa, límites de intervención penal y fortalecimiento institucional.....	60
4.3. Discusión	62
4.3.1. Insuficiencia normativa del COIP frente a los deepfakes	62
4.3.2. Límites del artículo 178 del COIP y problemas de subsunción.....	63

4.3.3. Afectación pluriofensiva y desprotección de la víctima	64
4.3.4. Dificultades probatorias, de autoría y de investigación penal	65
4.3.5. Derecho comparado y viabilidad de una reforma penal en Ecuador	65
 5. CAPÍTULO V. PROPUESTA DE REFORMA AL CÓDIGO ORGÁNICO INTEGRAL PENAL FRENTE A LOS DEEPFAKES	 68
5.1. Fundamentación de la propuesta.....	68
5.2. Finalidad y alcance de la propuesta	69
5.3. Proyecto de reforma legal	70
5.3.1. Exposición de motivos.....	70
5.3.2. Considerandos.....	71
5.3.3. Fórmula de expedición.....	72
5.3.4. Articulado de la reforma	72
5.3.5. Disposición final	73
5.4. Justificación técnico-jurídica del articulado	73
5.5. Viabilidad de la propuesta.....	76
 6. CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES.....	 77
6.1. Conclusiones	77
6.2. Recomendaciones	78

INDICE DE TABLAS

Tabla 1. Población de informantes entrevistados	38
Tabla 2. Alcance de los tipos penales vigentes frente a conductas vinculadas con deepfakes	41
Tabla 3. Diferencias entre la violación a la intimidad prevista en el COIP y los deepfakes como contenido sintético no consentido	44
Tabla 4. Bienes jurídicos afectados por la creación y difusión de deepfakes	47
Tabla 5. Derecho comparado sobre regulación o tratamiento jurídico de deepfakes en Colombia, Chile y Ecuador	50
Tabla 6. Elementos jurídicos que sustentan la necesidad de una tipificación penal específica sobre deepfakes en Ecuador.....	53
Tabla 7. Criterios sobre la insuficiencia normativa y la aplicabilidad de los tipos penales vigente.....	56
Tabla 8. Dificultades probatorias, de autoría y de afectación a bienes jurídicos	58
Tabla 9. <i>Criterios sobre reforma normativa, límites de intervención penal y fortalecimiento institucional</i>	60

INDICE DE FIGURAS

Figura. 1. Mapa del Ecuador	38
--	----

CAPÍTULO I: PROBLEMA

1. Título

**LA AUSENCIA DE UNA TIPIFICACIÓN ESPECÍFICA EN EL CÓDIGO
ORGÁNICO INTEGRAL PENAL SOBRE LA DESPROTECCIÓN DE LAS
VÍCTIMAS DE DELITOS DE CONTENIDO FALSO, O "DEEPPFAKES"**

1.1. Resumen

La investigación examina la ausencia de una tipificación penal específica en el Código Orgánico Integral Penal del Ecuador frente a los deepfakes y los efectos que ese vacío produce sobre la tutela de bienes jurídicos como la intimidad, la imagen, la honra, la identidad, la privacidad y la integridad personal. El inconveniente jurídico se advierte en que la legislación penal vigente incluye figuras afines a la materia, pero no elabora una descripción típica que considere de forma explícita la creación, manipulación o utilización de contenido sintético atribuido falsamente a una determinada persona identificable. A partir de aquí, el objetivo general fue analizar esa falta normativa y elaborar un marco regulatorio para su sanción. La investigación se desarrolló con un enfoque cualitativo y recurrió al método documental, al método interpretativo y al análisis jurídico; y como técnica principal se aplicó la revisión documental de fuentes normativas, doctrinales, jurisprudenciales y comparadas, entrelazadas con entrevistas a una jueza de garantías penales, un fiscal y un defensor público. Se tuvo la capacidad de la investigación para llegar a la conclusión de que el Código Orgánico Integral Penal no establece de manera directa la creación sintética de contenido falso mediante inteligencia artificial, dejando así sin encaje específico el núcleo comisivo del deepfake. Se corroboró que el artículo 178 del mismo cuerpo legal ofrece un nivel parcial de cobertura respecto de aquellos hechos de acceso, reproducción o difusión de contenido preexistente, sin entrar a mencionar la fabricación sintética del contenido. A ello, además, se añaden las dificultades probatorias en lo que se refiere a la autenticidad del archivo, a la trazabilidad, a la determinación de autoría y a la verificación forense. En esas condiciones, la falta de una tipificación específica supone una limitación de la respuesta penal clara y suficiente, favorece problemas de subsunción y debilita el resguardo de los bienes jurídicos comprometidos, por lo que se hace necesaria una reforma legislativa vinculada con un refuerzo institucional en la investigación digital y en la pericia forense.

PALABRAS CLAVE: DEEPFAKES; TIPIFICACIÓN PENAL; INTELIGENCIA ARTIFICIAL; BIENES JURÍDICOS; DERECHO PENAL

1.2. Abstract

This study addresses the lack of a specific criminal classification in Ecuador's Comprehensive Organic Criminal Code regarding deepfakes and the consequences this produces for the protection of legal interests such as privacy, image, honor, identity, personal data protection, and personal integrity. The legal problem lies in the fact that the current criminal framework provides related offences, yet it does not contain a legal definition that expressly covers the creation, manipulation, or use of synthetic content falsely attributable to an identifiable person. On that basis, the general objective was to analyze this legal gap and to propose a regulatory framework for punishment. The study followed a qualitative approach and relied on documentary, interpretative, and legal analysis methods. Its main technique was the documentary review of legal, doctrinal, jurisprudential, and comparative sources, complemented by interviews with a criminal guarantees judge, a prosecutor, and a public defender. The review showed that the Comprehensive Organic Criminal Code does not expressly classify the synthetic creation of false content through artificial intelligence, leaving the core conduct of deepfakes without precise legal fit. It was also found that Article 178 provides only partial coverage, since it focuses on acts of access, reproduction, or dissemination of pre-existing material, but not on the synthetic fabrication of the content itself. In addition, the conduct under study affects several legal interests and creates evidentiary difficulties related to file authenticity, traceability, authorship determination, and forensic verification. For that reason, the absence of a specific criminal classification limits a clear and sufficient criminal response, creates problems of legal subsumption, and weakens the protection of the affected legal interests, which makes legislative reform and institutional strengthening in digital investigation and forensic expertise necessary.

KEYWORDS: DEEPFAKES; CRIMINAL CLASSIFICATION; ARTIFICIAL INTELLIGENCE; LEGAL INTERESTS; CRIMINAL LAW.

1.3. Introducción

La irrupción de los deepfakes constituye una manifestación reciente de los riesgos derivados del uso indebido de la inteligencia artificial en entornos digitales. La posibilidad de crear o alterar contenidos con apariencia auténtica ha intensificado los problemas vinculados con la desinformación, la suplantación, la afectación de la imagen y la eventual vulneración de derechos personalísimos. En el contexto del derecho penal, este tema cobra especial interés en el sentido de que dichos recursos puedan atribuir hechos no existentes, dar a conocer material lesivo o crear situaciones que comprometen la tutela de bienes jurídicos y la respuesta del sistema de justicia ante las nuevas formas de manipulación digital.

La inteligencia artificial ha permitido la producción de contenidos audiovisuales con un alto grado de fidedignidad, entre ellos los deepfakes, manipulaciones sonoras y digitales que pueden acarrear consecuencias de tipo penal si están asociadas a hechos simulados, atribuyen conductas que no son ciertas o comprometen derechos de terceras personas. El mismo fenómeno, al menos en el contexto del derecho ecuatoriano, genera problemas a la hora de encuadrarlo dentro de los tipos penales existentes y en la propia tutela de las víctimas.

La problemática de la investigación reside en que no existe una tipificación penal explícita dentro del Código Orgánico Integral Penal para aquellas conductas que se vinculan con la creación, posesión y difusión de deepfakes, lo cual puede resultar en situaciones en las que la víctima no cuente con los debidos estándares mínimos de protección y el sistema de justicia penal tenga límites. Con base en lo expuesto, se determinará la relación que existe entre la falta normativa mencionada y el grado de suficiencia que tiene el Código Orgánico Integral Penal para una respuesta correcta hacia este tipo de conductas.

La investigación se propone realizar un análisis de la falta de tipificaciones penales explícitas en el Código Orgánico Integral Penal, así como su relación con el desamparo de quienes son víctimas de conductas vinculadas a deepfakes. En tal sentido, se proponen

objetivos orientados a identificar los límites de la norma penal vigente, examinar las bases normativas que corresponden a la teoría de la tipificación junto a la protección de los bienes jurídicos comprometidos, así como poder establecer criterios que permitan determinar si la normativa que está en vigor es una respuesta correcta y suficiente frente a tal fenómeno..

Para el cumplimiento de dicho objetivo, se procederá a observar el vacío de tipificación penal ante los deepfakes en el ordenamiento ecuatoriano. Luego, se analizará la norma de aplicación más el marco de justificación legal correspondiente, con el fin de comprobar la suficiencia o la insuficiencia de la respuesta penal en vigor ante conductas como las detalladas.

La investigación pretende verificar si el ordenamiento penal ecuatoriano permite la suficiente protección a las víctimas de conductas afincadas en los deepfakes o si se observa un vacío normativo que necesita una respuesta penal más intensa. En consecuencia, se busca ayudar a la construcción de unos elementos jurídicos que permitan la valoración de la suficiencia o la insuficiencia de la respuesta penal vigente.

El documento se estructura a partir de la delimitación del problema jurídico, de la revisión de la fundamentación teórica y la fundamentación jurídica, de la presentación de la metodología, del análisis con la respectiva discusión de resultados y de la formulación de conclusiones y recomendaciones, de manera que cada apartado contribuye a la revisión ordenada del vacío de tipificación penal específica frente a las conductas que podrían estar vinculadas a los deepfakes en el ordenamiento ecuatoriano..

1.4. Planteamiento del problema

La sociedad contemporánea se encuentra inmersa en una constante transformación tecnológica, donde la inteligencia artificial (IA) ha pasado de ser una disciplina científica a un elemento de profundo impacto en la vida diaria. En este contexto, la IA generativa ha dado lugar a un fenómeno emergente y preocupante: los

“deepfakes”. Este término se deriva de la combinación de "deep learning" (aprendizaje profundo), una rama de la IA que utiliza redes neuronales artificiales, y "fake" (falso), indicando que el contenido generado, aunque aparente ser auténtico, es una manipulación o creación sintética.

Los deepfakes pueden manifestarse en diversos formatos, incluyendo imágenes estáticas, archivos de audio o videos completos, y pueden ser creados con software de edición estándar o con sistemas avanzados de redes generativas antagónicas (GANs). La tecnología ha alcanzado un nivel de sofisticación tal que resulta extremadamente difícil para el ojo humano diferenciar lo real de lo artificial, lo que ha facilitado su uso con propósitos maliciosos.

La evolución exponencial de la inteligencia artificial (IA) generativa ha dado lugar a nuevas formas de criminalidad, entre las que destacan la creación de contenido falso, conocido como “deepfake”, con fines de producción de material sexual no consentido de personas adultas. En Ecuador, a pesar del aumento de la ciberdelincuencia, el Código Orgánico Integral Penal (COIP) no contiene una tipificación específica para sancionar estas conductas. Aunque existen figuras penales como la violación a la intimidad, su aplicación resulta deficiente para abordar la naturaleza única y sofisticada de los delitos cometidos con IA. Este vacío legal genera un escenario de impunidad y deja a las víctimas sin una adecuada tutela judicial, lo cual se agrava por la falta de capacidades institucionales y peritos especializados para la detección y el juzgamiento de estos crímenes.

1.5. Formulación del problema

¿El Código Orgánico Integral Penal contempla algún delito para sancionar la violencia sexual cometida mediante el uso de inteligencia artificial para crear deepfakes de personas adultas, o se requiere una reforma legislativa específica que incorpore un tipo penal determinado?

1.6. Hipótesis o supuesto

La ausencia de una tipificación específica en el Código Orgánico Integral Penal sobre el delito de deepfakes genera una desprotección legal para las víctimas, lo cual acarrea la vulneración de derechos fundamentales y la misma dificulta la sanción efectiva.

1.7. Variables

1.7.1. Variable independiente

Ausencia de una tipificación penal específica en el Código Orgánico Integral Penal respecto de la creación de deepfakes.

1.7.2. Variable dependiente

Alto nivel de desprotección legal que sufren las víctimas de delitos generados por los deepfakes en la creación de contenido explícito mediante esta inteligencia artificial.

1.8. Objetivos

1.8.1. Objetivo general

Analizar la ausencia de una tipificación específica en el Código Orgánico Integral Penal para los delitos de producción de contenido sexual no consentido mediante el uso de 'deepfakes' en adultos, y proponer un marco normativo para su sanción

1.8.2. Objetivos específicos

- Determinar la insuficiencia normativa en la ley penal del Ecuador para sancionar de manera efectiva el uso de "deepfakes" con fines de violación a la integridad sexual.
- Evaluar la inoperancia del artículo 178 (Violación a la intimidad) del COIP para la sanción de la creación y difusión de "deepfakes" de contenido sexual no consentido en adultos, y analizar el impacto psicosocial que esta violencia digital causa en las víctimas.

- Examinar los modelos legislativos de derecho comparado, como los de Colombia y Chile, para identificar estrategias exitosas en la tipificación de los delitos de "deepfake" y formular recomendaciones de reforma para el ordenamiento jurídico ecuatoriano.

1.9. Justificación

La presente investigación parte de una fuerte problemática de la actualidad y es urgente, la ausencia de una tipificación específica en el Código Orgánico Integral Penal (COIP) del Ecuador sobre la creación, posesión y difusión maliciosa de contenidos audiovisuales (falsos) mediante el uso de la tecnología deepfake, principalmente cuando los mismos son de carácter sexual no consentido y afectan a las mujeres. Este vacío normativo es relevante, tanto en términos sociales como jurídicos, debido a que genera escenarios de impunidad y desprotección de las víctimas, las mismas que enfrentan ciertas afectaciones a sus derechos fundamentales tales como la intimidad, la privacidad, seguridad persona y la honra.

El avance exponencial de la inteligencia artificial y las herramientas de edición digital ha propiciado la proliferación de deepfakes, es decir contenidos audiovisuales que simulan la realidad, pero que han sido manipulados para generar videos, imágenes o audios de personas en situaciones que no son reales, muchas de ellas son de índole sexual, por lo tanto, este fenómeno desafía la doctrina penal clásica, basada en la materialidad de la prueba y la protección de bienes jurídicos. La tecnología se vuelve confusa entre lo verdadero y lo falso, dificultando la detección y la sanción de los responsables de estos acontecimientos. La investigación este motivada por aquella necesidad ética de poder garantizar la protección efectiva de derechos humanos ante nuevas formas de violencia y vulnerabilidad propiciadas por la tecnología.

El derecho a la intimidad, integridad sexual, y entre otros son pilares del sistema democrático y de la dignidad de la persona, los cuales son reconocidos tanto en la Constitución de la Republica del Ecuador como en tratados internacionales, a pesar de ello el actual COIP ecuatoriano no contempla con claridad ni suficiencia la protección de

víctimas frente a la manipulación digital de imágenes o la creación de contenido sexual no consentido, a pesar de que el daño que genera es real.

El estudio no se limita simplemente a una cuestión teórica o de principios, sino que va más allá de ello y trata también de ofrecer soluciones concretas y aplicables al contexto jurídico social ecuatoriano. La reciente documentación de casos de deepfakes que han sido utilizados para obtener resultados de extorsión, hostigamiento y calumnia evidencia que la tecnología sirve de medio para ejercer violencia en el ámbito familiar, profesional y en el bienestar psicológico de las personas afectadas. No existe sanción adecuada para los mismos, lo cual impide su reparación, pero también protege de manera indebida a aquellos que perjudican u obtienen beneficios mediante la inteligencia artificial. Este trabajo se destaca por su enfoque disciplinario, integrado al derecho penal ecuatoriano, tecnología, derechos humanos, y violencia de género, este abordaje de estudio comparado entre Colombia y Chile comprende el fenómeno en toda su complejidad, al mismo tiempo identificar las limitaciones de la normativa vigente y así formular propuestas fundamentadas en evidencias.

Esta investigación se plantea como una propuesta de innovación aplicada, evaluando de algún modo la factibilidad de incluir un marco normativo específico dentro del Código Orgánico Integral Penal (COIP), para sancionar la creación y difusión de deepfakes de carácter sexual no consentido y las diferentes formas de violencia digital asociadas con la inteligencia artificial, es aquí donde podemos comprar la experiencia de Ecuador con reformas recientes en varios países de la región que han logrado avances en cuanto a la protección penal contra delitos generados por la IA, de este modo se destacan los resultados positivos en cuanto a la tutela judicial efectiva y la reparación integral de cada una de las víctimas .

2. CAPÍTULO II. MARCOS

2.1. Marco histórico

La discusión penal sobre deepfakes en Ecuador no surge de manera aislada con la aparición reciente de herramientas de inteligencia artificial, sino que se inserta en un proceso previo de evolución normativa en el que el ordenamiento fue reconociendo bienes jurídicos relevantes, consolidando garantías penales y ampliando la tutela sobre la información personal en entornos digitales. En esa trayectoria, el problema no radica en la inexistencia de protección jurídica, sino en el desfase que se produce cuando una forma nueva de manipulación sintética comienza a incidir sobre ámbitos ya tutelados sin que exista todavía una respuesta típica expresa para afrontarla en el plano penal.

2.1.1. Reconocimiento constitucional de derechos comprometidos por la representación sintética en Ecuador

La Constitución de la República del Ecuador de 2008 marca el primer momento relevante en la evolución interna del problema, porque fijó con mayor claridad la tutela de dimensiones personales que hoy resultan directamente expuestas frente a la manipulación sintética. La Constitución de la República del Ecuador, en el artículo 66, numerales 18, 19 y 20, garantiza “el derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona”, “el derecho a la protección de datos de carácter personal” y “el derecho a la intimidad personal y familiar” (Asamblea Nacional del Ecuador, Constitución de la República del Ecuador, 2008, pág. 49). Visto en perspectiva, ese reconocimiento permite advertir que el ordenamiento ecuatoriano ya había delimitado ámbitos sensibles de protección antes de la irrupción de la manipulación sintética. El problema posterior, entonces, no surge por falta de bienes jurídicos protegidos, sino por la aparición de una modalidad tecnológica nueva de afectación.

Junto con ese reconocimiento de derechos, la Constitución de 2008 también dejó fijado otro elemento decisivo para la trayectoria posterior del problema: la imposibilidad de responder penalmente fuera de los límites de la tipificación previa. El artículo 76, numeral 3, de la Constitución dispone que “nadie podrá ser juzgado ni sancionado por un acto u

omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza” (Asamblea Nacional del Ecuador, Constitución de la República del Ecuador, 2008, pág. 54). Esa garantía anticipa la dificultad que más tarde plantearían los deepfakes en el plano penal, ya que la reacción estatal no puede apoyarse en extensiones interpretativas frente a conductas no previstas. Con ello, la Constitución dejó definido el marco dentro del cual debía discutirse la protección penal futura de esas afectaciones.

2.1.2. Consolidación del principio de legalidad y tipicidad estricta en el COIP

La entrada en vigencia del Código Orgánico Integral Penal en 2014 representa el segundo gran momento en la trayectoria normativa del problema, porque convirtió en regla codificada una exigencia ya afirmada por la Constitución: La exigencia de ley previa que se debe contemplar para legitimar la intervención penal. El Código Orgánico Integral Penal establece en el artículo 5, numeral 1, que “no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 11); con lo cual el sistema penal ecuatoriano había puesto freno a respuestas punitivas construidas fuera de la previsión legal, pero años más tarde, cuando los deepfakes ya generaban nuevas formas de afectación, el propio marco ya exigía comprobar si la conducta fue efectivamente prevista por la ley penal..

La codificación de 2014 también volvió operativa esa garantía frente a conductas emergentes. El artículo 25 del COIP dispone que “los tipos penales describen los elementos de las conductas penalmente relevantes” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 11). Esa precisión reafirmó que la intervención penal debía apoyarse en descripciones normativas concretas. Más adelante, la aparición de los deepfakes hizo visible la necesidad de verificar si esas agresiones encontraban acomodo real dentro del catálogo vigente.

2.1.3. El problema de la cobertura típica frente a nuevas formas de manipulación sintética

A partir de esa base, el problema de la cobertura típica empezó a adquirir un relieve propio frente a las nuevas modalidades de agresión digital. El artículo 25 del COIP dispone que “los tipos penales describen los elementos de las conductas penalmente relevantes” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 11). Esa regla exige que la respuesta penal se apoye en una descripción legal concreta. Por ello, la aparición posterior de los deepfakes obliga a verificar si la conducta realizada encaja o no en un tipo vigente.

La dificultad aumenta cuando ya no se trata solo de un contenido falso, sino de una simulación capaz de reproducir imagen, voz o acciones con apariencia de autenticidad. El artículo 18 del COIP establece que “infracción penal es la conducta típica, antijurídica y culpable” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 7). En ese marco, la gravedad del hecho no basta por sí sola para activar el castigo. El problema consiste en determinar si esa forma de manipulación sintética fue prevista por la ley penal.

2.1.4. Expansión de la tutela de datos e identidad digital con la Ley Orgánica de Protección de Datos Personales

Un tercer momento en esta trayectoria aparece con la Ley Orgánica de Protección de Datos Personales de 2021, porque el ordenamiento ecuatoriano pasó de una tutela general de derechos a una regulación más concreta del tratamiento de información identificable en entornos digitales. La Ley Orgánica de Protección de Datos Personales, en el artículo 1, dispone que “el objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 4). Desde entonces, el problema de los deepfakes ya no se relaciona solo con la imagen o la honra, sino también con el uso de información personal de la víctima.

Este avance es importante porque el desarrollo de contenidos sintéticos a menudo se apoya en fotografías, registros de audio o manifestaciones faciales que permiten identificar a una persona. En este sentido, el art. 4, núm. 1, de la ley establece el dato como “dato que identifica o hace identificable a una persona natural, ya sea directa o indirectamente” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, p. 5). Por lo que, la afectación no versará solo sobre el hecho de que el contenido sea falso; también está el uso de los datos personales protegidos por la ley. La norma se aproxima así a las circunstancias materiales que hacen posible el deepfake, si bien es cierto que todavía no alcanza para resolver una eventual forma de tratamiento penal.

2.1.5. Consentimiento, licitud del tratamiento y persistencia del vacío penal

La evolución normativa iniciada con la Ley Orgánica de Protección de Datos Personales adquirió mayor precisión al incorporar el consentimiento como condición de licitud para el tratamiento de datos personales. El artículo 8 de la ley establece que “se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 8). Esta regla exige autorización del titular para usar información vinculada con su persona. Por eso, cuando un deepfake se construye con imagen, voz u otros rasgos identificables, también aparece un problema de licitud en el tratamiento de datos.

Ese desarrollo, sin embargo, no modificó por sí mismo la respuesta penal frente a la manipulación sintética. El artículo 2 de la misma ley señala que su objeto es regular “el tratamiento de datos personales, en todo tipo de soporte, por parte de personas naturales o jurídicas, de derecho público o privado” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 4). La norma fortaleció la tutela extrapenal sobre identidad y tratamiento de información, pero no resolvió el problema de tipificación penal. La protección creció, aunque la figura penal específica siguió ausente.

2.1.6. Colombia y la evolución desde la protección penal de datos hacia la suplantación mediante inteligencia artificial

En Colombia, la respuesta jurídica frente al deepfake siguió una ruta más específica cuando el Congreso empezó a tratar de forma expresa la suplantación mediante inteligencia artificial. El Proyecto de Ley 225 de 2024 Senado propuso modificar el artículo 296 del Código Penal sobre falsedad personal y, en su ponencia para segundo debate, definió al deepfake como “Contenido audiovisual (imagen, audio, video) hiper realista que es falso o engañoso, creado o modificado mediante sistemas de Inteligencia Artificial (Congreso de Colombia, Ponencia para segundo debate al Proyecto de Ley 225 de 2024 Senado, por medio del cual se modifica el artículo 296 de la Ley 599 de 2000, 2024, pág. 7). Ese momento resulta especialmente relevante porque desplaza el debate desde los delitos informáticos generales hacia una forma concreta de manipulación sintética vinculada con la identidad y la fe pública. En esa misma trayectoria, la Comisión Primera del Senado aprobó la iniciativa en primer debate en mayo de 2024 y, en septiembre del mismo año, la plenaria del Senado aprobó el proyecto y lo remitió a la Cámara de Representantes, lo que muestra que el problema dejó de ser una preocupación marginal y pasó a recibir tratamiento legislativo expreso.

La evolución del trámite también permite advertir que la reacción colombiana no se dirigió a crear un delito autónomo de deepfake, sino a proponer un agravante para la falsedad personal cuando la suplantación se realiza con inteligencia artificial. La Gaceta del Congreso de 2025 registró el texto aprobado en segundo debate del Proyecto de Ley 360 de 2024 Cámara – 225 de 2024 Senado y señaló que “Cuando la falsedad personal se realizare con la utilización de Inteligencia Artificial la multa se aumentará hasta en una tercera parte” (Congreso de Colombia, Texto aprobado en segundo debate del Proyecto de Ley 360 de 2024 Cámara – 225 de 2024 Senado, 2025, pág. 13). Esa previsión muestra una respuesta penal concreta todavía en trámite, inserta en el marco de la falsedad personal y no como figura autónoma de deepfake. Al mismo tiempo, el mismo proyecto vinculó el fenómeno con medidas de prevención y detección de “deepfakes, fraudes y suplantación de

identidad”, lo que permite advertir que en Colombia el problema ya fue identificado como una modalidad específica de engaño y afectación digital.

2.1.7. Chile y la transición hacia respuestas más cercanas a las imitaciones sintéticas

En Chile, el tratamiento legislativo del problema siguió una trayectoria que primero se vinculó con la violencia digital y después avanzó hacia una discusión más directa sobre deepfakes e imitaciones sintéticas. El proyecto que tipifica y sanciona la violencia digital, Boletín 13928-07, ingresó en 2020 y en 2024 pasó al Senado, donde continuó su tramitación en segundo trámite constitucional. Dentro de ese proceso, una nota institucional del Senado informó en septiembre de 2025 que la Comisión de la Mujer y Equidad de Género aprobó un nuevo artículo sobre violencia política digital, en el que se propuso sancionar la difusión de contenidos “verosímiles pero falsos, manipulados o creados mediante inteligencia artificial u otra tecnología” (Senado de Chile, 2025). Ese antecedente resulta importante porque muestra que el debate legislativo chileno ya empezó a reconocer, de forma expresa, que la manipulación de imágenes, sonidos y videos mediante inteligencia artificial puede producir afectaciones jurídicamente relevantes. En esa misma línea, el problema dejó de tratarse solo como una forma general de violencia digital y comenzó a conectarse con usos específicos de contenido sintético falso.

La evolución chilena se volvió aún más precisa con el proyecto ingresado a la Cámara de Diputadas y Diputados el 21 de agosto de 2025, Boletín 17795-19, cuyo texto identifica expresamente el fenómeno al señalar que el uso no autorizado de tecnologías capaces de reproducir imagen, cuerpo o voz genera “imitaciones digitales realistas sin su consentimiento —fenómeno conocido popularmente como deepfake” (Cámara de Diputadas y Diputados de Chile, 2025, pág. 2). En la misma moción se afirma que “aún no existe una norma específica que proteja frente a la suplantación digital mediante IA” (Cámara de Diputadas y Diputados de Chile, 2025, pág. 2). Ese hito es especialmente relevante para esta investigación porque muestra que en Chile el problema ya fue identificado de manera autónoma y vinculado con un vacío normativo concreto. De ese

modo, aunque todavía no exista una solución legislativa definitiva, la trayectoria chilena evidencia un camino de actualización que Ecuador puede observar como antecedente comparado frente a la necesidad de construir una respuesta penal más precisa.

2.1.8. Balance histórico del vacío típico en Ecuador frente al desarrollo regional

La trayectoria expuesta muestra que, en Ecuador, la protección jurídica avanzó por capas: primero se reconocieron derechos comprometidos por la manipulación sintética, después se consolidaron límites de legalidad y tipicidad, y más tarde se reforzó la tutela sobre datos e identidad digital. En el estudio **La omisión del delito de deepfake en el Código Orgánico Integral Penal en Ecuador** se sostiene que “no existe un tipo penal que individualice el delito de deepfake ya que únicamente existe normativa que engloba el delito” (Arévalo Fernández, 2024, pág. 55). Esa afirmación permite advertir que el problema no consiste en una ausencia total de tutela, sino en el rezago de la respuesta penal frente a una forma nueva de afectación. El ordenamiento avanzó en protección, pero no llegó a describir de modo expreso la creación o difusión de contenidos sintéticos lesivos.

La revisión del desarrollo regional reciente refuerza ese balance. En la misma investigación se sostiene que “debe existir una figura penal mediante la cual sancione este delito” (Arévalo Fernández, 2024, pág. 68). Tal afirmación pone de manifiesto que el vacío ya no puede ser entendido únicamente como una omisión descriptiva, sino como una problemática que requiere una respuesta penal expresa frente a la manipulación sintética. Precisamente en ese punto, la trayectoria ecuatoriana se encuentra en conexión con la trayectoria comparada regional: el reconocimiento del problema ha avanzado más rápidamente que la construcción de una respuesta penal específica, con lo que queda planteada la necesidad de analizar con rigor la suficiencia del COIP frente a los deepfakes.

2.2. Marco teórico

La generación y alteración sintética de imagen y voz ha transformado la falsificación audiovisual en una simulación con apariencia de autenticidad, lo que

incrementa su idoneidad para el engaño y amplía los escenarios de afectación jurídica en entornos de circulación masiva. En el artículo doctrinal *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, publicado en *California Law Review*, se advierte que los deepfakes “emergerán como mecanismos poderosos para que algunos exploten y saboteen a otros” (Chesney y Citron, 2019, pág. 1771). La advertencia doctrinal permite ubicar el problema más allá de la manipulación técnica: el contenido sintético puede convertirse en un medio para atribuir hechos inexistentes, suplantar identidades o provocar descrédito público sobre una persona real.

2.2.1. Derechos Fundamentales

2.2.1.1. Constitución y derechos vinculados a intimidad, imagen, honra y dignidad

El análisis penal del deepfake debe partir de los derechos fundamentales potencialmente afectados, ya que la simulación tecnológica utiliza atributos personales protegidos como imagen o voz para construir representaciones que aparentan autenticidad. En el artículo *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, publicado en *California Law Review*, se advierte que “algunos daños son sufridos por individuos o grupos, como cuando los deepfakes se emplean para explotar o sabotear identidades individuales” (Chesney y Citron, 2019, pág. 1758). De esta manera, la manipulación tecnológica adquiere relevancia jurídica cuando emplea la imagen o la voz de una persona para situarla en situaciones que afectan su valoración social o su posición frente a terceros.

En virtud de lo anterior, la protección constitucional de la imagen, la voz, la honra y el buen nombre va adquiriendo una relevancia directa. La Constitución de la República del Ecuador, en el artículo 66, numeral 18, establece lo siguiente: “El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona” (Asamblea Nacional Constituyente, 2008, pág. 29) El reconocimiento constitucional exhibe que la imagen y la voz corresponden a la esfera jurídica de la persona.

La afectación alcanza también la intimidad y el control sobre la circulación de información vinculada con la persona. La Constitución de la República del Ecuador, en el artículo 66, numeral 19, establece que “la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular” (Asamblea Nacional Constituyente, 2008, pág. 32). Desde esta previsión constitucional se comprende que la elaboración de deepfakes no se limita a la creación de un contenido falso, sino que implica la utilización no consentida de rasgos identificables que posteriormente se proyectan en una representación artificial con potencial lesivo.

La jurisprudencia constitucional ecuatoriana ha precisado, además, que la tutela no depende del formato del mensaje, sino del menoscabo que puede producir sobre la persona. En la Sentencia No. 105-23-IN/25 se expuso que las personas deben ser protegidas en relación con “expresiones, manifestaciones, alegaciones, verbalizaciones o cualquier clase de mensaje, sea en el formato que sea, que puedan mermar su dignidad humana” (Corte Constitucional del Ecuador, Sentencia No. 105-23-IN/25, 2026, pág. 30). Esa opinión permite encuadrar que la relevancia jurídica del deepfake se articula con la afectación que provoca sobre la honra, la dignidad o la imagen de la víctima, cuando la exposición sintética es creíble ante las demás personas.

La importancia de esos derechos fundamentales no suprime, sin embargo, la necesidad de examinar la respuesta penal desde parámetros estrictos de legalidad. En la obra *Garantismo penal*, publicada por la Universidad Nacional Autónoma de México, se sostiene que “el principio de legalidad y de la sujeción del juez a la ley, expresa los dos valores ético-políticos fundamentales de la jurisdicción en el Estado de derecho y en la democracia política” (Ferrajoli, *Garantismo penal*, 2006, pág. 35). Esa premisa permite distinguir entre la entidad constitucional del daño y la posibilidad de sancionarlo penalmente dentro de tipos previamente establecidos.

2.2.2. Derecho a la privacidad e intimidad

La privacidad y la intimidad se vuelven especialmente sensibles frente al deepfake cuando la tecnología inserta artificialmente a una persona en escenas o conductas

inexistentes que posteriormente circulan como si formaran parte de su vida real. En el artículo *Deepfakes and the Epistemic Backstop*, publicado en *Philosophers' Imprint*, se sostiene que los registros de audio y video “funcionan como un respaldo epistémico. Regulan nuestras prácticas testimoniales” (Rini, 2020, pág. 2). La observación permite comprender que la privacidad se vuelve vulnerable cuando la imagen o la voz dejan de funcionar solo como datos de identificación y pasan a sostener una apariencia de verdad que ubica a la persona en hechos inexistentes.

La intimidad se ve comprometida de manera directa cuando la representación sintética reutiliza rasgos personales para construir un contenido que expone a la persona en contra de su voluntad. La Constitución de la República del Ecuador, en el artículo 66, numeral 19, establece que “la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular” (Asamblea Nacional Constituyente, 2008, pág. 32). A partir de ese mandato puede sostenerse que el deepfake desplaza a la víctima del control sobre la circulación de su imagen, su voz o cualquier otro elemento que permita reconstruir artificialmente su presencia en un contexto falso.

La afectación se agrava cuando el contenido manipulado se difunde en entornos digitales de circulación amplia, donde la atribución falsa puede amplificarse rápidamente. En el artículo *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, publicado en *California Law Review*, se advierte que los deepfakes permiten crear audio y video de personas reales “diciendo y haciendo cosas que nunca dijeron o hicieron” (Chesney y Citron, 2019, pág. 1753). Esa precisión permite entender que la lesión a la intimidad no depende solo de la difusión, sino de la capacidad de la tecnología para reconstruir falsamente experiencias personales y presentarlas como verdaderas.

2.2.2.1. Ley Orgánica de Protección de Datos Personales y tutela de datos e imagen

La Ley Orgánica de Protección de Datos Personales aporta un marco útil para comprender por qué el deepfake no solo compromete la intimidad, sino también la facultad de decisión sobre información y rasgos que permiten identificar a la persona. En el artículo

1 de la ley se dispone que su objeto y finalidad es “garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 4). Esa formulación permite advertir que la tutela de datos protege la capacidad de decidir sobre el uso de elementos vinculados con la propia identidad.

La relación con el deepfake se vuelve más clara cuando la ley incorpora dentro de sus definiciones a los datos biométricos. En el artículo 4 se establece que el dato biométrico es un “dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 6). La consideración de las imágenes faciales en dicha categoría permite hacer la conexión entre la producción de deepfakes y el tratamiento de los datos que hacen referencia a la persona. La misma ley define el dato personal como “aquel que identifica o hace identificable a una persona natural, de forma directa o indirecta” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 6). Esa precisión es importante, pues en los deepfakes, la lesión no depende solo de reproducir de manera exacta el rostro o la voz, sino de la propia posibilidad de que otros reconozcan a la persona aparecida como si de verdad estuviera físicamente presente.

La utilidad de esta categoría aumenta cuando la representación artificial no reproduce un dato aislado, sino un conjunto de rasgos que permite individualizar a la persona frente a terceros. En la Ley Orgánica de Protección de Datos Personales, el artículo 4 también define tratamiento como cualquier “operación o conjunto de operaciones realizadas sobre datos personales” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, pág. 6). Esta previsión permite sostener que la elaboración de deepfakes puede involucrar no solo difusión posterior, sino también procesamiento previo de rasgos faciales, voz o patrones biométricos que integran la identidad digital de la persona.

2.2.3. Delito de calumnia

Para determinar si los deepfakes pueden encajar dentro de tipos penales ya existentes, resulta necesario analizar los delitos que protegen el honor y el buen nombre. Dentro de ese conjunto, la calumnia constituye una de las figuras más próximas para examinar la posible relevancia penal de ciertos deepfakes. El Código Orgánico Integral Penal, en el artículo 182, dispone que “La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 57). Esa formulación permite advertir que la calumnia no sanciona cualquier contenido ofensivo o humillante, sino la atribución falsa de un delito a una persona determinada.

La doctrina ha puesto manifiesto que la extensión del medio comisivo no merma la necesidad de mantener precisión sobre el contenido que se imputa. En esta línea, la obra Temas penales 2, editada por la Corte Nacional de Justicia, Felipe Rodríguez Moreno observa que “el verbo rector final será realizar imputación” (Rodríguez Moreno, 2017, pág. 155). Esa observación permite poner el foco de atención en el núcleo de la conducta típica y no solo en el soporte de su difusión.

Desde esa perspectiva, un deepfake podría adquirir relevancia en este ámbito cuando la simulación audiovisual atribuya de manera creíble un hecho delictivo inexistente a una persona concreta. En la obra Derecho penal, parte general, publicada por Editorial Reppertor, se sostiene que “una vez determinado el bien jurídico protegido en un delito, la interpretación podrá excluir del tipo respectivo las conductas que no lesionen ni pongan en peligro dicho bien jurídico” (Mir Puig, 2006, pág. 163). Esa precisión permite sostener que la intervención penal frente a un deepfake solo sería posible cuando la representación sintética encaje en la estructura típica del delito y afecte efectivamente el bien jurídico que la figura protege.

La insuficiencia de la calumnia se aprecia con mayor claridad cuando el contenido manipulado provoca descrédito intenso sin formular imputación delictiva expresa. En una

consulta absuelta sobre los artículos 182 y 271 del Código Orgánico Integral Penal, la Corte Nacional de Justicia señaló que la calumnia “consiste en la falsa imputación de un delito realizada por cualquier medio” (Corte Nacional de Justicia del Ecuador, 2019, pág. 2). Este criterio confirma que el problema no se agota en la falsedad del soporte, sino en el contenido específico atribuido a la persona afectada.

2.2.4. Bien jurídico protegido del delito de calumnia

Una vez identificado el tipo penal potencialmente aplicable, corresponde determinar cuál es el bien jurídico que protege la calumnia para evaluar si los daños producidos por un deepfake realmente encajan dentro de su ámbito de tutela. La determinación del bien jurídico protegido en la calumnia resulta necesaria para establecer hasta dónde puede llegar la respuesta penal frente a los deepfakes y cuándo la afectación producida desborda el ámbito de ese tipo penal. En la obra Derecho penal. Parte general, publicada por Editorial Reppertor, se sostiene que “una vez determinado el bien jurídico protegido en un delito, la interpretación podrá excluir del tipo respectivo las conductas que no lesionen ni pongan en peligro dicho bien jurídico” (Mir Puig, 2006, pág. 163). Esa afirmación permite advertir que la sola existencia de una falsedad técnica no basta para justificar relevancia penal.

A propósito de las consultas expuestas anteriormente, en el marco de una consulta absuelta sobre los artículos 182 y 271 del Código Orgánico Integral Penal, la Corte Nacional de Justicia estableció que “con la calumnia el bien jurídico protegido es la honra, y consiste en la falsa imputación de un delito realizada por cualquier medio” (Corte Nacional de Justicia del Ecuador, 2019, pág. 2). A partir de ahí, el criterio delimitó el alcance de la figura y permite no perder de vista que el problema penal no recae sobre cualquier afectación reputacional, sino sobre la que se produce cuando a una persona se le atribuye falsamente la realización de un hecho punible.

Cuando el contenido artificial presenta a la víctima como autora de un hecho punible, puede advertirse la afectación de la honra en un marco muy específico en torno al artículo 182 del COIP. Por el contrario, cuando la manipulación sintética ridiculiza, sexualiza, cosifica o expone a la persona, pero no le atribuye la comisión de un tipo punible

concreto, entonces la lesión puede llegar a ser intensa, pero quedará al margen del ámbito específico que la figura reserva para la falsa atribución de una conducta delictiva.

2.2.5. Código Orgánico Integral Penal y tipos penales próximos

Después de analizar la calumnia y su bien jurídico, resulta necesario examinar otras figuras del Código Orgánico Integral Penal que podrían relacionarse con la circulación o utilización de información personal. Definido el papel del contenido falso como medio comisivo, corresponde examinar los tipos penales más próximos dentro del Código Orgánico Integral Penal. El artículo 178 dispone que “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 30). Esa formulación permite advertir que el legislador describió un catálogo concreto de conductas vinculadas con datos, soportes informáticos o comunicaciones privadas.

La dificultad aparece con mayor claridad cuando el hecho no consiste en interceptar o difundir una comunicación previa, sino en fabricar un contenido inexistente a partir de rasgos personales reutilizados y luego ponerlo en circulación. La Constitución de la República del Ecuador, en el artículo 76, numeral 3, dispone que “nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal” (Asamblea Nacional Constituyente, 2008, pág. 37). Desde esa garantía, el artículo 178 no puede extenderse a fases no descritas, como la mera creación instrumental del contenido sintético, salvo que la conducta realizada corresponda realmente con alguno de sus verbos rectores.

La utilidad de revisar estos tipos próximos radica en precisar si el ordenamiento vigente ofrece una respuesta suficiente o si el fenómeno desborda la descripción legal existente. En el Código Orgánico Integral Penal, el artículo 178 enumera verbos como “acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique” (Asamblea Nacional del Ecuador, Código Orgánico Integral Penal, 2014, pág. 30). La enumeración evidencia que la norma regula conductas concretas sobre datos o comunicaciones, pero no

describe de forma expresa la fabricación de una representación audiovisual inexistente a partir de inteligencia artificial.

2.2.6. Contenido falso como delito

Para evitar que el análisis penal se limite a la mera existencia de contenido falso, es necesario precisar cuándo la falsedad adquiere relevancia dentro del Derecho penal. En el ámbito penal, la falsedad solo adquiere relevancia cuando funciona como medio para lesionar o poner en peligro un bien jurídico determinado. En la obra Derecho penal. Parte general, publicada por Editorial Reppertor, se sostiene que “la interpretación podrá excluir del tipo respectivo las conductas que no lesionen ni pongan en peligro dicho bien jurídico” (Mir Puig, 2006, pág. 163). Esa idea permite advertir que la falsedad, considerada en abstracto, no basta para justificar sanción penal.

Este criterio resulta aplicable al análisis de los deepfakes, pues la relevancia penal no depende únicamente del origen artificial del contenido, sino de su capacidad para inducir error, atribuir hechos inexistentes o generar una afectación concreta sobre la persona representada. En el estudio Deepfakes: Trick or Treat? se señala que “Los deepfakes aprovechan técnicas poderosas de aprendizaje automático e inteligencia artificial para manipular o generar contenido visual y de audio con un alto potencial de engaño” (Kietzmann et al., 2020, pág. 136). Esa característica permite concentrar la valoración penal en la idoneidad engañosa del contenido, en la finalidad con que se utiliza y en el bien jurídico comprometido.

2.2.6.1. Derecho comparado y parámetros normativos para criminalidad informática

El derecho comparado cumple una función específica dentro de esta investigación: identificar técnicas legislativas y objetos de tutela que puedan servir de base para valorar la suficiencia del COIP y orientar una propuesta penal frente al deepfake en Ecuador. En esa línea, Colombia y Chile aportan insumos distintos pero complementarios, porque permiten examinar cómo otros ordenamientos han vinculado la protección de datos, la falsificación

informática, la suplantación y las imitaciones digitales realistas con nuevas formas de afectación tecnológica.

En Colombia, un primer insumo útil aparece en la protección penal de datos personales. La Ley 1273 de 2009, en el artículo 269F sobre violación de datos personales, establece que “El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes” (República de Colombia, 2009). Esta formulación resulta relevante porque muestra una técnica típica de verbos rectores amplios, útil para describir distintas formas de captación, circulación y utilización indebida de información personal en entornos digitales.

El aporte colombiano se vuelve más cercano al objeto de esta tesis cuando la discusión legislativa incorpora expresamente la inteligencia artificial en supuestos de suplantación. En la noticia institucional del Senado de la República de Colombia sobre el Proyecto de Ley No. 225 de 2024, se indicó que la iniciativa “busca incluir el delito de falsedad personal para la modalidad de suplantación cuando se usa la Inteligencia Artificial (IA)” (Senado de la República de Colombia, 2024). Esta referencia resulta especialmente valiosa porque ya no se limita a la protección general de datos, sino que vincula de manera directa la IA con falsedad personal, fe pública y afectación de identidad, elementos especialmente próximos al problema penal del deepfake.

Chile aporta un criterio diferente, centrado en la manipulación de datos para producir apariencia de autenticidad. En la explicación oficial sobre delitos informáticos publicada por la Biblioteca del Congreso Nacional de Chile, se señala que comete falsificación informática quien “indebidamente introduzca, altere, dañe o suprima datos informáticos para que sean tomados como auténticos o usados para generar documentos auténticos” (Biblioteca del Congreso Nacional de Chile, 2022). Esto resulta ser importante para la presente tesis porque también permite llevar a cabo el análisis comparativo del problema de la autenticidad aparente, uno de los aspectos más sensibles del deepfake.

En el caso chileno, el antecedente más directo del objeto de la investigación no aparece en una ley de deepfake, sino que se identifica en proyectos de ley orientados a la regulación de las imitaciones digitales realistas y de la violencia digital relacionada con la inteligencia artificial. De hecho, en la misma ficha oficial del Boletín N.º 17795-19 se encuentra el proyecto de ley que “regula la creación y difusión de imitaciones digitales realistas de la imagen, cuerpo o voz de las personas, generadas mediante inteligencia artificial” (Cámara de Diputadas y Diputados de Chile, 2025). Este antecedente cumple una buena función porque manifiesta con claridad el reconocimiento de la necesidad de regular normativamente la reproducción artificial de los atributos personales, algo absolutamente central en cualquier propuesta penal sobre deepfakes.

En conclusión, Colombia y Chile han proporcionado ejemplos que resultan relevantes a la hora de sostener la propuesta ecuatoriana. La experiencia colombiana ilustra la posibilidad de incluir el fenómeno del deepfake en los tipos penales de suplantación y falsedad personal, y la chilena ofrece criterios relacionados con la autenticidad informática y con las normativas para regular las imitaciones digitales muy realistas. A partir de esas aportaciones, el derecho comparado hace también sus aportes normativos interesantes para poder contar con una respuesta penal más exacta frente al deepfake, acorde a la legalidad, la tipicidad estricta y a la tutela efectiva de bienes jurídicos.

2.2.7. Poder punitivo del Estado

La discusión sobre deepfakes también obliga a recordar que el poder punitivo del Estado actúa bajo límites estrictos. En la obra *Derecho y razón. Teoría del garantismo penal*, publicada por la Universidad Nacional Autónoma de México, Ferrajoli sostiene que “Las funciones del principio de legalidad penal son esencialmente tres: asegurar sobre todo la certeza del derecho, asegurar la sujeción del juez a la ley y asegurar la primacía de la legislación” (Ferrajoli, *Derecho y razón. Teoría del garantismo penal*, 2006, pág. 258). Con esa base, la sola gravedad social del fenómeno no alcanza para justificar una ampliación del castigo.

La necesidad de contención se entiende mejor si se toma en cuenta que el Derecho penal constituye la forma más intensa de intervención estatal sobre la persona. En la obra *Garantismo penal*, publicada por la Universidad Nacional Autónoma de México, se sostiene que “el principio de legalidad y de la sujeción del juez a la ley, expresa los dos valores ético-políticos fundamentales de la jurisdicción (Ferrajoli, *Garantismo penal*, 2006, pág. 35). Vista así, la reacción frente a tecnologías emergentes debe apoyarse en garantías y no solo en la alarma que producen sus efectos.

La cautela cobra sentido, además, porque los cambios tecnológicos suelen impulsar respuestas apresuradas. Allí el problema no se reduce a una posible falta de tutela, sino al riesgo de forzar tipos vigentes para abarcar conductas nuevas. Por eso, el examen del deepfake necesita mantenerse dentro de una lógica de intervención mínima, en la que la respuesta penal solo resulte legítima cuando otras vías sean insuficientes y, al mismo tiempo, se respete la estructura garantista del sistema.

2.2.8. Principio de lesividad en el COIP

El principio de lesividad permite separar lo socialmente reprochable de aquello que realmente justifica intervención penal. En un trabajo publicado en *Pensamiento Penal*, Torres sostiene que “el principio de lesividad puede entenderse como la imposibilidad de cualquier derecho de legitimar una intervención punitiva cuando a lo sumo no media un conflicto jurídico” (Torres, 2015, pág. 1). La idea resulta especialmente útil aquí, porque impide tratar cualquier deepfake como delito y obliga a verificar si existe una afectación real a un bien jurídico ajeno.

Este artículo examina el desarrollo de la progresión entre las preferencias de consumo y los comportamientos de compra de la Generación Z en relación con la moda sostenible. La Generación Z es la primera generación que ha crecido como experta nativa en medios digitales. El contexto de la misma le otorga, por un lado, una mayor influencia en el ámbito económico, pero, al mismo tiempo, un fuerte conjunto de valores medioambientales que podría cambiar el mundo de la moda. El estado de la cuestión se condensa a raíz de la investigación sobre los factores que determinan su forma de decidir

desde la sostenibilidad (exigen transparencia, autenticidad y responsabilidad social por parte de las marcas), pero, de la misma manera, respecto al tema de las contradicciones conductuales, en concreto, la distancia entre los valores y las prácticas. En definitiva, una separación entre sus actitudes a favor de la sostenibilidad y la forma de comprar que tienen, la cual suele estar afectada por principios económicos y por las modas ligadas al fast fashion.

La importancia del principio de lesividad se irá entendiendo mucho mejor cuando empecemos a contrastar usos distintos de la misma tecnología. No toda manipulación audiovisual produce una afectación penalmente trascendente, pues bien puede existir un uso humorístico, paródico o, incluso, un uso inocuo; en cambio, sí es cierto que cuando un deepfake tiene una finalidad de sexualización, de humillación, de suplantación o de atribución de hechos falsos a una persona identificable, la disputa deja de ser un uso incorrecto de una tecnología y pasa a poner en jaque bienes jurídicos cuya lesión sí puede justificar un cuestionamiento penal.

2.2.9. Principio de legalidad

Junto con la lesividad, el principio de legalidad ocupa un lugar decisivo en el análisis penal del deepfake. La Constitución de la República del Ecuador, en el artículo 76, numeral 3, dispone que “nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal” (Asamblea Nacional Constituyente, 2008, pág. 37). La garantía exige que la conducta prohibida esté descrita con claridad suficiente antes de que pueda imponerse una sanción.

La legalidad no se reduce a reclamar la existencia formal de una norma. También exige una descripción precisa de la conducta prohibida. En la obra Derecho penal, parte general, publicada por Editorial Reppertor, se sostiene que “una vez determinado el bien jurídico protegido en un delito, la interpretación podrá excluir del tipo respectivo las conductas que no lesionen ni pongan en peligro dicho bien jurídico” (Mir Puig, 2006, pág. 163). A partir de este concepto, la tipicidad estricta lo que impide es la traslación

automática de figuras que se asemejan a supuestos que el legislador no ha definido de forma lo suficientemente expresa.

La relevancia que tiene esa garantía se vuelve más intensa ante fenómenos tecnológicos que establecen nuevas formas de agresión. La existencia de un daño o menoscabo elevado no puede, por sí solo, llevar a cubrir vacíos con identificaciones a figuras cercanas. En este ámbito, la legalidad corta decisivamente la posibilidad de construir los tipos penales por analogía y, con ello, exige que se examine con detenimiento si el ordenamiento efectivamente describe el comportamiento que le es atribuido.

Eso hace que en el caso del deepfake el asunto no sea solamente advertir que la manipulación podría estar afectando de forma intensa a una persona, sino verificar si el COIP permite de forma clara la creación, utilización o difusión de esa representación artificial en un tipo penal más o menos específico. En esa línea, la discusión en torno a la tipificación no puede quedar concentrada solamente en la intensidad del daño, sino en la correspondencia estricta que debe existir entre el hecho y la descripción del mismo que previamente debe haber sido formulado en un tipo penal.

2.2.10. Deepfake

La delimitación conceptual del deepfake ocupa un lugar central en este marco teórico porque permite precisar el fenómeno que origina el problema jurídico analizado. En el artículo *Deepfakes and the Epistemic Backstop*, publicado en *Philosophers' Imprint*, Regina Rini sostiene que “La tecnología deepfake utiliza aprendizaje automático para fabricar grabaciones de video y audio que representan a personas reales haciendo y diciendo cosas que nunca hicieron ni dijeron” (Rini, 2020, pág. 1). La definición muestra que no se trata de una simple edición digital, sino de una fabricación audiovisual orientada a presentar como real una conducta inexistente.

Comprender el fenómeno exige, además, una precisión mínima sobre su funcionamiento. En el estudio *Deepfakes: Trick or Treat?*, publicado en *Business Horizons*, se señala que los deepfakes “aprovechan técnicas poderosas de aprendizaje automático e

inteligencia artificial para manipular o generar contenido visual y de audio con un alto potencial de engaño” (Kietzmann et al., 2020, pág. 136). Ahí se advierte que su fuerza no depende solo del resultado falso, sino del uso de sistemas capaces de reproducir rasgos faciales, voz y movimientos con creciente verosimilitud.

La particularidad del deepfake también se explica por la confianza que suele depositarse en los registros audiovisuales. En el mismo artículo publicado en *Philosophers’ Imprint*, se sostiene que los registros de audio y video “funcionan como un respaldo epistémico. Regulan nuestras prácticas testimoniales” (Rini, 2020, pág. 2). El punto es importante porque el engaño no nace únicamente de la manipulación técnica, sino del valor de verdad que socialmente se atribuye a la imagen y al sonido.

Otro rasgo decisivo aparece en su capacidad para atribuir a una persona real acciones, expresiones o contextos que nunca existieron. En el artículo *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, publicado en *California Law Review*, se advierte que esta tecnología hace posible crear audio y video de personas reales “diciendo y haciendo cosas que nunca dijeron o hicieron” (Chesney y Citron, 2019, pág. 1753). Así, la manipulación sintética ya no es una modificación técnica, sino que ha pasado a ser una forma de proyectar erróneamente una identidad, una conducta o una situación frente a otras personas. Así, la importancia jurídica del deepfake es la consecuencia de la confluencia de la verosimilitud, la atribución personal y la capacidad de circulación, y por ello puede afectar a la identidad, la honra, la intimidad y a la seguridad jurídica, y por lo tanto el examen penal exige poder diferenciar lo que se considera falsedad digital sencilla y lo que es una falsedad con incidencia jurídicamente relevante.

2.2.11. Violencia digital

La violencia digital permite comprender el espacio en el que los deepfakes lesivos alcanzan mayor intensidad. En el capítulo *El hábeas data en Ecuador*, incluido en *Apuntes de derecho procesal constitucional*, se sostiene que “una foto o un video digital puede viajar en segundos por la web y ser reproducida en periódicos digitales o redes sociales” (De la Torre y Montaña Pinto, 2011, pág. 179). La circulación en línea deja ver que la difusión no

es un elemento secundario del problema, sino el factor que amplifica la exposición de la víctima y vuelve más difícil contener el daño.

La intensidad del problema aumenta porque el entorno digital favorece la reproducción, persistencia y reaparición constante del contenido. Una vez difundido, el material puede ser replicado por terceros, almacenado en distintos soportes y reinsertado en nuevas plataformas, incluso cuando la víctima ya ha manifestado su oposición. La agresión inicial se transforma así en una afectación prolongada que excede el instante de la primera publicación.

La gravedad se percibe con mayor claridad cuando el contenido manipulado se usa para humillar, cosificar o intimidar mediante una difusión persistente. La Corte Constitucional del Ecuador, en la Sentencia No. 2064-14-EP/21, señaló que “esas imágenes gozan de un marco de protección reforzado y que, en principio, siempre que se rebase la esfera exclusivamente personal o doméstica” (Corte Constitucional del Ecuador, Sentencia No. 2064-14-EP/21, 2021, pág. 61). La norma exige valorar tanto la circunstancia de circulación cuanto la afectación material sobre la intimidad, la imagen y el honor.

En el caso del deepfake, la violencia digital es el sistema en que la manipulación sintética es capaz de generar un daño mayor. La circulación no solo amplía la extensión de la afectación, sino que, además, es prueba de su realidad ante el tercero y, paralelamente, hace más difícil regresar a la reputación o a la esfera de la intimidad afectada.. Por esta razón, el análisis del deepfake no puede ser separado del medio digital en el que circula, ya que es el lugar en el que la afectación es todavía más amplia, más persistente y más difícil de frenar.

3. CAPÍTULO III. METODOLOGÍA

3.1. Método

La metodología utilizada en la presente investigación tuvo un enfoque cualitativo, basada en el análisis de diferentes fuentes jurídicas, doctrinales, dogmáticas, históricas y filosóficas. Este enfoque permitió comprender los vacíos normativos y los efectos en cuanto a la desprotección de víctimas de deepfakes. Además, la investigación examinó el problema desde una perspectiva orientada a comprender no solo la ausencia de una regulación específica, sino también la forma en que dicha omisión incide en la protección de derechos fundamentales.

3.1.1. Método documental

Fue documental por cuanto la investigación se basó en el estudio de diferentes fuentes jurídicas, doctrinales, dogmáticas, históricas y filosóficas, así como en la revisión de casos jurisprudenciales y hechos relevantes dentro del ámbito legal en el Ecuador. Este método permitió comprender la variedad de fenómenos sociales a los cuales nos enfrentamos y relacionar el fenómeno investigado con la realidad jurídica ecuatoriana, observando las limitaciones existentes en la normativa vigente frente a nuevas formas de violencia digital.

3.1.2. Método interpretativo

Fue interpretativo por cuanto el objeto de estudio exigía interpretar normas, doctrina y criterios jurídicos para determinar el alcance de la respuesta penal frente a los deepfakes. A partir de este método, la investigación permitió examinar no solo la ausencia de una regulación específica, sino también la forma en que dicha omisión incide en la protección de derechos fundamentales. Bajo esa perspectiva, la revisión de fuentes jurídicas y doctrinarias permitió identificar criterios sobre intimidad, honra, imagen, libertad, dignidad y demás derechos fundamentales, aspectos necesarios para ubicar esta problemática dentro del ámbito penal.

3.1.3. Método de análisis jurídico

Fue de análisis jurídico por cuanto el desarrollo de la investigación se sostuvo en una lectura jurídica e interpretativa del problema, lo que permitió examinar la insuficiencia normativa a partir de fuentes pertinentes. A su vez, la revisión doctrinaria, dogmática, jurisprudencial e histórica facilitó la identificación de criterios útiles para sustentar la necesidad de regulación de los deepfakes y respaldar la propuesta planteada en el estudio. De este modo, se pudo poner en evidencia la gravedad de esta conducta y la necesidad existente de regular los deepfakes en la legislación ecuatoriana.

3.2. Tipo de investigación

3.2.1. Investigación descriptiva

Fue descriptiva por cuanto permitió identificar la problemática que existe debido al vacío legal referente al uso de deepfakes en hechos delictivos, así como las posibles propuestas de reforma y los derechos vulnerados. Desde su carácter descriptivo, la investigación permitió precisar los elementos centrales del problema jurídico estudiado, especialmente en relación con la falta de una regulación específica frente al uso de deepfakes en hechos delictivos. Esta aproximación facilitó la identificación de derechos vulnerados y de aspectos relevantes vinculados con la necesidad de reforma dentro del marco penal ecuatoriano.

3.2.2. Investigación exploratoria

Asu vez fue exploratoria por cuanto abordó un fenómeno emergente en lo relacionado con el derecho ecuatoriano, donde falta una tipificación específica para estos casos. Por su parte, el alcance exploratorio permitió profundizar en un fenómeno que todavía presenta escaso desarrollo en el derecho ecuatoriano, por lo que fue necesario acudir a enfoques jurisprudenciales, doctrinarios y comparados para ampliar su comprensión. Desde este contexto, se logró revisar experiencias normativas asumidas en otras jurisdicciones y conectarlas con las limitaciones que se han advertido en la normativa vigente en el contexto nacional.

Dicha clasificación estructuró la investigación en dos niveles complementarios. Por un lado, explicar el problema jurídico que resulta del vacío legal existente respecto al uso de los deepfakes en hechos delictivos y, por otro, examinar un fenómeno que sigue siendo poco desarrollado en el derecho ecuatoriano. No bastaba con exponer el problema, sino también ampliar su comprensión a partir de doctrina, jurisprudencia y derecho comparado. De ese modo, se precisó mejor la insuficiencia de la normativa vigente y se sostuvo la necesidad de una respuesta jurídica más adecuada.

3.3. Técnicas e instrumentos de investigación

3.3.1. Técnica de revisión documental

La primera técnica fue una revisión documental por cuanto se realizó un examen profundo del Código Orgánico Integral Penal, reglamentos, tratados internacionales sobre derechos humanos, doctrina, artículos sobre deepfakes, protección de datos y reformas legislativas en países como Colombia y Chile. A partir de dicha revisión, se recabaron elementos normativos y doctrinales en la materia de la tipificación penal del deepfake, la protección de derechos fundamentales y respuestas jurídicas a la violencia digital como nuevas formas. Se dio cumplimiento así a una de las tareas necesarias para lograr matizar el problema versado, especialmente para el ámbito penal ecuatoriano.

Así también, la revisión de estas fuentes permitió realizar el contraste entre la regulación ecuatoriana y las experiencias legislativas comparadas, en especial conforme a lo que otros países han determinado como medidas frente a la creación y la difusión de contenido falso no consentido. Tal contraste permitió determinar criterios de consideración para llevar a cabo el juicio de suficiencia o insuficiencia de la norma y así profundizar en el análisis desarrollado.

Como instrumento se empleó la matriz de análisis documental, a partir de la cual se lleva a cabo la materialización de lo recabado en fuentes normativas, doctrinales y comparadas, la cual sirve para sistematizar los contenidos relevantes en lo que respecta a

tipificación penal, la protección de derechos fundamentales, la violencia digital, la regulación comparada y los vacíos normativos, facilitando así el desarrollo ordenado del análisis jurídico..

3.4. Técnica de entrevista

Por otra parte la segunda técnica fue una entrevista por cuanto permitió obtener criterios especializados sobre el tratamiento jurídico de los deepfakes y reconocer vacíos normativos dentro del marco penal vigente. Esta técnica aportó insumos relevantes para examinar la suficiencia de la normativa actual frente a nuevas formas de violencia digital y para contrastar la realidad ecuatoriana con la necesidad de una respuesta jurídica más adecuada.

La utilización de la técnica anterior permitió la recolección de información de utilidad desde la perspectiva práctico-jurídica, complementando lo hallado en el análisis documental y doctrinal realizado en el trabajo. Así, fue posible fortalecer la comprensión sobre el problema investigado, así como justificar la propuesta planteada en el estudio.

Se utilizó la guía de entrevista como instrumento para la recolección ordenada y homogénea de la información. La guía de entrevista permitió estructurar las preguntas dirigidas a los entrevistados y la obtención de criterios relacionados con la tipificación penal de los deepfakes, la protección de derechos fundamentales y la insuficiencia de la regulación existente..

3.5. Criterios de inclusión y criterios de exclusión

3.5.1. Criterios de inclusión

Para la selección de la información pertinente al estudio, se consideraron los siguientes criterios de inclusión:

- Documentos académicos, sentencias, legislación y estudios doctrinarios que analizaran la tecnología deepfake y su impacto legal en el ámbito penal o social en el Ecuador o Latinoamérica.
- Testimonios de expertos y personas afectadas, así como análisis legislativo comparado en Latinoamérica respecto a deepfakes.
- Estudios comparados y casos sobre la creación y difusión de contenidos falsos dirigidos a la criminalización, prevención o sanción de las conductas asociadas con los deepfakes.

Estos criterios delimitaron la búsqueda a fuentes referidas directamente al problema del derecho que se indagaba. Con ello, se justifica la búsqueda sobre contenidos relativos al uso de deepfakes, la afectación de derechos fundamentales y la respuesta penal frente a estas conductas, evitando que la revisión se disperse en documentación que poco tenía que ver con el objeto de la investigación y, en consecuencia, mantuviera una línea de acuerdo con los objetivos.

Asimismo, la forma de aplicar estos criterios reunió información proveniente de diferentes vertientes, ya fuera doctrinaria, normativa o comparativa, algo que complementó el estudio del fenómeno. Aquello también permitió analizar casos y posicionamientos que hacían referencia a la afectación de derechos fundamentales, elemento de notable relevancia en el problema que se indagaba

La manera de aplicar estos criterios mantuvo la búsqueda dentro de los márgenes de un tema que era de interés y que se refería de manera directa al problema del derecho que se estaba indagando. De tal forma, la revisión se llevó a cabo en fuentes adecuadas para poder atender la información y no alejarse de lo que era el objeto de la investigación..

3.5.2. Criterios de exclusión

Para depurar la información y evitar la incorporación de material ajeno al objeto de estudio, se consideraron los siguientes criterios de exclusión:

- Artículos de opinión, fuentes sin revisión y estudios que no abordaran específicamente la relación entre los deepfakes, los derechos fundamentales y el contexto penal del Ecuador.
- Testimonios o aportes de personas no relacionadas con los delitos de ciberdelincuencia, delitos informáticos, violencia digital o deepfakes, así como contextualización enfocada en otros delitos digitales.
- Estudios cuantitativos sin un análisis cualitativo, ni investigaciones centradas en el uso de deepfakes para fines distintos a la afectación de derechos fundamentales.

Estos criterios excluyeron información que pudiera desviar el análisis hacia ámbitos no vinculados con el problema jurídico estudiado. Con ello, se purgó el material que se reunió y se retuvo exclusivamente el material cuya información guarda relación directa con la dimensión penal del fenómeno objeto de análisis. Con tal criterio, la revisión fue dirigida hacia el contenido que tenía que ver con los deepfakes y la afectación de los derechos fundamentales en el contexto ecuatoriano.

De la misma forma, dichos criterios purgaron el material recolectado, hasta llegar a descartar fuentes que no guardan relación con la temática del estudio o con los objetivos de la investigación. Esta depuración permitió conservar claridad en la delimitación del estudio y evitar dispersiones que debilitaran el análisis.

Estos criterios de exclusión conservaron la coherencia entre el objeto de investigación, los objetivos planteados y el análisis jurídico desarrollado. Esta delimitación evitó dispersiones innecesarias y concentró el estudio en contenidos vinculados con la dimensión penal del problema examinado

3.6. Población y muestra

La población de estudio estuvo conformada por tres participantes vinculados con el sistema de justicia penal: un juez de garantías penales, un fiscal y un abogado defensor público. No se aplicó fórmula de muestra, debido a que la población quedó definida en un total de tres personas. En consecuencia, se trabajó con la totalidad de los participantes identificada.

Tabla 1.

Población de informantes entrevistados

Instrumento	Población
Entrevista	Juez de Garantías Penales
Entrevista	Fiscal
Entrevista	Abogado defensor público
Total	3

Nota. La población de informantes se conformó por tres operadores del sistema de justicia penal

La consideración de esta población incorporó criterios provenientes de operadores jurídicos vinculados con la aplicación del derecho penal. Estas apreciaciones permitieron contrastar el análisis documental con una visión práctica sobre la suficiencia del marco normativo o sus insuficiencias frente al fenómeno investigado

3.7. Localización geográfica del estudio

La investigación se delimitó al territorio de la República del Ecuador.

Figura. 1.

Mapa del Ecuador



Nota.: La figura muestra el territorio de la República del Ecuador, ámbito geográfico en el que se delimitó la investigación

4. CAPITULO IV – RESULTADOS Y DISCUSIÓN

4.1. Resultados del análisis documental

La revisión de la Constitución de la República del Ecuador (2008, art. 66, num. 18, 19 y 20; art. 76, num. 3), del Código Orgánico Integral Penal (2014, arts. 25, 178 y 182) y de la Ley Orgánica de Protección de Datos Personales (2021, arts. 1, 4 y 8) evidencia que el ordenamiento jurídico ecuatoriano reconoce y protege bienes jurídicos directamente comprometidos por los deepfakes, pero no articula una respuesta penal expresa frente a la creación sintética de contenido falso mediante inteligencia artificial. El problema no se sitúa, por tanto, en la inexistencia de tutela jurídica sobre la intimidad, la imagen, la honra, la privacidad o los datos personales, sino en la ausencia de una construcción típica capaz de captar, con precisión normativa, una modalidad comisiva tecnológicamente diferenciada.

4.1.1. Insuficiencia del Código Orgánico Integral Penal frente a la creación de deepfakes

El Código Orgánico Integral Penal no contiene una tipificación penal específica que describa de manera expresa la creación de deepfakes como conducta penalmente relevante. La significación de esta conclusión aflora en tanto se contempla que el COIP, en su artículo 25, asocia la tipicidad a la descripción legal de las conductas penalmente relevantes, y asiste en su texto vigente a regulaciones de figuras cercanas como la de la violación a la intimidad (art. 178) y la de calumnia (art. 182), sin tener en cuenta una figura autónoma referida específicamente a la fabricación sintética de contenido falso mediante inteligencia artificial. Por lo tanto, cuando el ordenamiento penal ecuatoriano asienta sus mecanismos de protección de bienes jurídicos como la intimidad, el honor, la imagen, los datos personales o la fe pública, no prevé un tipo que recoja de forma directa la producción sintética de contenido falso mediante inteligencia artificial.

La revisión del COIP concluye que las figuras vigentes se fundamentan en los verbos rectores vinculados con conductas ya previstas por la ley. El artículo 178 condena, así, a quien "acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique" datos personales, mensajes, voz, audio, video, soportes informáticos o comunicaciones

privadas, y el artículo 182 castiga la "falsa imputación de un delito"; ninguno de los preceptos de los que se ocupa este segmento normativo establece, de forma autónoma, la producción, manipulación o utilización artificial de una representación falsa que se pueda atribuir con certeza a una persona determinable. Desde la dogmática del injusto, ello muestra un déficit de adecuación típica expresa respecto del núcleo comisivo del deepfake. Luego entonces, a pesar de que algunas de las posibles conductas resultantes de su utilización pueden, incluso, intentarse incluir dentro de tipos penales próximos, dicha operación es parcial, no resulta suficiente, desde el momento en que el problema de base es el déficit de adecuación típica expresa en relación con la conducta de producción sintética que tiene aptitud para realizar un daño.

Tabla 2.

Alcance de los tipos penales vigentes frente a conductas vinculadas con deepfakes

Norma o figura jurídica	Conducta regulada	Posible punto de conexión típica	Déficit de cobertura típica frente a la creación sintética
Art. 178 COIP. Violación a la intimidad	Sanciona el acceso, interceptación, examen, retención, grabación, reproducción, difusión o publicación no consentida de datos personales, mensajes, voz, audio o video	Puede relacionarse con la difusión o publicación posterior de contenido íntimo o personal asociado a la víctima	No describe de forma expresa la creación sintética de contenido falso mediante inteligencia artificial, sino conductas recaídas sobre información o material ya existente

Art. 182 COIP. Calumnia	Sanciona la falsa imputación de un delito en contra de otra persona	Podría vincularse con deepfakes que atribuyan falsamente la comisión de un delito a una persona determinada	Su ámbito de protección se restringe a la honra mediante falsa imputación delictiva; no abarca de manera general la creación de contenido sintético sexual, degradante o suplantatorio
			No constituye por sí sola una base típica penal suficiente para sancionar la creación de deepfakes sin una descripción legal expresa dentro del COIP
Constitución de la República del Ecuador (art. 66, nums. 18, 19 y 20; art. 76, num. 3)	Reconoce derechos fundamentales vinculados con la dignidad, la privacidad, la imagen, la intimidad y la protección de datos personales, además del principio de legalidad sancionadora	Permite identificar los bienes jurídicos comprometidos por los deepfakes	
Ley Orgánica de Protección de Datos Personales (arts. 1, 4 nums. 1 y 4, y 8)	Regula el tratamiento de datos personales, biométricos e información identificable	Puede relacionarse con el uso no consentido de imagen, voz o datos biométricos para construir un deepfake	Su protección es relevante en el ámbito de datos, pero no sustituye la necesidad de una tipificación penal específica sobre la

Tipos penales próximos vinculados con falsedad, suplantación o afectación de bienes jurídicos	Protegen ámbitos específicos según la conducta descrita por la ley	Pueden servir como referentes parciales para intentar subsumir ciertas conductas derivadas del uso de deepfakes	fabricación sintética de contenido lesivo
			Su aplicación exige operaciones de subsunción extensiva que no resuelven de manera suficiente la conducta base de creación sintética mediante inteligencia artificial

Análisis e interpretación

El ordenamiento jurídico penal ecuatoriano tiene un alcance fragmentario respecto al deepfake, ya que las figuras del tipo penal reguladas actualmente reaccionan sobre efectos jurídicos derivados de la actividad que provoca dicha situación, pero no sobre la conducta-base que explícitamente consiste en la producción de una representación sintética, atribuible irrealmente a una persona cuya identificación puede llegar a ser posible. Este tipo de contexto hace que la reacción penal se desplace hacia las consecuencias posteriores del hecho y deja completamente fuera de la captación directa el núcleo comisivo hecho por la inteligencia artificial generativa.

La técnica de tipificación existente genera, por tal motivo, un problema de subsunción estructural. La creación artificial de contenido no tiene correspondencia típica expresa dentro del COIP, de suerte que la persecución penal queda reducida a una reconducción indirecta hacia figuras jurídicas cercanas. Esa forma conduce a debilitar la certeza del derecho y a reducir la capacidad del sistema de ofrecer respuesta adecuada para una forma de agresión digital tecnológicamente diferenciada.

La falta de normativa, que resulta determinante y fundamental, tiene un efecto dogmático y constitucional. Dogmático porque se produce un desajuste entre el hecho, el

bien jurídico y el tipo. Constitucional porque provoca un mayor riesgo de interpretaciones extensivas que no son compatibles con el artículo 76, numeral 3, de la Constitución de la República del Ecuador ni con el artículo 25 del Código Orgánico Integral Penal.

4.1.2. Limitaciones del artículo 178 del COIP frente a los deepfakes

El artículo 178 del Código Orgánico Integral Penal es una de las figuras más cercanas al problema investigado, dado que establece sanción a conductas relacionadas con el acceso, la reproducción, difusión o publicación no consentida de información, datos personales, voz, audio o video. Pero, al presentar un catálogo cerrado de los verbos rectores, su ámbito de acción típica se proyecta sobre la realización de actos de intromisión o bien de divulgación sobre un material real o existente y no sobre la fabricación algorítmica de escenas falsas de apariencia auténtica.

El artículo 178 presupone un objeto material preexistente sobre el cual recae el acceso, la reproducción o la difusión no consentida; en cambio, en los deepfakes el objeto lesivo puede ser artificialmente construido a partir de imagen facial, voz o datos biométricos, en términos compatibles con la definición de dato personal y dato biométrico contenida en la Ley Orgánica de Protección de Datos Personales (2021, art. 4, nums. 1 y 4). Esta limitación demuestra que la respuesta penal actual recae, principalmente, sobre la lógica de la divulgación no consentida, y no sobre la falsificación identitaria obtenida mediante fabricación sintética.

Tabla 3.

Diferencias entre la violación a la intimidad prevista en el COIP y los deepfakes como contenido sintético no consentido

Elemento de análisis	Artículo 178 COIP. Violación a la intimidad	Deepfakes como contenido sintético no consentido	Limitación identificada
-----------------------------	--	---	------------------------------------

Objeto material de la conducta	Datos personales, mensajes, voz, audio, video o información personal ya existente	Representación sintética falsa creada mediante inteligencia artificial con apariencia de autenticidad	El tipo penal se orienta a material real o previamente existente, no a contenido artificialmente fabricado
Conducta principal	Acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar sin consentimiento	Crear, manipular y eventualmente difundir contenido falso atribuido a una persona real	La creación sintética del archivo no aparece descrita expresamente en la norma
Forma de afectación	Intromisión o difusión ilegítima de información íntima o personal	Suplantación visual o audiovisual, atribución falsa de conductas y exposición degradante de la víctima	La lesión se produce por una técnica distinta a la prevista originalmente por el legislador
Relación con el consentimiento	La falta de consentimiento recae sobre el acceso o difusión de información personal o íntima	La falta de consentimiento recae sobre el uso de rasgos identitarios para fabricar un contenido inexistente	El artículo 178 no regula de forma expresa el uso no consentido de imagen o biometría para crear contenido falso

Posibilidad de subsunción	Puede aplicarse frente a actos de difusión o publicación no consentida	Solo podría utilizarse parcialmente cuando el deepfake ya ha sido difundido	No ofrece cobertura típica suficiente sobre la fase de creación del contenido sintético
---------------------------	--	---	---

Análisis e interpretación

El artículo 178 aporta una respuesta parcial frente al deepfake porque su función típica permanece anclada a una lógica de intromisión o divulgación sobre material preexistente. Esta adyacencia funcional es a la vez explicación de la utilidad periférica, pero no habilita a que pase a ser eje central de la respuesta penal a una técnica comisiva cuya particularidad reside en que el contenido al que se llega es artificial.

La limitación del precepto nos lo muestra como estructural y no cuantitativa. La deficiencia de la norma no se corrige ampliando interpretativamente el significado de sus verbos rectores, porque ello significaría incorporar una figura que no ha sido descrita por el legislador. De este modo, la norma tiene un sentido para ciertos efectos que emergen del fenómeno, pero no puede brindar en su interior una correspondencia típica aproximada a la fabricación de una representación sintética y falsa que se atribuye a una persona determinada. La respuesta penal únicamente desde la perspectiva del artículo 178 provoca, en consecuencia, una asimetría entre lo que acontece y el tipo: mientras que la lesión típica del deepfake se construye en el modo de una construcción artificial de una identidad representada, la norma en vigor responde desde una lógica de acceso o difusión. Aquella distancia es la que justifica la necesidad de una formulación típica más precisa.

4.1.3. Bienes jurídicos comprometidos por los deepfakes

Los deepfakes comprometen de manera concurrente varios bienes jurídicos de relevancia constitucional y penal. En sede constitucional, ello se conecta de forma directa con el artículo 66, numerales 18, 19 y 20, de la Constitución de la República del Ecuador

(2008), que protegen el honor y el buen nombre, la imagen y la voz, la protección de datos personales y la intimidad personal y familiar; en sede penal, esa afectación múltiple explica por qué el fenómeno no se deja reducir de modo suficiente a un único tipo próximo.

El daño cometido no ataca únicamente a un solo interés protegido, sino que ataca a una serie de derechos que necesariamente son interdependientes, como la intimidad, la privacidad, la imagen, el honor, el buen nombre, la dignidad y, en determinados supuestos, la integridad de la víctima. Este carácter de pluralidad de afectaciones no hace sino reforzar que el fenómeno en cuestión es de naturaleza compleja y pluriofensiva, por lo que no está permitido realizar una valoración jurídica que se limite a la falsedad del contenido o a la simple difusión de lo que se presenta como falso.

Tabla 3.

Bienes jurídicos afectados por la creación y difusión de deepfakes

Tabla 4.

Bienes jurídicos afectados por la creación y difusión de deepfakes

Bien jurídico o derecho comprometido	Forma de afectación mediante deepfakes	Proyección jurídico-penal de la afectación
Intimidad (Constitución, art. 66, num. 20)	La víctima es artificialmente situada en escenarios que pertenecen a la esfera más personal o reservada mediante contenidos falsamente atribuidos a su identidad	Se compromete la esfera privada de la persona, aun cuando el contenido sea sintético y no corresponda a un hecho real
Privacidad y protección de datos (Constitución, art. 66,	Uso no consentido de imagen, voz, fotografías, datos biométricos o información	Se afecta el control de la persona sobre sus datos, atributos identitarios y proyección en entornos digitales

num. 19; LOPDP, arts. 1, 4 y 8)	identificable para construir una representación falsa	
Imagen y voz (Constitución, art. 66, num. 18)	Manipulación o reutilización de rasgos visuales o sonoros para atribuir a la víctima apariencias o conductas inexistentes	Se vulnera la representación externa de la persona y su facultad de decidir sobre el uso de su propia imagen
Honra y buen nombre (Constitución, art. 66, num. 18; COIP, art. 182)	Difusión de contenido falso con apariencia verosímil que deteriora la valoración social de la víctima	Se genera descrédito, estigmatización o humillación frente a terceros
Dignidad	La persona es instrumentalizada mediante inteligencia artificial y convertida en objeto de manipulación digital sin consentimiento	Se compromete el valor intrínseco de la persona y su autonomía sobre la propia identidad representacional
Integridad personal	La víctima puede ser expuesta artificialmente en escenas, actos o contextos falsos con consecuencias psíquicas, emocionales y sociales reales	La afectación trasciende lo meramente digital y puede incidir en la integridad psíquica, el desenvolvimiento social y la esfera de dignidad personal de la víctima

Análisis e interpretación

La gravedad jurídica del deepfake proviene de su capacidad para reorganizar artificialmente la posición de la víctima frente a terceros. La lesión no se agota en la falsedad del soporte, sino que alcanza a la representación social de la persona, al ámbito

privado de la persona, al ámbito del control sobre los atributos identitarios que ya reconoce el ordenamiento como dignos de ser tutelados.

La confluencia de lesiones da razón también de la insuficiencia de las respuestas penales parciales. Cuando, en efecto, el fenómeno se enfrenta como si se tratara de intimidad o honra o imagen o datos personales, la reacción normativa queda fragmentada y se pierde de vista la unidad lesiva que introduce el retrato sintético de una determinada persona incorrectamente asumida en esta representación.

En términos de teoría del bien jurídico, esta estructura pluriofensiva exige una lectura unitaria del injusto. La ausencia de una tipificación específica no solo plantea un problema de encuadramiento típico, sino también de comprensión adecuada del alcance lesivo del fenómeno en el marco del derecho penal ecuatoriano.

4.1.4. Aportes del derecho comparado: Colombia y Chile

Tanto Colombia como Chile han comenzado a reconocer de manera más directa los riesgos jurídicos asociados al uso de inteligencia artificial para la creación de deepfakes, aunque mediante técnicas legislativas distintas. En Colombia, ello se observa en el Proyecto de Ley 225 de 2024 Senado y en la información oficial del Senado de la República difundida el 8 de mayo de 2024, donde se señala que la iniciativa busca incluir el delito de falsedad personal para la modalidad de suplantación cuando se usa inteligencia artificial; en Chile, la aproximación se advierte en el Boletín N.º 17795-19, que regula la creación y difusión de imitaciones digitales realistas de imagen, cuerpo o voz generadas mediante inteligencia artificial (Cámara de Diputadas y Diputados de Chile, 2025, pp. 2-4).

Desde dicha combinación, el derecho comparado ofrece criterios útiles para el derecho ecuatoriano, especialmente en lo que respecta al reconocimiento de la inteligencia artificial como medio comisivo, la utilización de atributos identitarios no consentidos y la necesidad de una reacción normativa más firme frente a la producción de contenido lesivo sintético. En lo que concierne a técnica legislativa, el modelo que ofrece Colombia es más cercano al de suplantación y a la falsedad personal, mientras que Chile se acerca con más

precisión a la regulación de las imitaciones digitales realistas de la imagen, la voz y el cuerpo.

Tabla 5.
Derecho comparado sobre regulación o tratamiento jurídico de deepfakes en Colombia, Chile y Ecuador

País	Enfoque identificado	Técnica normativa observada	Aporte para el caso ecuatoriano
Colombia	Reconocimiento del uso de inteligencia artificial en supuestos vinculados con suplantación y falsedad personal (Proyecto de Ley 225 de 2024 Senado; Comisión Primera del Senado, 8 de mayo de 2024)	Incorporación del fenómeno dentro de iniciativas relacionadas con falsedad personal, uso de IA y protección frente a suplantaciones	Aporta criterios para comprender el deepfake como medio de suplantación, engaño e instrumentalización de identidad
Chile	Reconocimiento más explícito en cuanto a imitaciones digitales realistas de imagen, voz y cuerpo producidas mediante inteligencia artificia (Boletín N.º 17795-19, 2025, p. 2)	Proceso de avance hacia proyectos de regulación de la creación y difusión de contenidos sintéticos sin consentimiento y su relación con la violencia digital	Proporciona un punto de referencia más cercano a la naturaleza del deepfake y a la exigencia de regular el uso no consentido de atributos identitarios

		Aplicación	Evidencia
	Ausencia de tipificación penal específica sobre deepfakes y tratamiento fragmentario a través de tipos próximos	indirecta o parcial de figuras vinculadas con intimidad, honra, datos personales o falsedad	insuficiencia normativa y necesidad de una respuesta más precisa frente a la creación y utilización lesiva de contenido sintético

Análisis e interpretación

El derecho comparado confirma que el deepfake ya ha sido jurídicamente reconocido como una modalidad diferenciada de riesgo y, por ello, como un fenómeno que exige una respuesta normativa técnicamente delimitada. La experiencia en la región revela que la inteligencia artificial aquí no responde simplemente a un contexto fáctico, sino que cumple con la función de comisividad, esto es, tiene una incidencia determinante en la construcción de la figura del injusto, en la determinación del objeto material y en la forma de lesión de los bienes jurídicos que se ven comprometidos.

La comparación que se observa entre Colombia y Chile permite proponer dos técnicas de regulación destacadas. La primera tiene una orientación integradora del fenómeno en las figuras asociadas a la falsedad personal y la suplantación; la segunda tiene una orientación más centrada en la creación y difusión de imitaciones digitales fieles y en los usos no consentidos con rasgos de carácter identitario. En este sentido, la diferencia constituye un criterio útil para tratar el caso ecuatoriano, pues pone de manifiesto que la actualización normativa puede construirse con modelos distantes entre sí, pero ello no debe impedir que mantenga las características propias de la claridad típica, la correspondencia con el hecho y la delimitación de alcance de la prohibición penal.

Para el caso ecuatoriano, la significación del derecho comparado es confirmatoria y orientativa. Confirmatoria porque demuestra que el vacío actual no se debe a una imposibilidad conceptual de regulación, sino a un vacío legislativo ante un fenómeno ya

conocido en la región; orientativa porque permite advertir que, en esta instancia, una respuesta correcta jurídicamente debe reconocer de uno u otro modo la idiosincrasia del medio comisivo, la atribuibilidad del contenido a una persona determinada y la capacidad lesiva que permite la representación sintética; de ahí que, en todo caso, el derecho comparado conlleva la confirmación, por un lado, de la viabilidad de una actualización típica que sea coherente con una política criminal garantista y con la legalidad y taxatividad.

4.1.5. Necesidad de una tipificación penal en Ecuador

El ordenamiento penal ecuatoriano se caracteriza por la existencia de una escasa norma relevante en torno a los deepfakes, una escasez de reglamentación más que obvia si se trata del caso en el que se emplea la técnica deepfake para suplantar identidades, para atribuir hechos o conductas, para manipular la imagen o voz de una persona o cuando se afecta la dignidad, la honra, la imagen y la intimidad de la víctima.

Desde el punto de vista del principio de legalidad, recogido en el artículo 76, inciso 3 de la Constitución de la República del Ecuador (2008), y de la exigencia de tipicidad que proclama el artículo 25 del COIP (2014), se materializa un déficit de previsión legal expresa en el caso de una modalidad comisiva tecnológicamente diferenciada. Lo que se encuentra a la base del contenido de los deepfakes con un propósito nocivo, como la suplantación de identidades, la atribución de hechos o conductas falsas o la manipulación de la imagen o voz de una persona, también guarda relación con la falta de una descripción típica expresa que permita afrontar la producción del contenido falso de manera clara y precisa, empleando la inteligencia artificial en el ámbito de la creación de deepfakes.

En definitiva, la reacción penal actual se hace desde la fragmentación y, a su vez, es dependiente de figuras paralelas que no logran incorporar ni la particularidad técnica ni la estructura pluriofensiva del fenómeno. Se puede, por lo tanto, aventurar a partir del análisis documental la posibilidad de sostener la necesidad de una delimitación penal más precisa, más conforme a los principios de legalidad, lesividad, proporcionalidad y mínima intervención. Pues bien, ese perfil no se agota exclusivamente en la sanción de la difusión, sino que también se debe tipificar la creación, manipulación, puesta en circulación y uso de

contenido falso sintético, atribuible a una persona individualizada, que pueda, además, resultar una conducta idónea para lesionar bienes jurídicos esenciales.

En esa dirección, el modelo típico técnicamente más adecuado debería perfilar al menos el objeto material, la ausencia de consentimiento, la atribuibilidad del contenido a una persona determinada y la idoneidad lesiva de la conducta.

Tabla 6.

Elementos jurídicos que sustentan la necesidad de una tipificación penal específica sobre deepfakes en Ecuador

Elemento identificado	Hallazgo documental	Relevancia para la necesidad de tipificación
Déficit de tipicidad expresa	Los tipos penales vigentes solo cubren de manera parcial efectos derivados del fenómeno, pero no la creación misma del contenido sintético	Evidencia un vacío típico respecto del núcleo técnico y lesivo del deepfake
Cobertura fragmentaria del injusto	La intimidad, imagen, honra, dignidad, privacidad e integridad pueden verse comprometidas simultáneamente	Demuestra que el fenómeno presenta una estructura pluriofensiva que no se agota en una sola figura próxima
Límites del artículo 178 COIP	La violación a la intimidad fue diseñada para material real o previamente existente, no para contenido sintético fabricado mediante inteligencia artificial	Confirma que la respuesta penal actual resulta cercana, pero insuficiente

Principio de legalidad y taxatividad (Constitución, art. 76, num. 3; COIP, art. 25)	No es admisible extender por analogía tipos penales vigentes para abarcar conductas no descritas expresamente	Justifica la necesidad de una figura clara que evite interpretaciones extensivas incompatibles con el debido proceso
Derecho comparado regional	Colombia y Chile han avanzado hacia respuestas normativas más próximas al fenómeno	Muestra que la actualización legislativa es jurídicamente viable y coherente con la evolución regional
Protección de la víctima	La ausencia de un tipo específico debilita la tutela penal efectiva frente a nuevas formas de violencia digital	Refuerza la necesidad de una respuesta penal más precisa y congruente con la gravedad del daño

Análisis e interpretación

La necesidad de tipificación específica no surge de una reacción expansiva frente a la novedad tecnológica, sino de una exigencia de coherencia interna del sistema penal. Cuando una modalidad de agresión presenta un núcleo comisivo diferenciable y, pese a ello, solo puede ser abordada a través de figuras próximas, el problema deja de ser meramente interpretativo y pasa a ser de insuficiencia estructural de la ley penal.

La razón decisiva que permite una mejor fundamentación de la respuesta es que el deepfake transforma el esquema habitual de la imputación jurídico-penal del daño, ya que no hay una mera imputación de un resultado dañino que ya está legislado, sino que hay que reconocer que la inteligencia artificial introduce un medio comisivo que es capaz de realizar una representación falsamente atribuible a una persona que es susceptible de perjudicar de una forma convergente diferentes bienes jurídicos. Si tal especificidad no está contemplada en la ley, al sistema no le queda más que reaccionar a través de fórmulas indirectas que merman a la par la protección de la víctima y la certeza del derecho.

En consecuencia, la tipificación específica aparece jurídicamente necesaria porque permite restablecer la correspondencia entre hecho, bien jurídico y descripción típica, evitando vacíos de tutela frente a formas cualificadas de manipulación digital basadas en inteligencia artificial. En ese contexto, la actualización típica no amplía injustificadamente el ius puniendi; más bien, ordena su ejercicio dentro de los límites de legalidad, taxatividad y mínima intervención.

4.2. RESULTADOS DE LAS ENTREVISTAS

Las entrevistas realizadas a una jueza de garantías penales, un fiscal y un defensor público muestran que el tratamiento jurídico de los deepfakes en el Ecuador aún presenta vacíos de tipificación, dificultades de subsunción, problemas probatorios y limitaciones institucionales para su investigación. En la práctica penal, el marco normativo vigente no ofrece una respuesta precisa frente a esta forma de afectación, por lo que resulta necesaria una respuesta jurídica más clara.

4.2.1. Criterios sobre la insuficiencia normativa y la aplicabilidad de los tipos penales vigentes

Las respuestas de los operadores jurídicos coinciden en un punto central: el COIP no ofrece una cobertura suficiente para las conductas cometidas mediante deepfakes.

Aunque el ordenamiento contiene figuras próximas, su alcance sigue siendo parcial frente a una conducta que combina manipulación digital, uso de inteligencia artificial, alteración de identidad y eventual difusión de contenido sexual no consentido.

.Tabla 7.

Criterios sobre la insuficiencia normativa y la aplicabilidad de los tipos penales vigente

Categoría de análisis	Jueza	Fiscal	Defensor público	Resultado comparado	Aporte al objetivo específico
Suficiencia normativa del COIP	Reconoce que existen tipos vinculados con conductas cometidas por medios digitales, pero no una figura específica para deepfakes	Señala que no existe un tipo penal específico para estos hechos	Considera que las normas vigentes no son claras ni precisas para abordar el deepfake como delito autónomo	Los tres operadores coinciden en que el COIP no ofrece una respuesta específica y suficiente frente al fenómeno, aunque reconocen la existencia de figuras próximas	Contribuye a determinar la insuficiencia normativa de la ley penal ecuatoriana (Objetivo específico 1)
Aplicabilidad de los tipos penales vigentes	Menciona violación a la intimidad, suplantación de identidad y otras figuras digitales como referencias parciales	Vincula el problema principalmente con violación a la intimidad, pero sin adecuación clara	Advierte que los tipos existentes no describen el elemento de manipulación mediante inteligencia artificial	Las figuras penales actualmente vigentes solo permiten un encuadramiento parcial, porque no captan de manera expresa la lógica técnica del deepfake	Aporta a examinar los límites de subsunción en la normativa penal vigente (Objetivo específico 1)
Alcance práctico del artículo 178 del COIP	Lo asocia a supuestos próximos, pero no como respuesta específica al fenómeno	Lo reconoce como aproximación cercana, aunque no suficiente	Lo considera una referencia posible, pero incapaz de abarcar integralmente la conducta	El artículo 178 aparece como una vía de aproximación para efectos derivados, especialmente la difusión, pero no resuelve la creación sintética del contenido	Permite evaluar la inoperancia práctica del artículo 178 frente a los deepfakes (Objetivo específico 2)

La insuficiencia normativa del COIP no únicamente se origina a partir de la ausencia de la definición legal correspondiente al deepfake. El problema es de otro tipo y se origina en una incongruencia entre la estructura típica que se encuentra vigente y la forma en que se realiza esta conducta. En la serie de entrevistas se da una coincidencia evidente: las figuras que le son similares fueron creadas para supuestos diversos y, por lo tanto, solo son capaces de abarcar partes del problema; por lo tanto, el problema no es únicamente de tipo terminológico, sino de adecuación típica.

Si tomamos esto como base, el abogado señala que el núcleo del problema reside en la no descripción del elemento técnico que diferencia esta conducta de las otras que se encuentran ya descritas por la ley; el Ministerio Fiscal, desde un punto de vista más técnico, confirma que no se puede realizar una clasificación sencilla; la magistrada reconoce que existen tipos vinculados con conductas realizadas a través de medios informados, pero insiste en que ninguna da respuesta a la lógica propia del deepfake. En conjunto, estas respuestas visibilizarían que la insuficiencia normativa no es equivalente a poder afirmar que no existe tutela de bienes jurídicos tales como la identidad o la intimidad, sino que el marco normativo es incapaz de describir cómo se produce el actuar y el tipo de perjuicio que tiene esta conducta, que en este caso es severo.

Dentro de ese marco, el artículo 178 del COIP opera como una referencia cercana, pero no suficiente. Su utilidad aparece sobre todo en la fase de difusión o en ciertos efectos derivados del hecho. Por eso, su inoperancia práctica debe entenderse como evidencia de que el fenómeno rebasa la lógica típica para la que fue concebida esa norma. El contraste entre los tres entrevistados confirma, así, que el obstáculo principal se encuentra en los límites de subsunción del ordenamiento penal vigente frente a una modalidad de agresión digital que no ha sido prevista de forma expresa.

4.2.2. Dificultades probatorias, de autoría y de afectación a bienes jurídicos

La respuesta penal frente a los deepfakes también se ve condicionada por la complejidad técnica de su investigación. La discusión no recae solo en la existencia del archivo, sino en su autenticidad, en la posibilidad de demostrar su alteración, en la

identificación de su origen y en la reconstrucción de su trazabilidad. En ese escenario, la pericia forense digital adquiere un papel central, pues de ella depende en buena medida la posibilidad de sostener una imputación penal seria.

Tabla 8.

Dificultades probatorias, de autoría y de afectación a bienes jurídicos

Categoría de análisis	Jueza	Fiscal	Defensor público	Resultado comparado	Aporte al objetivo específico
Relevancia de la pericia forense digital	La considera la prueba principal para este tipo de hechos	Reconoce falencias institucionales en materia de pericias digitales en Ecuador	Señala que sin pericia informática especializada no sería posible acreditar la alteración del archivo	La prueba pericial digital constituye el eje técnico de la investigación, aunque su eficacia se ve limitada por debilidades institucionales y falta de especialización	Aporta a identificar las dificultades probatorias del fenómeno investigado (Objetivo específico 2)
Determinación de autoría y formas de participación	Advierte dificultades cuando la conducta se comete desde otro país	Reconoce falta de experiencia práctica para precisar autoría o complicidad	Distingue entre quien crea o altera el archivo y quien lo difunde	La atribución de responsabilidad penal presenta alta complejidad por la intervención posible de varios sujetos y por la dimensión transnacional del fenómeno	Contribuye a comprender los obstáculos prácticos para la imputación penal (Objetivo específico 2)
Bienes jurídicos comprometidos	Destaca integridad psicológica, sexual y protección del dato	Enfatiza la intimidad personal y familiar	Señala afectación a identidad, buen nombre, intimidad e integridad psíquica	Los criterios recogidos muestran una afectación pluriofensiva que compromete intimidad, identidad, honra, integridad psíquica y protección de datos	Aporta a examinar la afectación advertida en la víctima desde la perspectiva de los operadores jurídicos (Objetivo específico 2)

La fragilidad probatoria tiene un vínculo directo con la eficacia del sistema penal, como señala la jueza al enfatizar el valor de la prueba pericial para el reconocimiento de datos de origen y localización; el público defensor destaca que sin la pericia no será posible determinar con certeza la manipulación del archivo; el fiscal, por su parte, reconoce la existencia de fallas institucionales en esta materia. La contraposición de las respuestas pone de manifiesto que la debilidad no es solo jurídica, sino que es, además, técnico-institucional. Por tanto, la respuesta penal podría seguir siendo insuficiente, aun con mayor precisión normativa.

En la misma línea se pone de manifiesto la autoría y la forma de participación. Las respuestas muestran que el deepfake quiebra la linealidad con la que suelen pensarse otras conductas, ya que puede participar quien crea o altera el archivo y, en un momento diferido, quien lo difunde. A ello se suma la dimensión transnacional que resulta evidente para la jueza y la ausencia de una experiencia práctica que señala el fiscal. Por tanto, el problema de la imputación no consiste solo en encontrar un hecho dañino, sino en reconstruir una cadena de intervención muy precisa que puede involucrar a varios sujetos, distintos momentos de la acción y problemas de competencia.

Las respuestas, desde el enfoque de la lesión, coinciden en que el fenómeno no compromete un único bien jurídico. En efecto, el fiscal hace énfasis en la respuesta que ataca a la intimidad, mientras que el defensor público se extiende para dar cuenta de la lesión a la identidad, al buen nombre y a la integridad psíquica; la jueza la amplía e incluye, también, la protección del dato personal y la integridad psicológica y sexual, motivo por el cual esta diversidad de énfasis no hace que se quiebre la coherencia del resultado; antes bien, sostiene que el deepfake se entienda como una forma de agresión digital de alcance pluriofensivo, capaz de llevar aparejadas consecuencias reales para la víctima y de exigir, por tanto, una respuesta penal que no reduzca el problema a la sola difusión del archivo.

4.2.3. Criterios sobre reforma normativa, límites de intervención penal y fortalecimiento institucional

. La discusión pasa de una idea general de reforma a un debate más técnico sobre el alcance legítimo de la intervención penal. Mientras el fiscal se inclina por la creación de un tipo penal específico y la jueza defiende una respuesta legislativa más clara dentro de un marco de protección más amplio, el defensor público introduce una advertencia garantista: no toda utilización no autorizada de imagen, voz o contenido digital amerita criminalización.

Tabla 9.

Criterios sobre reforma normativa, límites de intervención penal y fortalecimiento institucional

Categoría de análisis	Jueza	Fiscal	Defensor público	Resultado comparado	Aporte al objetivo específico
Necesidad de reforma normativa	Considera necesaria una respuesta legislativa más clara	Se inclina por la creación de un tipo penal específico	Prefiere una revisión cautelosa, orientada a reformar tipos existentes	Existe acuerdo en la necesidad de revisar el marco penal, aunque difieren en la técnica legislativa más adecuada para hacerlo	Contribuye a sustentar la necesidad de una propuesta de reforma en el COIP (Objetivo específico 3)
Límites de la intervención penal	Prioriza la protección de la persona y sus datos frente al daño generado	No desarrolla ampliamente este punto, pero apoya la tipificación	Advierte que no toda utilización no autorizada debe criminalizarse	La respuesta penal debe diferenciar entre afectaciones graves, especialmente las de contenido sexual no consentido, y supuestos que no justifican intervención punitiva	Aporta a delimitar una respuesta penal compatible con legalidad, proporcionalidad y mínima intervención (Objetivo específico 3)
Fortalecimiento institucional y cooperación	Subraya la cooperación internacional y la competencia transnacional	Reconoce insuficiencias prácticas en el tratamiento del fenómeno	Destaca necesidad de inversión en tecnología, pericia y capacidad investigativa	La actualización normativa debe ir acompañada de capacidades reales de investigación digital, pericia especializada y cooperación entre instituciones y Estados	Sirve de base para formular lineamientos de respuesta institucional complementarios a la reforma normativa (Objetivo específico 3)

Este contraste permite delimitar con mayor exactitud el objeto de una posible reforma. Las entrevistas no llevan a un aumento de lo punitivo, sino a la necesidad de diferenciar, por un lado, entre supuestos de lesividad grave, sobre todo en relación con los supuestos de contenido sexual no consentido, y, por otro, entre unos supuestos que no justificarían una respuesta penal. A esta altura, el principal aporte del criterio del defensor público no es la negación de la necesidad de que haya regulación, sino la defensa de que todas las propuestas respeten el principio de legalidad, el principio de proporcionalidad y el principio de mínima intervención. Y de ahí la reafirmación de que la actualización normativa tiene que realizarse de manera precisa y no mediante fórmulas amplias o inciertas.

Además, las entrevistas no reducen la reforma a la sola creación de un tipo penal. La jueza incorpora la protección del dato personal, de la identidad y de la integridad psicológica y sexual como ejes de una regulación futura, mientras que el fiscal la relaciona con la intimidad personal y familiar. En la misma línea, los criterios incluidos manifiestan que una reforma legislativa ofrece muy poco si ella no es acompañada por unas capacidades reales de investigación digital, de especialización pericial y de cooperación internacional. Esto es indicativo de que no se soluciona el problema solo con la ley.

Por tanto, el resultado de la comparación con las entrevistas constituye una base útil para la elaboración de la propuesta de investigación. Existe soporte para la propuesta de una revisión del COIP; ahora bien, esta revisión debe ir acompañada de delimitación material del injusto, criterios de intervención mínima y potenciación institucional. Por tanto, la respuesta penal no puede ser pensada como algo aislado, sino como parte de una estrategia de protección frente a nuevas formas de violencia digital.

Finalmente, los criterios de los operadores jurídicos resaltan que la respuesta penal que resulta frente a los deepfakes es insuficiente no solo por los límites de adecuación típica, sino también por la complejidad probatoria y por las limitaciones institucionales que dificultan su investigación. Además, la problemática compromete bienes jurídicos como la

intimidad, la identidad, la integridad psíquica y la protección de datos personales. Todo ello refuerza la necesidad de una respuesta normativa e institucional más precisa dentro del sistema penal ecuatoriano.

4.3. Discusión

4.3.1. Insuficiencia normativa del COIP frente a los deepfakes

El ordenamiento ecuatoriano reconoce y protege bienes jurídicos como la intimidad, la imagen, la honra y los datos personales. Sin embargo, esa tutela no se evidencia en una tipificación penal puntual sobre la creación sintética de contenido falso por parte de la inteligencia artificial. Así, el problema no será la demostración del desamparo jurídico, sino que se debe a la inexistencia de una previsión de carácter penal expresa para dicha figura comisiva. La carencia de protección se produce precisamente ahí: los bienes jurídicos están efectivamente reconocidos, pero la conducta que los lesiona en esta dirección no aparece descrita con la nitidez propia del derecho penal.

Arévalo Fernández (2024) ya anticipó que la legislación ecuatoriana no era suficientemente amplia para hacer frente a las víctimas del deepfake. Dicho diagnóstico se muestra certero, pero aquí adquiere un sentido mucho más preciso; pues la insuficiencia no se reduce a un problema normativo ni a la simple no existencia de una mención legal del fenómeno, sino a que lo clave es que el COIP no ofrece una formulación típica válida para encajar la creación artificial de los contenidos que se asignan erróneamente a una persona identificable. Así, la vacuidad no sería solo terminológica, sino que adquiriría un sentido estructural, porque afecta al propio encaje típico de la conducta..

La misma línea puede advertirse en Caiza, Marfetan y Machado (2025), quienes señalaron la ausencia de regulación específica sobre evidencias generadas con inteligencia artificial. No obstante, ese antecedente se concentra en la autenticidad y en la aceptación probatoria del material manipulado. Aquí la cuestión se desplaza a un plano anterior: la tipicidad penal de la conducta. Por eso, la insuficiencia normativa no incide únicamente en la valoración posterior del archivo, sino también en la posibilidad de contar con una base penal clara desde el inicio. En ese punto se debilita la correspondencia entre hecho, bien

jurídico y tipo penal, que es precisamente donde una respuesta jurídico-penal comienza a perder consistencia.

4.3.2. Límites del artículo 178 del COIP y problemas de subsunción

El artículo 178 del COIP es, dentro del régimen vigente, una de las referencias más cercanas al fenómeno estudiado, pues regula conductas de acceso, reproducción, difusión o publicación no consentida de información, voz, audio o video. Sin embargo, esa cercanía no es suficiente para satisfacer el problema de forma adecuada. El deepfake no siempre agota la difusión del archivo. De hecho, en un número considerable de ocasiones, el propio núcleo de la conducta se encuentra antes, en la confección artificial de una representación falsa con aspecto de veracidad. Desde esta línea de razonamiento, el tipo vigente solo prevé momentos posteriores del hecho, pero no respecto de la conducta base que lo permite.

Arévalo Fernández (2024) argumenta que las normas vigentes sobre la intimidad son insuficientes para explicar lo que resulta del deepfake. La coincidencia con esta afirmación es evidente, aunque aquí la problemática se plantea con un mayor rigor dogmático. El problema no es solo un problema normativo de desactualización, sino de subsunción. El artículo 178 parte de un objeto material real o preexistente. Dado que el deepfake es creación sintética de un contenido, esa fase previa no cuenta con una descripción típica expresa en el precepto vigente.

En una línea parecida, Caiza, Marfetan y Machado (2025) concluyen que, aunque se trata de un archivo manipulable a través de la pericia, persiste un problema anterior: la ausencia de un tipo penal que describa de manera clara la creación sintética como conducta relevante, motivo por el cual el artículo 178 solo ofrece una cobertura periférica de la circulación del archivo, sobre todo en lo que respecta a casos de difusión no consentida.. No alcanza, en cambio, a recoger de forma integral la estructura del injusto advertida en esta investigación. Por eso su aplicación no puede llenar con suficiencia el vacío típico sin tensionar la legalidad estricta y la taxatividad, límites que en derecho penal no admiten desplazamientos interpretativos amplios.

4.3.3. Afectación pluriofensiva y desprotección de la víctima

Los resultados muestran que el deepfake no produce una afectación aislada. La creación y la difusión de contenidos sintéticos falsamente atribuibles a una persona puede comprometer, de forma concurrente, la intimidad, la imagen, la honra, la dignidad, los datos personales e incluso la integridad psíquica. De esta forma, la conducta evidenciaría una configuración pluriofensiva que impide reducir el fenómeno a una figura penal cercana. La desprotección de la víctima no está solo explicada por la falta de sanción, sino más bien por la insuficiencia de una respuesta penal que fuera capaz de captar la complejidad de la lesión.

Arévalo Fernández (2024) relaciona aquella labor de elaboración de las imágenes, es decir, el deepfake, con la afectación a la imagen, la honra, la dignidad y el buen nombre; planteamiento que se mantiene con el carácter observado, aunque a continuación se revisa desde un prisma más estrictamente dogmático. No se trata de ir enumerando derechos coartados, sino de dar cuenta de una dinámica del injusto que rebasa la lógica de tipos contruidos para lesiones yuxtapuestas. En esta línea, Caiza, Marfetan y Machado (2025) hacen ver que el deepfake pone en riesgo varios bienes jurídicos, y esta investigación analiza la cuestión, pero desde la perspectiva concreta de la víctima y el límite de una posible reacción normativa fragmentada y dispersa. Las entrevistas avalan tal perfil poco favorable.

Los operadores jurídicos diseccionan las afectaciones simultáneas de la intimidad, de la identidad, del buen nombre, de la integridad psicológica y de la tutela de datos.. En definitiva, la desprotección de la víctima no se convierte en una fórmula vacía de contenido, sino que es, más bien, el trasunto del desfase entre la complejidad del daño y la protección jurídica disponible. La respuesta penal en vigor da cuenta de las manifestaciones parciales del hecho, pero no constituye una forma de aprehender la unidad lesiva de una acción que altera artificialmente la posición jurídica y social de la persona afectada respecto a los terceros..

4.3.4. Dificultades probatorias, de autoría y de investigación penal

La discusión sobre los deepfakes no termina en la tipificación penal. Su investigación exige prueba técnica suficiente sobre la alteración del archivo, su trazabilidad y la identificación de quienes intervinieron en el hecho. En esa situación, la criminalística de las tecnologías digitales ocupa un lugar central. De ella dependerá no solo la comprobación de la manipulación, sino también la correspondiente atribución del hecho de forma más sólida y la aclaración de la posible intervención de los responsables. La carencia advertida por ello no es solo normativa, sino también probatoria e institucional.

Desde la postura de Caiza, Marfetan y Machado (2025) se había evidenciado una brecha entre la tecnología de los deepfakes y la posibilidad que se daba desde el Estado ecuatoriano. El comentario se corroboró en las entrevistas con las y los participantes, pero también permitió ver otra dimensión del problema. La limitación a la hora de probar las modificaciones del archivo no es solo técnica, sino que además ha de reconstruir autorías, modalidades de participación e incluso, en ciertos casos, obstáculos relacionados con la competencia por un problema ligado con la transnacionalidad de los hechos. Eso ha posibilitado también pautar la discusión del tema más allá del mero archivo falso y abrir la posibilidad de plantear una acusación penal congruente.

Una eventual reforma del Derecho penal, aunque mejore la claridad típica, se antojaría insuficiente si no va acompañada de fortalecer la capacidad pericial, la capacidad investigadora y la cooperación interinstitucional. La respuesta jurídica ha de ser pensada de manera integral. No basta describir normativamente la conducta.. También hace falta dotar al sistema de herramientas idóneas para su comprobación, atribución y juzgamiento conforme al debido proceso.

4.3.5. Derecho comparado y viabilidad de una reforma penal en Ecuador

El derecho comparado muestra que el fenómeno de los deepfakes ya comenzó a recibir atención normativa en otros países de la región. Los resultados de esta investigación indican que Colombia y Chile han desarrollado aproximaciones distintas, aunque útiles para

el caso ecuatoriano. En Colombia, el problema se conecta con la suplantación, la falsedad personal y la inteligencia artificial como medio comisivo. Frente a la cuestión de la prohibición, la regulación en Chile es más certera en cuanto a las representaciones digitales realistas de la imagen, la voz y el cuerpo, así como con la incorporación de la violencia digital. Esas referencias pueden permitirnos valorar si existe viabilidad jurídica para plantear una reforma penal en Ecuador, así como qué cautelas deben ser necesarias para abordarla.

Arévalo Fernández (2024) sugiere ya recurrir al derecho comparado para evidenciar el atraso de la legislación ecuatoriana. Esa vía es válida. Sin embargo, el estudio que se ha llevado a cabo demuestra que la solución no acepta únicamente un modelo legislativo, sino varios tipos de respuesta. Su función no está, sin embargo, en replicar, sino en extraer criterios dignos para el contexto ecuatoriano, entre los que cabe contar el reconocimiento expreso de la inteligencia artificial como medio comisivo, el uso no consentido de los rasgos identitarios, así como la delimitación de los supuestos de especial lesividad..

Las entrevistas, si bien refuerzan esa viabilidad, recogen también las cautelas necesarias. Por un lado, algunos operadores tienden a adoptar una tipificación concreta, mientras que otros apuntan el matiz de que toda reforma debe respetar la legalidad, la taxatividad, la proporcionalidad y la mínima intervención. Tal y como también viene a indicar la revisión del derecho comparado, el hecho de que la reforma del derecho penal de los deepfakes en el Ecuador no solo es jurídicamente viable, sino que, en todo caso, hay que construirla de forma suficientemente precisa para describir acertadamente la conducta prohibida y evitar de esta manera que se generen expansiones punitivas incompatibles con un modelo garantista.

En conclusión, la discusión permite sostener que la falta de una tipificación penal sobre los deepfakes en Ecuador no puede considerarse una omisión menor, cuando en el fondo hay un déficit en la protección de las víctimas y en la reacción del sistema penal. El déficit normativo del COIP, los límites del artículo 178 del COIP, la configuración pluriofensiva del daño y las dificultades probatorias e institucionales son pautas que

configuran un escenario de desprotección que difícilmente puede solucionarse de manera adecuada con las figuras penales actuales.

A su vez, el derecho comparado muestra que una actualización normativa es viable, siempre que respete los principios de legalidad, taxatividad, proporcionalidad y mínima intervención. De ahí que la ausencia de tipificación específica no solo limite la sanción penal, sino que también debilite la tutela efectiva frente a nuevas formas de agresión digital basadas en inteligencia artificial.

5. CAPÍTULO V. PROPUESTA DE REFORMA AL CÓDIGO ORGÁNICO INTEGRAL PENAL FRENTE A LOS DEEPFAKES

5.1. Fundamentación de la propuesta

La regulación penal ecuatoriana no contiene una tipificación específica frente a las conductas realizadas mediante deepfakes. Aunque el ordenamiento vigente protege bienes jurídicos como la intimidad, la imagen, la honra, la dignidad y la protección de datos personales, reconocidos en la Constitución de la República del Ecuador y desarrollados en la Ley Orgánica de Protección de Datos Personales, esa tutela resulta insuficiente cuando el hecho consiste en la creación, manipulación o difusión de contenido sintético falsamente atribuible a una persona identificada o identificable. En tales casos, la respuesta penal se encuentra finalmente respaldada en figuras afines que no recogen con exactitud la especificidad técnica de tal afectación.

En realidad, la principal deficiencia consiste en la falta de una descripción típica expresa del núcleo comisivo del deepfake, es decir, de la fabricación sintética de contenido que tenga una apariencia de realidad mediante inteligencia artificial u otras técnicas por el estilo. La respuesta penal que se sigue concluye en los tipos que únicamente recogen efectos posteriores, como es la difusión no consentida o la afectación al honor, y no en la conducta que origina el daño en sí ni en el razonamiento técnico que la hace posible. Desde esa perspectiva, estamos ante un déficit normativo no solo de tipo terminológico, sino de tipo estructural, enfrentándose al riesgo de lesionar la adecuación típica que exige el art. 25 del Código Orgánico Integral Penal y desvincular el hecho, el bien jurídico y la descripción legal.

A su vez, esa insuficiencia se va a ver potencialmente potenciada por los riesgos que genera una interpretación extensiva que se aleje del contenido del artículo 76 numeral 3 de la Constitución de la República del Ecuador.. A lo anterior hemos de acompañar la naturaleza pluriofensiva del fenómeno, en tanto el uso de los deepfakes puede afectar de forma concurrente la intimidad, la privacidad, la imagen, la honra, la identidad representacional, la dignidad o, incluso, la integridad psíquica de la persona que los padece.

De modo que no se trata de un simple cambio digital carente de relevancia, sino de un tipo de agresión tecnológica diferenciada con apreciable capacidad para generar consecuencias jurídicas y sociales de gravedad.

En tal sentido, la reforma se justifica en la necesidad de una respuesta normativa más ajustada a los principios de legalidad, taxatividad y mínima intervención, que no solo permitirá acortar la falta de respuesta, sino también superar los límites de figuras próximas como el artículo 178 del Código Orgánico Integral Penal y lograr una mayor certeza del derecho. Tal necesidad se ve corroborada por el derecho comparado, especialmente por los avances en el reconocimiento del fenómeno del deepfake que se observan en Colombia y en Chile, en cuanto ya se convirtió en un problema jurídico que ha exigido una respuesta legislativa concreta o una regulación más cercana a su estructura técnica.

5.2. Finalidad y alcance de la propuesta

Dicha reforma introduce en el Código Orgánico Integral Penal una respuesta exacta ante la creación, manipulación o difusión de deepfakes cuando estas conductas sean potencialmente idóneas para lesionar bienes jurídicos reconocidos por el sistema penal. Su finalidad es proveer al sistema penal de una fórmula legal expresa que permita tratar esta problemática, dado que el fenómeno de los deepfakes se enmarca dentro de su propia configuración material sin tener que depender de interpretaciones forzadas a partir de tipos penales cercanos. De hecho, la remisión a figuras cercanas, como la violación a la intimidad o la calumnia, no basta para dar cuenta de una conducta que contiene manipulación tecnológica, atribución personal, apariencia de autenticidad y potencialidad de lesionar un ámbito indeterminado de bienes jurídicos.

En esta línea, la propuesta delimita como objetivo una figura autónoma que permita tratar la cuestión en función de sus propios componentes, pero sin llegar a extender la respuesta penal a todas las manipulaciones digitales y a cualquier manipulación que conlleve la utilización de inteligencia artificial. En definitiva, quedan excluidos aquellos supuestos inocuos, aquellos supuestos donde la hipotética conducta no es idónea para lesionar un derecho de carácter penal, así como también actuaciones manipulativas que no

tengan la potencialidad de causar una lesión jurídicamente relevante. En consecuencia, la respuesta punitiva queda reservada para aquellos casos en los que la utilización no consentida de elementos identificativos de una determinada persona se produce mediante procedimientos tecnológicos con potencialidad de confeccionar contenido sintético falsamente atribuible.

Esta delimitación únicamente resulta operativa siempre que el contenido sea apto para lesionar la intimidad, el honor, la imagen, la dignidad, la identidad y la garantía de la protección de datos de carácter personal. Así, la propuesta se ciñe a los principios de la legalidad, la lesividad y la proporcionalidad correspondientes a la pena. La reforma, frente a una lógica del castigo expansivo, por el contrario, responde a un imperativo de precisión normativa frente a una forma de agresión digital que, en la actualidad, provoca problemas de subsunción y debilitación, por ende, del acceso a una tutela efectiva para la víctima dentro del sistema penal ecuatoriano. La delimitación también es coherente con los resultados documentales, con las pautas recogidas en entrevistas y con las referencias comparadas que se han examinado en el desarrollo de la investigación.

5.3. Proyecto de reforma legal

5.3.1. Exposición de motivos

El desarrollo acelerado de la inteligencia artificial ha dado lugar a nuevas formas de manipulación digital, entre las cuales destacan los deepfakes, entendidos como contenidos sintéticos de imagen, audio o video capaces de atribuir falsamente a una persona acciones, expresiones o contextos inexistentes con apariencia de autenticidad. Los riesgos de afectación a la intimidad, la imagen, la honra, la dignidad, la identidad y la protección de datos de carácter personal, así como demás subámbitos de tutela reconocidos, son más amplios a raíz del fenómeno descrito, al incrementar su ámbito de acción. Tal es el caso del derecho penal contemporáneo; este fenómeno puede agravar el problema, si se entiende que se debe tomar en consideración el efecto de la forma de actuar y la magnitud de la consecuencia.

En el ordenamiento jurídico ecuatoriano, el Código Orgánico Integral Penal ofrece figuras cercanas que pueden contribuir, aunque de forma parcial, a la correcta cobertura de los efectos del uso de deepfakes, en especial en materia de la difusión no consentida de contenido o de afectación del honor, pero el ordenamiento vigente no prevé una tipificación que describa la creación, manipulación o utilización de contenido sintético que sea erróneamente atribuible a una persona identificada o identificable mediante inteligencia artificial.

El resultado de ello es la producción de problemas de adecuación típica, la producción de respuestas interpretativas dispersas y la no producción de un tipo penal protector frente a una forma comisiva distinta desde el punto de vista de las últimas tecnologías de la comunicación e información. En concreto, el artículo 178 del Código Orgánico Integral Penal no pone en relación correctamente el estadio de la creación sintética del contenido, mientras que el artículo 25 de la ley expresa que debe existir una exposición típica concreta de la conducta penalmente relevante.. Por lo tanto, la introducción de una respuesta penal más específica frente a las conductas realizadas mediante deepfakes es conforme con el Código Orgánico Integral Penal en los nuevos escenarios de afectación por la utilización indebida de las nuevas tecnologías y mantiene la respuesta del Estado dentro de los parámetros de legalidad, tipicidad, lesividad, proporcionalidad y mínima intervención.

A su vez, esta necesidad de actualización encuentra respaldo en el derecho comparado, pues los avances observados en Colombia y Chile evidencian que el fenómeno ya ha sido reconocido en la región como una modalidad de afectación que exige respuesta legislativa específica o una regulación más próxima a su estructura técnica.

5.3.2. Considerandos

CONSIDERANDO:

Que la Constitución de la República del Ecuador reconoce y garantiza el derecho al honor y al buen nombre, la protección de la imagen y la voz de la persona, la protección de datos personales y el derecho a la intimidad personal y familiar;

Que el principio de legalidad exige que toda conducta penalmente relevante se encuentre descrita de manera previa, expresa y taxativa en la ley;

Que el desarrollo de la inteligencia artificial ha dado lugar a nuevas formas de manipulación sintética de imagen, audio y video, conocidas como deepfakes, con capacidad para afectar bienes jurídicos de relevancia constitucional y penal;

Que la legislación penal vigente no contiene una regulación específica que permita responder con suficiente precisión a la creación, manipulación o difusión de contenido sintético falsamente atribuible a una persona;

Que resulta necesario adecuar el Código Orgánico Integral Penal a las nuevas formas de afectación derivadas del uso indebido de tecnologías de inteligencia artificial, a fin de fortalecer la protección de los derechos fundamentales y la seguridad jurídica;

5.3.3. Fórmula de expedición

LA ASAMBLEA NACIONAL

EXPIDE:

LA SIGUIENTE LEY REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL
PENAL FRENTE A LOS DEEPFAKES

5.3.4. Articulado de la reforma

Artículo 1.- Incorpórese a continuación del artículo 178 del Código Orgánico Integral Penal el siguiente artículo innumerado:

“Artículo innumerado.- Creación y difusión lesiva de contenido sintético falsamente atribuible.- La persona que, mediante inteligencia artificial o tecnologías análogas, cree o altere imagen, audio o video, de modo que el contenido resulte falsamente atribuible a una persona natural identificada o identificable, sin su consentimiento y con aptitud para lesionar su intimidad, imagen, honra, dignidad, identidad o protección de datos personales, será sancionada con pena privativa de libertad de uno a tres años.

Con la misma pena será sancionada la persona que difunda dicho contenido en conocimiento de su carácter sintético y de su atribuibilidad falsa.

La pena será de tres a cinco años cuando la conducta se realice con finalidad de extorsión, intimidación, lucro, descrédito o suplantación de identidad, o cuando la difusión se efectúe mediante medios de acceso abierto o plataformas que faciliten su reproducción masiva.

No constituirá infracción penal la utilización de tecnologías de inteligencia artificial o de manipulación digital cuando no exista atribuibilidad lesiva respecto de una persona identificada o identificable ni aptitud para comprometer bienes jurídicos protegidos.”

5.3.5. Disposición final

Disposición final.- La presente ley reformativa entrará en vigencia a partir de su publicación en el Registro Oficial.

5.4. Justificación técnico-jurídica del articulado

La propuesta normativa incorpora una descripción típica más precisa frente a las conductas realizadas mediante deepfakes, ya que el ordenamiento penal ecuatoriano no contiene actualmente una formulación expresa capaz de captar el núcleo comisivo de este fenómeno. La elaboración del artículo en cuestión se articula en relación con elementos esenciales, entre ellos, el uso de inteligencia artificial o tecnologías análogas, la creación o alteración de imagen, audio o video, la atribuibilidad falsa del contenido a una persona identificada o identificable, la no existencia de autorización con carácter previo y la

capacidad lesiva respecto de bienes jurídicos tutelados. Esta elaboración se corresponde con el requerimiento de tipicidad que se encuentra regulado en el artículo 25 del Código Orgánico Integral Penal y el principio de legalidad del artículo 76 numeral 3 de la Constitución de la República del Ecuador.

Asimismo, la alusión a imagen, audio o video evita las fórmulas excesivamente abiertas y recoge de una forma más exacta la forma en la que operan los deepfakes. De la misma manera, la exigencia de que el contenido pueda resultar erróneamente asignado a una persona en concreto introduce un criterio de delimitación más severo, pues impide extender el tipo a supuestos en los que no opera una concreta vinculación individual. Así, el artículo no sanciona cualquier manipulación digital, sino únicamente aquella que proyecta artificialmente la identidad de una persona en un contexto por el que se perjudica la imagen, la voz, la intimidad y el honor, conforme a la protección constitucional de los mismos, sin olvidar la protección de datos personales que ya es objeto de una legislación especial.

Igualmente, la elección de los verbos crear, alterar y difundir responde a una exigencia de mayor taxatividad. La conducta básica recaerá en la creación o modificación del contenido sintético y la difusión se castigará por separado en el caso de que el autor actúe plenamente consciente de la naturaleza sintética del contenido y de la falsedad de su atribución. Así, se superará lo que ya concede el artículo 178 del Código Orgánico Integral Penal, dado que se proyecta específicamente al contenido preexistente, y se alcanzará a evitar confundir la producción de contenido con la mera difusión en el caso de que el producto sea sintético y se evidencie la falsedad de su atribución.

Un requisito de esta propuesta consiste en no eliminar automáticamente la aplicación del artículo 178 del Código Orgánico Integral Penal, pues la propuesta se dirige a una hipótesis distinta de producción o modificación de un contenido sintético falsamente atribuible y a su difusión a sabiendas de la falsedad de la atribución. Al mismo tiempo, el artículo 178 es completamente útil para hacer frente a la difusión no consentida de material

genuino o preexistente. Así pues, esta distinción nos va a permitir limitar los conflictos de interferencia, además de permitir una relación sistemática de la reforma.

El agravante vinculado con extorsión, intimidación, lucro, descrédito o suplantación de identidad tiene que ver con criterios más objetivos de delimitación, pues se relaciona con fines concretos que son los que aumentan la lesividad de la conducta. Igual que el hecho de la difusión frente a medios de acceso abierto o plataformas que favorecen la reproducción masiva, en tanto que ello justifica un mayor reproche ante la ampliación del daño y por la mayor dificultad para contener el contenido. La propuesta de pena guarda sentido en el ámbito de proporcionalidad a partir de las figuras próximas del propio Código Orgánico Integral Penal.

La pena de base de uno a tres años responde a lo dispuesto por el artículo 178, y también aquí se prevé una pena de uno a tres años para la violación de la intimidad, lo cual parece razonable, porque la propuesta también protege bienes jurídicos relativos a la intimidad, a la imagen o a la información personal, aunque lo hace respecto de una modalidad técnica distinta. Al tiempo, es capaz de superar la reacción sancionadora prevista para la calumnia del artículo 182, que es sancionada con una pena de seis meses a dos años, porque el deepfake no queda reducido a una simple imputación de contenido falso, sino que incorpora una reproducción sintética de rasgos identificatorios, una apariencia de autenticidad y una mayor capacidad de expansión de la lesión.

La pena agravada de tres a cinco años responde a casos donde concurren finalidades de intensificación del injusto o mecanismos de propagación que multiplican la lesividad del contenido, de manera que la respuesta punitiva respeta una relación de proporcionalidad con la gravedad del hecho que queda descrita.. Finalmente, la cláusula de exclusión cumple una función garantista, ya que impide que la norma se interprete de forma expansiva respecto de usos tecnológicos carentes de atribuibilidad lesiva o de afectación jurídicamente relevante. En consecuencia, la propuesta ofrece una respuesta penal más clara, compatible con la legalidad, la taxatividad y la mínima intervención.

5.5. Viabilidad de la propuesta

Considerada la propuesta desde el punto de vista del ordenamiento ecuatoriano, se concluye que es perfectamente viable, ya que se ampara en bienes jurídicos ya reconocidos por la Constitución de la República del Ecuador, así como por el sistema penal vigente, tales como la intimidad, la imagen, la honra, la dignidad o la protección de datos de carácter personal. Así las cosas, no se está proponiendo una tutela de alcance diferente al marco jurídico nacional, sino que se está armonizando la respuesta penal que se debe ofrecer ante una modalidad tecnológica que no goza de un tipo penal lo suficientemente adecuado en la actualidad.

Desde la perspectiva constitucional, la reforma es compatible con el principio de legalidad, ya que presenta una conducta de modo más claro y expreso ante una situación que hoy en día genera problemas de subsunción y que disminuye el riesgo de interpretaciones extensivas no compatibles con el artículo 76 numeral 3 de la Constitución de la República del Ecuador; en el plano del Derecho penal, también es compatible con la estructura del Código Orgánico Integral Penal, ya que no expande indefinidamente el castigo, sino que ofrece una respuesta específica e individualizada a una conducta diferenciada desde el punto de vista tecnológico, a la par que reconoce la exigencia de tipicidad del artículo 25 y las limitaciones que advertía respecto a la aplicación del artículo 178.

Igualmente, la propuesta puede relacionarse con la metodología cualitativa, documental e interpretativa de la investigación y con los resultados previos sobre la insuficiencia normativa, los límites del artículo 178 y la necesidad de una tipificación más concreta, así como con la viabilidad más práctica que confieren los resultados de la investigación, que muestran insuficiencia normativa, problemas de adecuación típica y necesidad de actualización normativa, junto con el derecho comparado y la relación de los referentes de Colombia y Chile, que muestran la adecuación normativa frente a conductas realizadas con deepfakes.

6. CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La normativa penal ecuatoriana no ofrece, en su estado actual, una respuesta suficiente frente a los deepfakes, pues el Código Orgánico Integral Penal no incorpora una tipificación penal específica que describa de manera expresa la creación, manipulación o utilización de contenido sintético falsamente atribuible a una persona identificable. Esa ausencia repercute directamente en la adecuación típica de la conducta y restringe la posibilidad de una respuesta punitiva clara dentro de los límites de la legalidad y la taxatividad.

El artículo 178 del Código Orgánico Integral Penal tampoco es adecuado para la creación o para la difusión de deepfakes. En efecto, su estructura habitual apunta, mayoritariamente, a actividades de acceso, reproducción o difusión no autorizadas de material ya existente, pero no prevé la construcción del contenido a través de la inteligencia artificial. A ello se añaden dificultades de tipo dogmático y probatorio, pues la conducta estudiada afecta de manera concurrente a la intimidad, la imagen, la honra, la dignidad, la identidad, la privacidad y la integridad personal, por no hablar de las dificultades que conlleva la autoría, la trazabilidad y la verificación forense en la fase procesal.

Por último, la revisión del derecho comparado en Colombia y en Chile permite aventurar que la reforma del derecho penal ecuatoriano no solo es posible, sino que es necesaria. Los avances mostrados en esos sistemas de derecho evidencian que el fenómeno ya se está comenzando a tener como una variante de afectación jurídica relacionada con la suplantación, la falsedad y el uso no consentido de atributos identitarios. Por lo tanto, la propuesta de reforma desarrollada en los resultados que hemos alcanzado se encuentra alineada con los principios de legalidad, lesividad, proporcionalidad y mínima intervención..

6.2. Recomendaciones

Se recomienda incorporar en el Código Orgánico Integral Penal una tipificación penal específica para la creación, manipulación y utilización de deepfakes cuando estas conductas lesionen bienes jurídicos como la intimidad, la imagen, la honra, la dignidad, la privacidad, la identidad o la integridad personal. Una formulación típica precisa reduciría los problemas de subsunción y reforzaría la certeza jurídica frente a esta modalidad de conducta.

Es necesario fomentar la capacidad de las instituciones del sistema de justicia penal mediante la especialización de jueces, fiscales, abogados de oficio y peritos en evidencias digitales e inteligencia artificial, informática forense, autenticidad de archivos, trazabilidad y autoría. Se requiere especialización técnica para mejorar la investigación, la apreciación de la prueba y el acceso a la tutela judicial efectiva de las víctimas.

Es importante tener en cuenta los criterios que nos ofrece el derecho comparado, sobre todo la legislación colombiana y la chilena, acerca del reconocimiento de la inteligencia artificial como medio comisivo, el uso no consentido de los atributos identificadores de la víctima y la conveniencia de una delimitación típica bien determinada de las penalizaciones a través de la utilización de la inteligencia artificial. La consideración de estas experiencias puede ser útil para una regulación penal bien determinada, a la vez garantista y adaptada a las nuevas manifestaciones de la criminalidad tecnológica.

BIBLIOGRAFÍA

Adeoye-Olatunde, O., & Olenik, N. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy*, 4(10), 1358-1367. <https://docs.lib.purdue.edu/phprpubs/6/>

Arévalo Fernández, N. (2024). *La omisión del delito de deepfake en el Código Orgánico Integral Penal en Ecuador*. Universidad Católica de Cuenca. <https://dspace.ucacue.edu.ec/bitstreams/225cef55-862e-40d9-8718-fd977a7b63d3/download>

Arias-Odón, F. (2023). Investigación documental, investigación bibliométrica y revisiones sistemáticas. *REDHECS: Revista Electrónica de Humanidades, Educación y Comunicación Social*, 31(22), 9-28. <https://dialnet.unirioja.es/descarga/articulo/9489470.pdf>

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador*. <https://www.asambleanacional.gob.ec/es/constitucion-republica-ecuador>

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador*. <https://www.asambleanacional.gob.ec/es/constitucion-republica-ecuador>

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. https://www.unodc.org/cld/uploads/res/document/ecu/2014/codigo_organico_integral_penal_html/Codigo_Organico_Integral_Penal_2014.pdf

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. <https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos>

Biblioteca del Congreso Nacional de Chile. (2022). *Delitos informáticos*. <https://www.bcn.cl/leychile>

Burneo Carrera, J. (2024). El jurista exégeta: argumentación e interpretación jurídica en el contexto ecuatoriano. *Ratio Iuris. Revista de Derecho*, 12(1), 19-30.
<https://dspace.uces.edu.ar/handle/123456789/6893>

Cámara de Diputadas y Diputados de Chile. (2025). *Regula la creación y difusión de imitaciones digitales realistas de la imagen, cuerpo o voz de las personas, generadas mediante inteligencia artificial*.
<https://www.camara.cl/verDOC.aspx?prmFICHATIPO=DIP&prmID=84844&prmLOCAL=0&prmTipo=FICHAPARLAMENTARIA>

Celis Vela, D. (2024). La investigación dogmática en el derecho: un análisis reconstructivo sobre el quehacer académico de los juristas. *Revista de la Facultad de Derecho y Ciencias Políticas*, 54(141).
<https://revistas.upb.edu.co/index.php/derecho/article/view/8331>

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. https://scholarship.law.bu.edu/faculty_scholarship/640/

Congreso de Colombia. (2024). *Ponencia para segundo debate al Proyecto de Ley 225 de 2024 Senado, por medio del cual se modifica el artículo 296 de la Ley 599 de 2000*. <https://svrpubindc.imprenta.gov.co/senado/>

Congreso de Colombia. (2025). *Texto aprobado en segundo debate del Proyecto de Ley 360 de 2024 Cámara – 225 de 2024 Senado*.
<https://svrpubindc.imprenta.gov.co/senado/>

Corte Constitucional del Ecuador. (2021). *Sentencia No. 2064-14-EP/21*.
<https://www.corteconstitucional.gob.ec/sentencia-2064-14-ep-21/>

Corte Constitucional del Ecuador. (2026). *Sentencia No. 105-23-IN/25*.
https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXR

hIjoicm8iLCJ1dWlkIjoiZTI0MmU5NmUtYTMxYS00ZjgwLThjNmMtZTU4YTg4OTVmNzA5LnBkZiJ9

Corte Nacional de Justicia del Ecuador. (2019). *Consulta sobre calumnia y ejercicio privado de la acción penal*.
https://www.cortenacional.gob.ec/cnj/images/pdf/consultas_absueltas/Penales/infraccion-penal/019.pdf

De la Torre, R., & Montaña Pinto, J. (2011). *El habeas data en Ecuador*.
https://repositorio.consejodecomunicacion.gob.ec/bitstream/CONSEJO_REP/3783/1/Apuntes%20de%20derecho%20procesal%20CCE.pdf

Ferrajoli, L. (2006). *Derecho y razón. Teoría del garantismo penal*. Trotta.

Ferrajoli, L. (2006). *Garantismo penal*. Instituto de Investigaciones Jurídicas, UNAM. <https://archivos.juridicas.unam.mx/www/bjv/libros/9/4122/9.pdf>

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la investigación*. McGraw-Hill.
<https://books.google.com.pe/books?id=SJR2zgEACAAJ>

Kayesa, N., & Shung-King, M. (2020). The role of document analysis in health policy analysis studies in low and middle-income countries: Lessons for HPA researchers from a qualitative systematic review. *Health Policy Open*, 2, 100024.
<https://doi.org/10.1016/j.hpopen.2020.100024>

Kietzmann, J., Lee, L., McCarthy, I., & Kietzmann, T. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135-146.
<https://www.sciencedirect.com/science/article/pii/S0007681319301590>

Mir Puig, S. (2006). *Derecho penal: Parte general*. Repertor.
<https://proyectozero24.com/wp-content/uploads/2021/09/Mir-Puig-2006-Derecho-Penal.-Parte-General.pdf>

- República de Colombia. (2009). *Ley 1273 de 2009*.
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36912>
- Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosophers' Imprint*, 20(7), 1-16. <https://quod.lib.umich.edu/p/phimp/3521354.0020.007>
- Rodríguez Moreno, F. (2017). El delito de calumnia en la legislación ecuatoriana. Corte Nacional de Justicia.
https://www.cortenacional.gob.ec/cnj/images/pdf/publicaciones_cnj/Temas%20Penales%202.pdf
- Senado de Chile. (2025). *Comisión de la Mujer aprobó norma que reconoce el delito de violencia política digital*.
<https://www.senado.cl/comunicaciones/noticias/comision-de-la-mujer-aprobo-norma-que-reconoce-el-delito-de-violencia>
- Senado de la República de Colombia. (2024). *Comisión Primera aprueba proyecto que busca frenar delitos de suplantación por IA*.
<https://www.senado.gov.co/index.php/el-senado/noticias/5605-comision-primer-a-prueba-proyecto-que-busca-frenar-delitos-de-suplantacion-por-ia>
- Taco-Sánchez, L. (2025). Delitos digitales de contenido íntimo generado mediante inteligencia artificial: necesidad de tipificación en el COIP. *Societec*.
<https://institutojubones.edu.ec/ojs/index.php/societec/article/view/68>
- Torres, H. (2015). *La operatividad del principio de lesividad*.
<https://www.pensamientopenal.com.ar/system/files/2015/08/doctrina41645.pdf>

ANEXOS

Anexo I: Guía de entrevista semiestructurada para operadores del sistema penal

Propósito general

Levantar criterios técnicos de aplicación práctica para sustentar el diagnóstico normativo sobre la insuficiencia de tipificación penal frente a deepfakes sexuales no consentidos en personas adulta.

Instrucciones de aplicación

La duración aconsejada es de 25 a 35 minutos.

Modalidad: Presencial

Registro: audio

Explicar finalidad académica

respuestas.

Guion de apertura común

1. Agradecimiento por su tiempo.
2. Explicar que la entrevista es académica, orientada a comprender criterios prácticos sobre persecución y juzgamiento de conductas vinculadas con deepfakes sexuales no consentidos en personas adultas.
3. Indicar que no se recopilarán datos sensibles de casos concretos ni información reservada.
4. Solicitar autorización para registrar audio o tomar notas.
5. Confirmar que la participación es voluntaria y puede omitirse cualquier respuesta.

Informantes

- Juez de garantías penales – Dra. Mayra Chango

- Fiscal – Dr. Diego Paz
- Defensor público – Dr. Luis Eduardo Castillo

Preguntas

1. ¿Conoce en que consiste el deepfake?
2. Desde la perspectiva del principio de legalidad y de la exigencia de taxatividad penal, ¿considera que el COIP contiene actualmente tipos penales con un grado suficiente de determinación normativa para sancionar conductas ilícitas cometidas mediante deepfakes?
3. En términos de tipicidad, tanto objetiva como subjetiva, ¿cuáles son los principales obstáculos para poder subsumir conductas asociadas a deepfakes en los tipos penales actualmente vigentes?
4. ¿Qué bienes jurídicos consideran que serían susceptibles de afectación mediante el uso ilícito del deepfake y cuáles, a su juicio, darían lugar a una intervención del derecho penal con mayor solidez o certeza?
5. ¿Qué importancia tiene en el apartado probatorio la pericia forense digital, la autenticidad e integridad del archivo y la trazabilidad de la difusión de los archivos para poder vehicular una imputación penal?
6. ¿Qué restricciones consideran que existen para poder identificar la autoría, coautoría o formas de participación en la creación, modificación o difusión de deepfakes que sean pertinentes a efectos penales?
7. ¿Creen que la ausencia de una tipificación expresa de deepfakes puede dar lugar a inseguridad jurídica para la solución de los casos concretos?
8. Desde la política criminal, ¿creen necesaria una tipificación específica sobre conductas delictivas en relación con deepfakes? Justifiquen su respuesta
9. En caso de que llegara a haber una reforma, ¿qué elementos objetivos o subjetivos del tipo penal se consideran imprescindibles para articular una figura penal orientada a conductas que se desenvolvesen mediante deepfakes? ¿Qué criterios permitirían

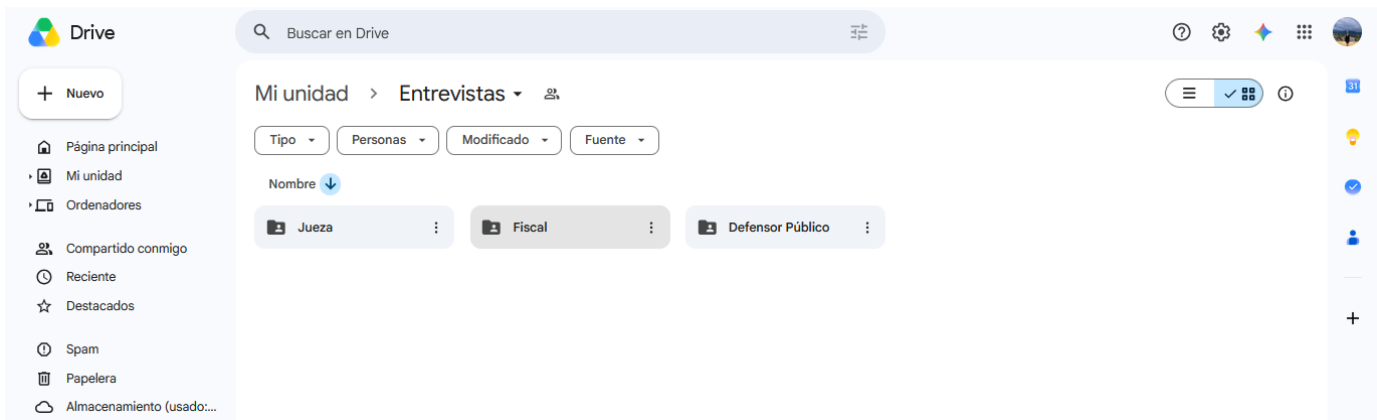
diferenciar, desde el derecho penal y el principio de mínima intervención, los usos ilícitos de deepfakes de aquellos supuestos que no ameriten respuesta punitiva?

10. Desde su conocimiento, ¿qué observaciones considera indispensables para que una eventual propuesta legislativa sobre deepfakes sea compatible con un modelo penal respetuoso de derechos, garantías y límites al ius puniendi?

Anexo II: Entrevista – Fiscal



Anexo III: Grabaciones en audio – Entrevistas - Juez – Fiscal – Defensor



Público

Anexo IV: Certificación de haber realizado una entrevista académica, por parte de la Jueza del Tribunal de Garantías Penales de Bolívar