



UNIVERSIDAD
CATÓLICA
DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

**RESPONSABILIDAD PENAL POR LA DIFUSIÓN DE
IMÁGENES ÍNTIMAS NO CONSENTIDAS GENERADAS CON
INTELIGENCIA ARTIFICIAL EN ECUADOR**

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

AUTORES: VINICIO ALEJANDRO CALLES CADENA

EDUARDO ALEJANDRO GRANJA ROSERO

DIRECTOR: DR. JOSE FELIPE HIDALGO, MGS.

CUENCA - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

**RESPONSABILIDAD PENAL POR LA DIFUSIÓN DE
IMÁGENES ÍNTIMAS NO CONSENTIDAS GENERADAS CON
INTELIGENCIA ARTIFICIAL EN ECUADOR**

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

AUTORES: VINICIO ALEJANDRO CALLES CADENA

EDUARDO ALEJANDRO GRANJA ROSERO

DIRECTOR: DR. JOSE FELIPE HIDALGO PALACIOS, MSG.

CUENCA – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



Universidad
Católica
de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Vinicio Alejandro Calles Cadena portador(a) de la cédula de ciudadanía N° 1400714422. Declaro ser el autor de la obra: **“Responsabilidad penal por la difusión de imágenes íntimas no consentidas generadas con inteligencia artificial en Ecuador.”**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 18 de noviembre de 2025

F: 

Vinicio Alejandro Calles Cadena

C.I. 1400714422



Universidad
Católica
de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Eduardo Alejandro Granja Rosero portador(a) de la cédula de ciudadanía N° **0932017635**. Declaro ser el autor de la obra: **"Responsabilidad penal por la difusión de imágenes íntimas no consentidas generadas con inteligencia artificial en Ecuador"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **19 de noviembre de 2025**

F. 

Eduardo Alejandro Granja Rosero

C.I. **0932017635**



Universidad
Católica
de Cuenca

CERTIFICADO DEL TUTOR

Yo, José Felipe Hidalgo Palacios, certifico que el presente proyecto de titulación / artículo científico, con el título “Responsabilidad penal por la difusión de imágenes íntimas no consentidas generadas con inteligencia artificial en Ecuador” fue desarrollado por Vinicio Alejandro Calles Cadena y Eduardo Alejandro Granja Rosero, con números de cédula 1400714422 y 0932017635, bajo mi supervisión.

F:

Jose Felipe Hidalgo Palacios

C.I. 0105243513

Dedicatoria

Dedico este trabajo, ante todo, a mi familia, por ser el pilar que ha sostenido cada paso de mi formación. A mis padres y hermanos, por su amor inagotable y por enseñarme que la disciplina y la constancia son el camino hacia cualquier meta.

Extiendo esta dedicatoria con especial cariño a mis tíos y primos, por su apoyo constante, sus consejos y por acompañarme siempre con afecto sincero.

Dedico también este logro a mi novia, Nicole, por su compañía, su paciencia y por creer en mí incluso en los momentos más complicados. Su apoyo ha sido fundamental en este proceso.

Esta tesis también está dedicada a todas las personas que han sido víctimas de violencia digital, con la esperanza de que este trabajo aporte a la construcción de espacios más seguros y dignos.

Vinicio Alejandro Calles Cadena

Dedico este proyecto de tesis a mi amada esposa Gabriela, y a mi hija Danna Emilia, quienes han sido mi mayor inspiración y motivo para continuar adelante incluso en los momentos más difíciles.

A mi esposa, por su paciencia, su apoyo incondicional y por creer en mí cuando las fuerzas flaqueaban, siempre motivándome a seguir adelante sin importar las adversidades. A mi compañera incansable, a quien debo cada momento de calma y cada impulso para seguir. Gracias por sostenerme con tu paciencia, por compartir desvelos y alegrías, y por creer en este sueño cuando yo dudaba. A mi hija, por recordarme cada día el valor de luchar por un futuro mejor y por iluminar mi camino con su alegría y pureza, pequeña luz de mis días, por enseñarme que todo esfuerzo tiene sentido y por regalarme la sonrisa que renovó mi fuerza.

A mi familia, que ha sido mi guía y mi sostén en cada etapa de este proceso. Gracias por brindarme un hogar lleno de comprensión, por acompañarme con palabras de aliento cuando más las necesitaba y por enseñarme el valor del esfuerzo y la perseverancia. En especial a mis abuelos Miguel y Elvia por cada consejo que me guio durante todo el camino, y por su infinito apoyo. Este logro es tan suyo como mío, porque sin su amor, comprensión y sacrificio, nada de esto habría sido posible.

Eduardo Alejandro Granja Rosero

Agradecimientos

Mi agradecimiento especial y en primer lugar al **Dr. José Felipe Hidalgo Palacios**, director de este trabajo, por su guía académica, su compromiso, sus observaciones oportunas y por acompañar con profesionalismo cada etapa de este proceso investigativo. Su apoyo fue fundamental para el desarrollo y culminación de esta tesis.

Agradezco también a Dios por darme la fortaleza, serenidad y claridad necesarias para avanzar incluso en los momentos de mayor dificultad.

A mis padres, por su apoyo incondicional, por su esfuerzo y por ser la base que sostiene cada logro en mi vida.

A mis hermanos ya mis primos, por ayudarme en cada momento que lo necesite para este proceso.

A mis tíos, por su respaldo constante, sus palabras de ánimo y por ser una parte importante de mi crecimiento personal y profesional.

A mi novia, Nicole, gracias por tu paciencia, tu comprensión y por acompañarme durante todo este camino universitario con cariño y apoyo sincero. A su madre, por su recibimiento, cordialidad y respeto hacia mí.

A mi compañero Alejandro Granja, que fue parte fundamental para el desarrollo de todo este proyecto

A mis docentes de la Carrera de Derecho de la Universidad Católica de Cuenca, quienes contribuyeron a mi formación integral, ética y profesional.

Finalmente, agradezco a todas las personas que luchan contra la violencia digital y defienden la dignidad humana en los entornos tecnológicos. Este trabajo busca aportar a esa causa.

Vinicio Alejandro Calles Cadena

Agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad, por brindarme una vida llena de oportunidades hermosas que me han ayudado a crecer y a ser mejor cada día.

A mi madre y a mi padre por ser el pilar fundamental en, por su incondicional a través del tiempo, y por ser los guías en mi camino.

A mi compañero Alejandro Calles por ser parte fundamental durante todo el proceso de desarrollo de mi proyecto.

A mis maestros por su arduo trabajo de enseñanza día a día, por permitirme plasmarme de sus valiosos conocimientos, por brindarme su mano y por ayudarme a lograr el objetivo tan soñado.

Eduardo Alejandro Granja Rosero

Resumen

Las tecnologías basadas en IA han transformado por completo la forma en que se crean y comparten imágenes, lo que ha generado un problema significativo dentro del derecho penal. Hoy cualquier persona puede producir un *deepfake* o un *deepnude* que luce totalmente real, incluso sin que exista una fotografía original. Esto afecta bienes jurídicos esenciales como la intimidad, la imagen y la dignidad, pues estas imágenes íntimas falsas se difunden con rapidez, dañan la reputación de las personas y las exponen a una violencia digital que muchas veces es invisible, pero igual de grave que una agresión física.

El inconveniente es que la normativa penal ecuatoriana no está preparada para enfrentar este fenómeno. El COIP exige la existencia de una imagen real para sancionar la difusión de contenido íntimo, lo que deja sin protección a las víctimas de imágenes sintéticas creadas con IA.

Aplicar estas conductas por analogía tampoco resulta viable, porque vulneraría el principio de legalidad. Por ello se produce un vacío normativo que favorece la impunidad y dificulta la labor de fiscales y jueces.

Mientras países como España, Reino Unido y varios estados de EE. UU. ya cuentan con regulaciones específicas, Ecuador continúa sin una respuesta clara. Esto vuelve urgente reformar el derecho penal para incorporar estas nuevas formas de violencia digital y garantizar que la dignidad y la intimidad permanezcan protegidas en la era tecnológica.

Palabras clave: *Derecho Penal, deepfake, deepnudes, imágenes íntimas, Inteligencia Artificial.*

Abstract

Artificial Intelligence (AI) technologies have completely transformed the way images are created and shared, posing a significant challenge for criminal law. Today, anyone can produce a deepfake or deepnude that looks completely real, even without an original photograph. This affects essential legal rights such as privacy, image, and dignity, as these fake intimate images spread quickly, damage reputations, and expose individuals to digital violence that is often invisible yet just as serious as physical aggression.

The problem is that Ecuadorian criminal law is not prepared to address this phenomenon. The Comprehensive Organic Criminal Code (COIP, by its Spanish acronym) requires the existence of a real image to punish the dissemination of intimate content, leaving victims of AI-generated synthetic images unprotected.

Applying these behaviors by analogy is also not feasible, because it would violate the principle of legality. This creates a regulatory gap that encourages impunity and complicates the work of prosecutors and judges.

While countries such as Spain, the United Kingdom, and several U.S. states already have specific regulations in place, Ecuador still lacks a clear legal response. This makes it urgent to reform criminal law to incorporate these new forms of digital violence and ensure that dignity and privacy remain protected in the technological era.

Keywords: Criminal Law, deepfake, deepnudes, intimate images, Artificial Intelligence.

Índice

TABLA DE CONTENIDO

| | |
|---|--------------------|
| <i>Declaratoria de autoria</i> | <i>II</i> |
| <i>Certificado del tutorDedicatoria</i> | <i>IV</i> |
| <i>Agradecimientos</i> | <i>VI</i> |
| <i>Resumen</i> | <i>VIII</i> |
| <i>Abstract</i> | <i>IX</i> |
| <i>Índice</i> | <i>X</i> |
| <i>1. Introducción</i> | <i>1</i> |
| <i>2. Capítulo I : Fundamentos del derecho penal y bienes jurídicos afectados por la creación y difusión de imágenes íntimas sintéticas generadas mediante inteligencia artificial</i> | <i>4</i> |
| <i>2.1. Conceptos penales básicos y bienes jurídicos protegidos</i> | <i>4</i> |
| <i>2.2. Definición de deepfakes y deepnudes</i> | <i>7</i> |
| <i>2.3. Principios penales relevantes</i> | <i>9</i> |
| <i>2.4. Normativa penal vigente en ecuador</i> | <i>11</i> |
| <i>2.5. APLICABILIDAD A IMÁGENES ÍNTIMAS SINTÉTICAS</i> | <i>15</i> |
| <i>2.6. CASOS Y EJEMPLOS NACIONALES RELEVANTES</i> | <i>19</i> |
| <i>2.7. REFERENCIAS COMPARADAS MÍNIMAS</i> | <i>22</i> |
| <i>2.8. CONCLUSIONES PARCIALES</i> | <i>27</i> |

| | | |
|----------------|---|-----------|
| 3. | <i>CAPÍTULO II: Limitaciones normativas y vacíos en la imputación penal de imágenes íntimas falsas en el marco jurídico ecuatoriano</i> | 28 |
| 3.1. | Clasificación de limitaciones normativas | 31 |
| 3.1.1 | Deficiencias en la tipificación | 33 |
| 3.1.2 | Tensiones con los principios del derecho penal | 34 |
| 3.1.3 | Dificultades de adaptación frente a las transformaciones tecnológicas | 35 |
| 3.1.4 | La necesidad de un replanteamiento estructural | 36 |
| 3.2. | Vacíos legales específicos | 37 |
| 3.3. | Retos prácticos en la imputación penal | 40 |
| 3.3.1 | Identificación de autores y partícipes | 41 |
| 3.3.2 | Complejidad en la participación delictiva | 42 |
| 3.3.3 | Obtención y preservación de la prueba electrónica | 43 |
| 3.3.4 | Dimensión transnacional y cooperación judicial | 44 |
| 3.3.5 | Necesidad de estrategias integrales | 45 |
| 3.4. | Impacto en política criminal | 46 |
| 3.5. | Articulación de medidas preventivas, reactivas y restaurativas | 48 |
| 3.6. | Cooperación internacional y gobernanza digital | 49 |
| 3.7. | Hacia un modelo integral de política criminal | 50 |
| 3.8. | Conclusiones parciales | 51 |
| 3.8.2 | Conclusión general de este capítulo | 56 |
| 4. | <i>CAPÍTULO III: Jurisprudencia y doctrina penal internacional aplicables a los deepfakes y la violencia digital: bases para una reforma penal ecuatoriana</i> | 57 |

| | |
|--|-----------|
| 4.1. Marco penal comparado | 58 |
| 4.1.1 Conclusión comparativa: | 60 |
| 4.2. Instrumentos penales internacionales relevantes..... | 60 |
| 4.3. Jurisprudencia penal internacional | 64 |
| 4.4. Doctrina penal internacional | 68 |
| 4.4.2 Conclusión parcial..... | 72 |
| 4.5. Propuestas de reforma para Ecuador | 73 |
| 4.5.1 Reforma penal necesaria | 74 |
| 4.5.2 Tipificación expresa de los deepnudes | 75 |
| 4.5.3 Agravantes por uso de inteligencia artificial..... | 76 |
| 4.5.4 Responsabilidad de plataformas digitales | 77 |
| 4.5.5 Conclusión parcial..... | 78 |
| 4.6. Conclusiones parciales | 78 |
| 5. Conclusiones | 82 |
| 5.1. Insuficiencia del marco penal ecuatoriano..... | 82 |
| 5.2. Vulneración de derechos fundamentales..... | 83 |
| 5.3. Dificultades probatorias y tecnológicas | 84 |
| 5.4. Tendencias comparadas y estándares internacionales..... | 85 |
| 5.5. Doctrina penal y necesidad de adaptación digital | 85 |
| 5.6. Perspectiva de género y reparación integral..... | 86 |
| 5.7. Propuesta general de política criminal..... | 87 |
| 5.8. Conclusión final..... | 88 |

***Referencias bibliográficas*..... 89**

***Anexos*..... 93**

1. Introducción

El avance acelerado de la inteligencia artificial (IA) ha transformado profundamente los entornos digitales, generando nuevas oportunidades, pero también desafíos éticos y jurídicos. Entre estos desafíos, uno de los más inquietantes es la creación y difusión de imágenes íntimas sintéticas, es decir, imágenes falsificadas mediante IA que representan a personas reales en situaciones sexualizadas sin su consentimiento. Esta práctica, conocida como deepnudes, constituye una forma emergente de violencia digital que vulnera derechos fundamentales como la intimidad, la dignidad y la imagen personal (Simó Soler, 2023). El presente trabajo se propone analizar la insuficiencia del marco penal ecuatoriano para sancionar eficazmente estos actos y evaluar la necesidad de una reforma legislativa que responda a la complejidad de esta nueva forma de agresión.

En el contexto ecuatoriano, la difusión de imágenes íntimas reales sin consentimiento ha sido reconocida como una infracción penal en el artículo 178 del Código Orgánico Integral Penal (COIP), el cual protege la intimidad personal y familiar. Sin embargo, este artículo no contempla de manera expresa los casos en los que las imágenes son generadas artificialmente y no tienen un referente fotográfico real. Esta omisión normativa deja a las víctimas en un vacío legal, generando una "impunidad estructural" (Trujillo Cabrera, 2023), pues los agresores no enfrentan una tipificación penal clara, y las instituciones de justicia carecen de herramientas jurídicas adecuadas para la persecución del delito.

La preocupación sobre el impacto de estas tecnologías en los derechos fundamentales ha sido compartida por organismos internacionales. La Agencia de los Derechos Fundamentales de la Unión Europea (2020) advirtió que los deepfakes, cuando son utilizados para generar

contenido sexual no consentido, pueden constituir una forma de violencia de género digital que revictimiza a mujeres y niñas, perpetuando estereotipos y afectando gravemente su integridad emocional. La problemática no solo es jurídica, sino también social, pues evidencia cómo las nuevas tecnologías pueden ser instrumentalizadas para reproducir formas de dominación y violencia ya existentes.

Diversos autores han sostenido que el Derecho Penal debe adaptarse a los desafíos que presentan las tecnologías emergentes, sin sacrificar los principios fundamentales como la legalidad, la tipicidad y la proporcionalidad. Zaffaroni, por ejemplo, plantea que el Derecho Penal no puede mantenerse estático ante nuevas realidades sociales y tecnológicas, pues su función de tutela requiere respuestas efectivas y contextualizadas (Zaffaroni, 2009). Por su parte, Jakobs (2005) señala que el Derecho Penal del ciudadano debe incorporar mecanismos que protejan la seguridad personal y la confianza en el entorno digital, ya que estas nuevas formas de vulneración tienen efectos concretos en la autonomía y en la identidad de las personas.

El fenómeno de los deepnudes plantea también complejidades desde el punto de vista de la imputación penal. A diferencia de los delitos tradicionales, en los que la acción delictiva tiene un agente claro, en los delitos digitales intervienen múltiples actores: quien genera el contenido, quien lo encarga, quien lo difunde y, en ciertos casos, incluso las plataformas digitales que permiten su circulación. Roxin (2010), mediante la teoría del dominio del hecho, sostiene que debe considerarse autor a quien tiene el control funcional del acto típico, lo cual podría extender la autoría penal a quienes manejan los algoritmos generadores o a quienes ordenan la creación de estas imágenes con conocimiento de su ilicitud.

Desde una perspectiva de género, la difusión de imágenes íntimas falsas afecta desproporcionadamente a las mujeres, lo cual ha sido ampliamente documentado por Simó Soler (2023). La autora sostiene que la generación y divulgación de contenido íntimo falso perpetúa el control sobre los cuerpos femeninos, reproduce patrones de dominación y constituye una forma de violencia simbólica que exige respuestas penales claras. En consecuencia, propone la tipificación autónoma de esta conducta como una modalidad agravada de violencia digital y de género.

La doctrina penal ecuatoriana aún no ha abordado de forma exhaustiva este fenómeno. Sin embargo, existen esfuerzos académicos que apuntan hacia una reinterpretación del tipo penal del artículo 178 del COIP. Guzmán y Ramírez (2021) sostienen que la interpretación de esta norma debe ser evolutiva y considerar no solo las imágenes reales, sino también las sintéticas, en tanto que generan el mismo daño a la integridad psicoemocional de las víctimas. Este enfoque interpretativo permitiría una protección más eficaz de los bienes jurídicos sin necesidad de esperar reformas legislativas, aunque con el riesgo de tensionar el principio de legalidad.

En el plano comparado, se observan avances significativos. En España, por ejemplo, la Ley Orgánica 10/2022, conocida como Ley de Garantía Integral de la Libertad Sexual, incluye sanciones para la difusión de contenido sexual no consentido, incluyendo el generado por medios tecnológicos. En Estados Unidos, varios estados como California y Texas han tipificado los deepfakes sexuales como delito, reconociendo el daño que estos pueden causar a la reputación y la privacidad de las personas. Estas experiencias comparadas evidencian la urgencia de que Ecuador adopte medidas similares que reflejen la evolución de los delitos digitales.

Así, el presente trabajo de investigación se centra en analizar si el marco jurídico penal vigente en Ecuador es adecuado para sancionar la difusión de imágenes íntimas generadas con inteligencia artificial sin consentimiento. Para ello, se abordará la doctrina penal relevante, los principios del Derecho Penal, la jurisprudencia nacional y comparada, así como las propuestas de reforma legislativa que permitan cerrar los vacíos existentes. A través de un enfoque cualitativo y analítico, se espera aportar elementos que fundamenten la necesidad de una regulación específica en esta materia, con el fin de garantizar una protección real y efectiva de los derechos fundamentales en el entorno digital.

Finalmente, la investigación parte de la hipótesis de que la falta de una regulación penal expresa sobre imágenes íntimas sintéticas debilita gravemente la protección de la intimidad y la dignidad personal en el Ecuador. Este vacío normativo no solo obstaculiza la imputación penal efectiva de los agresores, sino que también contribuye a la impunidad, desincentivando la denuncia y aumentando el riesgo de revictimización. Como sostiene Citron (2019), “la tecnología debe ser regulada cuando amplifica el daño, desiguala las relaciones de poder y mina la capacidad de las personas para ejercer sus derechos fundamentales”.

En este contexto, el Derecho Penal está llamado a responder con herramientas eficaces, proporcionadas y acordes a los principios del Estado constitucional de derechos y justicia, en el que se reconozca que la protección de la dignidad humana debe prevalecer incluso ante los desafíos que imponen las nuevas tecnologías.

2. Capítulo I : Fundamentos del derecho penal y bienes jurídicos afectados por la creación y difusión de imágenes íntimas sintéticas generadas mediante inteligencia artificial

En los últimos tiempos con la aparición de las tecnologías que están basadas en la inteligencia artificial (IA) y su acceso al público general, ha demostrado una nueva forma de crear contenido visual permitiendo que los usuarios puedan crear imágenes desde cero de forma que sean percibidas de forma totalmente realista para el ojo humano. Dado este desarrollo, se han creado imágenes íntimas o de carácter sexual de personas reales combinadas con la tecnología de la IA, todo esto sin consentimiento de las personas que aparecen en las imágenes o fotos generando así una preocupación en aumento. Estos comportamientos presentan desafíos reveladores para nuestro derecho penal ecuatoriano, el cual al estar basado en marcos normativos conservadores no logran contemplar de manera específica y directa la rápida y compleja difusión de dichas imágenes. Por esto, es crucial examinar la ley penal actual para que enfrente estos distintos escenarios.

Este tema representa un problema latente que exige una respuesta urgente desde el Derecho Penal. De acuerdo con Simó Soler (2023), el surgimiento constante de nuevas herramientas basadas en inteligencia artificial obliga a examinar sus efectos sociales y jurídicos, especialmente cuando generan conductas que pueden vulnerar derechos fundamentales. La autora advierte que el Derecho no puede mantenerse ajeno a estos cambios tecnológicos, pues la falta de regulación y análisis puede derivar en nuevas formas de violencia o afectación a la dignidad humana. En este sentido, la reflexión penal debe adelantarse a los riesgos que trae la inteligencia artificial y adaptarse a los desafíos que plantea su uso indebido.

Es evidente que la legislación tiene muchas limitaciones a la hora de poder penalizar las distintas responsabilidades en torno a estas imágenes sintéticas. Las leyes que rigen en la actualidad fueron estructuradas con el fin de regular comportamientos y conductas de violación de intimidad donde no se contempla la revolución tecnológica en cuanto a la inteligencia artificial. A esto, se suma que la evolución tecnológica avanza a pasos agigantados dejando de lado un marco jurídico tradicional que necesita adecuarse a los nuevos cambios y conductas.

La creación y la difusión de imágenes íntimas generadas por IA crea un impacto que va más allá de la afectación personal, sino que afecta a una escala de nivel social importante. Los daños que presentan las víctimas frente a estas conductas se ven involucradas en su reputación, su bienestar, auto estima e incluso con sus relaciones interpersonales, sumando que su rol en la sociedad se puede ver realmente afectado. De igual modo, las imágenes sintéticas son distribuidas con velocidad apabullante y de forma masiva creando así todo un ambiente digital de vulnerabilidad para muchos usuarios los cuales no solo afecta a las víctimas si no a quienes consumen el contenido debido a su máxima difusión como amigos, familiares, compañeros de trabajo. Desde la óptica penal, este contexto evidencia la dificultad en la que se encuentra el marco jurídico respecto a la protección de la intimidad y la dignidad en la situación de comportamientos ilegales relacionados con el avance tecnológico.

Según Jescheck y Weigend (2002), el Derecho Penal tiene la función de proteger los valores esenciales que permiten la convivencia dentro de una sociedad, es decir, aquellos bienes cuya vulneración pone en riesgo el orden social y la seguridad colectiva. Los autores sostienen que, precisamente por su importancia, el Estado debe garantizar su defensa mediante el uso

legítimo de la coacción penal. En otras palabras, el Derecho Penal actúa como el último recurso para preservar la armonía social cuando otros mecanismos no son suficientes.

2.1. Conceptos penales básicos y bienes jurídicos protegidos

El derecho penal resguarda valores fundamentales específicos para la convivencia, dichos valores tienen el nombre de bienes jurídicos. Los bienes jurídicos sirven como limitantes del poder que tiene el estado para sancionar, basando la intervención penal en casos donde hay lesiones graves a los intereses esenciales de los mismos. En el contexto de esta investigación, los bienes jurídicos más notables son la intimidad, la imagen y la dignidad, dichos bienes han sido afectados de forma directa por las tecnologías actuales y entre ellas la IA que produce imágenes sintéticas con carácter sexual.

De acuerdo con Roxin (2010), el bien jurídico funciona como una especie de límite natural al poder punitivo del Estado, ya que solo se justifica la intervención penal cuando lo que está en juego son intereses realmente esenciales para la vida social o la integridad del individuo. En este sentido, el Derecho Penal no debe actuar de forma desmedida, sino únicamente cuando se busca proteger valores fundamentales cuya afectación compromete la convivencia y la seguridad jurídica.

La intimidad es el espacio personal privado que cada persona tiene y por derecho a estar protegido de intromisiones ajenas. El estado ecuatoriano a través de la Constitución reconoce de

forma expresa a la intimidad como derecho fundamental, por lo tanto representa que también debe considerarse un bien jurídico tutelado de forma penal de cara a conductas como manipulación de imágenes íntimas y la difusión de estas mismas.

La Constitución de la República del Ecuador (2008) incorpora dentro de su catálogo de derechos el principio de intimidad personal y familiar, estableciendo que toda persona tiene derecho a mantener un espacio privado libre de intromisiones o presiones externas. En términos simples, el Estado reconoce que cada individuo necesita una esfera donde pueda desarrollarse con libertad, tanto en su vida cotidiana como en el ámbito familiar, sin que terceros interfieran o difundan aspectos que pertenecen a su privacidad. Este derecho, aunque tradicionalmente se entendía en el plano físico o doméstico, hoy adquiere un sentido mucho más amplio por el entorno digital, donde una imagen, una conversación o incluso un dato pueden hacerse públicos en cuestión de segundos.

Por eso, la intimidad debe asumirse como un límite frente al acceso o manipulación no consentida, sobre todo cuando la tecnología y la inteligencia artificial facilitan la creación o difusión de información personal sin autorización. En ese sentido, el respeto a la intimidad no solo garantiza la tranquilidad individual, sino que también protege la dignidad y la libertad de decidir sobre uno mismo, evitando que la vida privada se convierta en un objeto de exposición o consumo digital. Todo esto demuestra que el derecho a la intimidad no es un concepto estático, sino un principio vivo que debe adaptarse a los cambios tecnológicos y sociales que caracterizan al mundo actual (Constitución de la República del Ecuador, 2008).

Las personas tienen el derecho a la imagen que certifica el uso y el control de su representación corporal. Hoy por hoy, la IA representa un peligro nuevo al haber la posibilidad

de que se puedan crear imágenes ficticias con rostros de personas existentes sin su consentimiento, afectando así la autonomía de la víctima y también comprometiendo la identidad frente a otros terceros.

De acuerdo con Varela (2021), la protección del derecho a la imagen se enfrenta a nuevos desafíos derivados del uso creciente de la inteligencia artificial. El autor plantea que la manipulación digital, al alterar o reconstruir la apariencia de una persona, puede vulnerar directamente su identidad, su autonomía y su capacidad de decidir cómo quiere ser representada. En ese sentido, la tecnología no solo afecta la esfera estética o visual, sino también la percepción social y moral del individuo, generando daños que trascienden lo material. Por eso, se vuelve urgente que el Derecho Penal y las políticas públicas ajusten sus mecanismos de protección, garantizando que la dignidad y la imagen personal mantengan su valor incluso frente a los nuevos escenarios digitales donde la manipulación de contenido se ha vuelto común (Varela, 2021).

La dignidad es la base sobre la cual reposan el resto de derechos y no solo se forma como un principio rector, sino que también es por sí solo un bien jurídico que actúa de forma autónoma. Por esto la jurisprudencia ecuatoriana indica que la dignidad es un presupuesto totalmente necesario para el ejercicio de los demás derechos lo que llevaría a que se viera afectado por la difusión de los DeepNudes que vulneraría de forma directa este núcleo importantísimo.

La Corte Constitucional del Ecuador, en la Sentencia No. 003-18-SIN-CC, ha sostenido que la dignidad humana es el punto de partida sobre el cual descansan todos los demás derechos reconocidos por la Constitución. En otras palabras, este principio actúa como el núcleo que da sentido a la existencia del ser humano dentro del orden jurídico, ya que sin dignidad no habría posibilidad real de ejercer libertades ni de exigir respeto a la intimidad o la imagen. La Corte interpreta que la dignidad no es un valor abstracto, sino una condición concreta que el Estado debe garantizar en toda actuación pública o privada que afecte a una persona. Por eso, la protección penal de la dignidad se vuelve indispensable frente a las nuevas formas de exposición o manipulación digital, donde las imágenes o los datos personales pueden ser usados sin consentimiento y de manera que degradan la identidad misma de la víctima (Corte Constitucional del Ecuador, Sentencia No. 003-18-SIN-CC).

2.2. Definición de deepfakes y deepnudes

Un deepfake es un contenido audiovisual que es creado con el uso de la inteligencia artificial alterando o creando imágenes o videos similares a contenido audiovisual real. Por otro lado, esta el DeepNude que es una subcategoría de los DeepFakes, donde el DeepNude es especialmente perjudicial ya que estos se comprenden en crear imágenes íntimas o de carácter sexual sin el consentimiento de la persona que aparece en la imagen y todo esto puede suceder con la posibilidad de no existir la existencia de una imagen previa, es decir, no edita una foto si no que la crea directamente desde cero.

Según Simó Soler (2023), los llamados deepfakes representan uno de los riesgos más recientes y complejos para la protección de los derechos fundamentales.

Estas tecnologías permiten crear o modificar imágenes y videos con apariencia real, pero cuyo contenido es completamente falso, afectando de manera directa la intimidad, la reputación y la dignidad de quienes aparecen en ellos. La autora explica que la manipulación digital no solo produce daño moral o psicológico, sino que también erosiona la confianza social en la veracidad de la información, generando un entorno donde lo falso puede sustituir a lo verdadero sin dificultad. En ese sentido, advierte que el Derecho Penal debe empezar a reaccionar frente a estas conductas, pues su impacto va más allá del ámbito privado, llegando a vulnerar principios como la autodeterminación personal y la identidad misma del sujeto. Por eso, la respuesta jurídica no puede quedarse atrás, ya que los deep fakes no solo son un fenómeno tecnológico, sino una nueva forma de violencia simbólica y social (Simó Soler, 2023).

La creación de deepnudes usa algoritmos muy complejos que funcionan con un aprendizaje extenso y profundo a través de redes neuronales informáticas almacenadas en grandes bases de datos. Las personas sufren alto riesgo de victimización y la difusión en internet es difícil de controlar todo esto debido a la tecnología sofisticada que manejan al crear imágenes falsas en alta resolución.

La Agencia de Derechos Fundamentales de la Unión Europea (2020) explica que los deepfakes se basan en el uso de técnicas de aprendizaje profundo o deep learning que hacen posible recrear rostros, voces o movimientos con una precisión casi idéntica a la realidad. En

otras palabras, estos sistemas recopilan y procesan grandes volúmenes de información visual y sonora para generar imágenes o vídeos sintéticos que resultan difíciles de distinguir de los auténticos. Esta capacidad técnica, aunque se presenta como un avance en el campo de la inteligencia artificial, también abre la puerta a graves vulneraciones de derechos, pues permite manipular la identidad de una persona, modificar su imagen o incluso ponerla en situaciones inexistentes sin su consentimiento.

En ese contexto, el desafío jurídico radica en cómo equilibrar la innovación tecnológica con la protección de la privacidad y la dignidad humana, evitando que el uso de estos algoritmos se convierta en una herramienta de difamación o violencia digital (Agencia de Derechos Fundamentales de la Unión Europea, 2020).

2.3. Principios penales relevantes

El derecho penal ecuatoriano en cuanto a su aplicación está delimitado por principios esenciales que buscan que la seguridad jurídica sea garantizada. En el artículo 76 de la Constitución y en el artículo 5 del COIP se encuentra el principio de legalidad el cual expresa que ninguna acción puede considerarse como un delito si no está escrito en la ley con anterioridad. El principio de legalidad se ve fuertemente reforzado por la rigurosa tipicidad y la prohibida analogía de in malam partem. A esto, se tiene que considerar el principio de mínima intervención penal que sostiene que el derecho penal es una herramienta que se tiene que usar en última instancia. Muchos autores de la doctrina ecuatoriana y extranjera como Silva Sanchez,

Jakobs o Avila Santamaría, recalcan que el ius puniendi debe ser racional, proporcional y limitado en cuanto a la protección de los bienes jurídicos esenciales.

La Constitución de la República del Ecuador (2008) establece, dentro de las garantías básicas del debido proceso, que ninguna persona puede ser juzgada ni sancionada por un acto u omisión que no esté previamente definido como infracción penal. Este principio refleja la esencia misma de la legalidad penal, donde el poder punitivo del Estado sólo puede ejercerse dentro de los límites que la ley ha determinado con claridad. Dicho en términos más simples, nadie puede ser castigado por algo que la ley no haya previsto expresamente, lo que asegura que el Derecho Penal actúe con previsibilidad y no con arbitrariedad.

Por su parte, el Código Orgánico Integral Penal (2014) refuerza esta idea al disponer que toda aplicación del derecho penal debe observar los principios de legalidad, mínima intervención, proporcionalidad y necesidad. Estos pilares no sólo orientan la interpretación judicial, sino que también funcionan como barreras frente al abuso del poder punitivo, recordando que la sanción penal debe ser el último recurso, aplicable únicamente cuando otros mecanismos no resultan suficientes.

Autores como Silva Sánchez (2013) coinciden en que la expansión del derecho penal moderno ha sido impulsada por una creciente presión social para criminalizar toda conducta nueva que genere alarma o rechazo colectivo. Sin embargo, advierte que esa tendencia debe ser contenida por los principios de mínima intervención y proporcionalidad, para evitar que el sistema penal se convierta en una herramienta de control excesivo más que de justicia.

En la misma línea, Ávila Santamaría (2015) plantea que el Derecho Penal ecuatoriano debe entenderse desde una visión garantista, donde la función del castigo no sea ampliar la

represión, sino asegurar el respeto a los derechos fundamentales y limitar el poder punitivo del Estado. Este enfoque coloca a la persona en el centro de la política criminal, recordando que la justicia penal debe actuar bajo parámetros de humanidad y equilibrio.

De manera complementaria, Jakobs (1995) sostiene que el Derecho Penal cumple una función de garantía, al establecer que solo se puede sancionar aquello que esté previamente descrito como delito. Con ello se busca proteger la seguridad jurídica y evitar que los ciudadanos sean sometidos a decisiones arbitrarias o impredecibles. En conjunto, estas posturas doctrinales demuestran que el Derecho Penal, más que un instrumento de castigo, debe ser un sistema de protección racional, limitado por los principios de legalidad y respeto a la dignidad humana (Constitución de la República del Ecuador, 2008; Código Orgánico Integral Penal, 2014; Silva Sánchez, 2013; Ávila Santamaría, 2015; Jakobs, 1995).

2.4. Normativa penal vigente en Ecuador

En la actualidad el marco legal de Ecuador contiene disposiciones que buscan proteger la intimidad así como la imagen de las personas pero con algunas limitaciones. En el COIP en su artículo 178 existe la sanción a la violación de la intimidad por difundir datos o imágenes sin permiso. El artículo 179 del COIP se refiere en cuanto a pornografía de menores de edad y en el artículo 180 regula también otro tipo de publicaciones prohibidas. Todas estas disposiciones regulan conductas a tratar en esta investigación, pero el limitante que se encuentra es que es necesaria una imagen real creando un vacío frente a las imágenes creadas con inteligencia artificial.

El Código Orgánico Integral Penal (2014) dispone, dentro de su parte especial, varios artículos orientados a la protección de la intimidad y la imagen personal. En el artículo 178, se establece que toda persona que divulgue información privada, imágenes, mensajes o grabaciones sin autorización o sin el consentimiento de quien resulta afectado comete un delito sancionado con pena privativa de libertad. En esencia, esta norma busca evitar la exposición no consentida de la vida privada, garantizando que los datos personales y la correspondencia digital estén resguardados frente a cualquier intromisión. Aunque originalmente se pensó para proteger comunicaciones reales, hoy su alcance se proyecta también hacia el ámbito digital, donde las filtraciones y publicaciones sin permiso son cada vez más frecuentes.

De manera complementaria, el artículo 179 del COIP (2014) sanciona a quien genere o distribuya material de contenido sexual que involucre la imagen de niños, niñas o adolescentes, reconociendo la gravedad del daño que este tipo de actos causa en la integridad psicológica y moral de las víctimas. Este precepto refleja una especial sensibilidad frente a los grupos vulnerables, estableciendo que el derecho penal debe actuar con firmeza cuando se atente contra la inocencia o la dignidad de menores de edad.

Por su parte, el artículo 180 del mismo cuerpo legal prevé sanciones para quien publique o difunda cualquier tipo de contenido prohibido por la ley, extendiendo la responsabilidad a situaciones donde la imagen, la palabra o la representación digital se convierten en vehículos de daño. Esta disposición amplía el espectro de protección y permite entender que el Estado reconoce la existencia de nuevos medios de vulneración, muchos de ellos facilitados por la tecnología y las redes sociales.

En conjunto, estos artículos evidencian que el ordenamiento penal ecuatoriano ya contiene una estructura básica de tutela a la intimidad y la dignidad, aunque todavía carece de un tipo específico que abarque las imágenes sintéticas creadas por inteligencia artificial, como ocurre en el caso de los deepnudes. Por eso, resulta indispensable reformar y actualizar el COIP, de manera que contemple expresamente estas formas modernas de agresión digital y refuerce la protección de los derechos personales frente al avance tecnológico (Código Orgánico Integral Penal, 2014)

La doctrina ecuatoriana ha identificado el COIP y asevera que no se contempla de forma expresa a la protección en referencia a imágenes íntimas falsas. El análisis de Guzman y Ramirez (2021) destaca que existe una falta de tipificación en el artículo 178 respecto a sancionar conductas relacionadas con la difusión de contenido sintético y por lo tanto advierte que el alcance de este artículo se queda corto. Por otro lado, Paredes Castañeda (2022) analiza cómo otros países reconocen las nuevas formas de violencia digital y entra en debate la opción de incluir estas nuevas formas dentro de la política criminal.

De acuerdo con Guzmán y Ramírez (2021), el ordenamiento penal ecuatoriano todavía mantiene una visión limitada en cuanto a la protección de la intimidad, ya que solo contempla los casos en los que existe una imagen real de la víctima. Esto deja fuera situaciones más complejas, como la difusión de imágenes creadas artificialmente mediante inteligencia artificial, que pueden causar el mismo o incluso un mayor daño moral y psicológico. Los autores sostienen que esta omisión genera un vacío legal evidente, pues las herramientas digitales actuales permiten falsificar rostros o cuerpos con un nivel de realismo que pone en riesgo la identidad, la honra y la dignidad de las personas. En ese sentido, la legislación ecuatoriana todavía no alcanza a dimensionar el alcance de la manipulación digital, dejando desprotegidas a las víctimas de los

denominados deep nudes, cuya afectación no radica en la veracidad del contenido, sino en la exposición pública y la humillación que provoca.

Por su parte, Paredes Castañeda (2022) afirma que la violencia digital debe ser entendida como una nueva forma de agresión que requiere respuestas normativas concretas y actualizadas, capaces de reconocer los riesgos que implican las tecnologías emergentes. Según el autor, las normas penales tradicionales ya no son suficientes para contener la magnitud del daño que puede generar la manipulación digital, especialmente cuando atenta contra la dignidad humana y los derechos fundamentales. En su análisis, destaca la necesidad de crear un marco penal moderno, que no solo sancione estas conductas, sino que también contemple medidas preventivas y de reparación integral para las víctimas. De esta forma, el Derecho Penal se mantendría en sintonía con la realidad social y tecnológica, garantizando una protección efectiva frente a los nuevos escenarios de vulneración digital (Guzmán & Ramírez, 2021; Paredes Castañeda, 2022).

La Corte Constitucional del Ecuador, en la Sentencia No. 916-22-JP/24, analizó un caso donde una persona fue excluida de un proceso de selección militar por portar un tatuaje, concluyendo que dicha actuación vulnera varios derechos constitucionales, entre ellos el de la imagen personal. Según el razonamiento del tribunal, la imagen propia forma parte de la identidad individual, y cualquier limitación basada en la apariencia física supone una forma de discriminación que atenta contra la dignidad del ser humano. La Corte resaltó que el Estado no puede restringir oportunidades ni ejercer poder sancionador sobre la base de características estéticas o de expresión corporal, ya que hacerlo implica desconocer la autonomía y la libertad de cada persona para decidir sobre su cuerpo. Este criterio reafirma que la protección del derecho a la imagen debe ser entendida no solo en su dimensión visual, sino también como una expresión

de la individualidad y autenticidad personal (Corte Constitucional del Ecuador, Sentencia No. 916-22-JP/24).

En una línea complementaria, la Corte Constitucional, mediante la Sentencia No. 003-18-SIN-CC, enfatizó que la dignidad humana constituye la base de todos los derechos constitucionales, funcionando como un presupuesto indispensable para su ejercicio y garantía efectiva. En términos simples, sin dignidad no puede hablarse de libertad, igualdad ni justicia. Este principio orienta toda interpretación constitucional y obliga al Estado a proteger la integridad de las personas frente a actos que puedan degradarse o exponerlas sin consentimiento.

En el contexto actual, donde las tecnologías digitales pueden alterar o difundir imágenes personales sin autorización, este precedente adquiere aún más fuerza, recordando que la dignidad no puede ser relativizada por los avances tecnológicos, sino que debe ser reafirmada como límite frente a los abusos que la inteligencia artificial podría generar (Corte Constitucional del Ecuador, Sentencia No. 003-18-SIN-CC).

2.5. APLICABILIDAD A IMÁGENES ÍNTIMAS SINTÉTICAS

El centro de debate en el análisis radica en determinar si es que la creación y difusión de deep nudes puede ser sancionada con el artículo 178 del COIP. Es obvio que la intimidad al ser un bien jurídico protegido se ve afectada, debido a que la norma exige que exista una imagen real para adecuarse al tipo penal. Esta exigencia no permite que las representaciones artificiales se adecuen a la tipicidad directa, por lo tanto, se reconoce una laguna legal. Tratar de ajustar estas

conductas a través de analogía terminaría siendo contradictorio al principio de legalidad, el cual es pilar importante del derecho penal.

De acuerdo con Simó Soler (2023), aplicar el artículo 178 del COIP a los casos de imágenes sintéticas creadas mediante inteligencia artificial supondría forzar el alcance del tipo penal más allá de su tenor literal, lo que equivaldría a incurrir en una analogía prohibida en derecho penal. La autora explica que extender la interpretación de una norma concebida para imágenes reales hasta abarcar las creadas artificialmente rompe con el principio de legalidad, vulnerando los límites del poder punitivo del Estado. Esto deja en evidencia que el sistema penal ecuatoriano aún no cuenta con herramientas normativas capaces de responder frente a estas nuevas conductas tecnológicas, que afectan bienes jurídicos esenciales como la intimidad y la dignidad personal (Simó Soler, 2023).

Como consecuencia, el bien jurídico se ve afectado con los deepnudes, pues no hay tipicidad en el marco legal actual. Este vacío legal demuestra que hay una necesidad real por crear disposiciones específicas que sancionen estas conductas.

Según Llanea (2021), la irrupción de la inteligencia artificial plantea retos inéditos para la política criminal, ya que surgen nuevas formas de lesionar bienes jurídicos fundamentales sin que exista una previsión legal que las contemple expresamente. El autor advierte que estas tecnologías generan espacios de impunidad al permitir la comisión de actos lesivos que no encajan con las figuras penales tradicionales. Por ello, sostiene que es necesario repensar la

estructura del derecho penal, adaptándola a los desafíos del entorno digital y asegurando que las normas no queden obsoletas frente a los avances tecnológicos (Llaneza, 2021).

Asimismo, hay que considerar que la utilización de las nuevas tecnologías de generación de imágenes no solamente vulnera la intimidad, sino también la dignidad y el derecho a la imagen propia, reforzando así la necesidad de un tratamiento legal adecuado.

Para Carbajo Cascón (2020), la inteligencia artificial introduce riesgos penales emergentes que muchas veces no encuentran cabida dentro de los tipos existentes, lo que hace urgente una reflexión normativa sobre la creación de nuevos delitos. Explica que las herramientas tecnológicas avanzan a un ritmo más rápido que la legislación, generando situaciones donde el daño se produce, pero la ley no logra describirlo ni sancionar correctamente. En ese sentido, plantea que el Derecho Penal debe modernizarse e integrar marcos adaptativos, capaces de atender los problemas derivados del uso indebido de algoritmos y contenidos generados artificialmente (Carbajo Cascón, 2020).

En la misma línea, Varela (2021) argumenta que el derecho a la imagen frente a las tecnologías de inteligencia artificial necesita una protección normativa específica, ya que la manipulación digital puede afectar de forma directa la identidad, la autonomía y la dignidad de las personas. El autor explica que cuando se crean representaciones falsas, se lesiona la capacidad del individuo de decidir sobre su propia imagen y sobre cómo quiere ser percibido por los demás. Este fenómeno, al mismo tiempo, provoca un daño moral profundo, pues distorsiona la identidad personal y despoja a la víctima del control sobre su propia figura. Por eso, propone

que el ordenamiento jurídico incorpore normas penales claras y modernas, capaces de salvaguardar la dignidad y autenticidad del individuo frente al avance de la manipulación digital (Varela, 2021).

Fuera de Ecuador han existido casos de creación y difusión de deepnudes que no llegaron a proceso judicial, pero sí generaron un gran impacto mediático y, por tanto, reflexión académica. El caso ilustrativo fue el de la aplicación llamada DeepNude en 2019, que permitía crear desnudos artificiales de mujeres a partir de fotografías reales. Tras este escándalo, la aplicación fue retirada, pero su código inspiró el surgimiento de otras aplicaciones que continuaron circulando en internet. Asimismo, en 2020, en la aplicación Telegram en Italia, se reportaron varias comunidades donde operan bots capaces de generar deepnudes de mujeres y adolescentes de manera automática. Estos acontecimientos causaron alarma social y demostraron que no existen aún herramientas jurídicas adaptadas a las nuevas formas de violencia digital.

Tanto Chesney y Citron (2019) como Simó Soler (2023) coinciden en que casos como la aplicación DeepNude o los bots de Telegram muestran cómo la tecnología puede ser utilizada para producir y difundir violencia digital sin consecuencias judiciales inmediatas. Los autores sostienen que estos hechos reflejan la facilidad con la que se pueden generar contenidos sintéticos de apariencia real, los cuales afectan la intimidad, la reputación y la dignidad de las personas involucradas. Además, advierten que la respuesta del derecho penal sigue siendo insuficiente frente al ritmo de desarrollo tecnológico, lo que deja una brecha preocupante entre la realidad social y la capacidad jurídica de protección. Por eso, enfatiza en la necesidad de

establecer marcos legales más claros y preventivos, capaces de anticiparse a las consecuencias del mal uso de la inteligencia artificial (Chesney & Citron, 2019; Simó Soler, 2023).

2.6. CASOS Y EJEMPLOS NACIONALES RELEVANTES

En Ecuador se registraron diferentes casos de difusión no consentida de contenido íntimo, los cuales son conocidos popularmente como “packs”, evidenciando patrones de acoso, extorsión y daño a la reputación. En 2019 ocurrió uno de los sucesos más relevantes en el país, en específico en la provincia de Manabí, donde varios estudiantes de bachillerato denunciaron la difusión masiva de fotografías de carácter sexual que fueron obtenidas sin consentimiento previo. Este caso provocó que la Defensoría del Pueblo se pronunciara, advirtiendo sobre la necesidad de reforzar la regulación en cuanto a la violencia por medios digitales (Diario El Comercio, 2019; Defensoría del Pueblo, Boletín Oficial, 2019).

Si bien es cierto que este caso gira en torno a imágenes reales, el resultado final refleja lo que también producen los deepnudes: vulneración a la intimidad, afectación social y dificultad para retirar los contenidos de las plataformas digitales. Los adolescentes, mujeres y figuras públicas son las principales afectadas, configurando así una forma clara de violencia digital de género y revelando las falencias institucionales frente al riesgo de victimización.

Como explica Hervas Paredes (2023), la difusión no consentida de material íntimo en entornos digitales pone de manifiesto vacíos de protección legal y barreras estructurales que impiden una tutela efectiva del derecho a la intimidad. En su análisis, el autor señala que la falta de protocolos claros, la lentitud de las investigaciones y la ausencia de normas adaptadas a los

entornos tecnológicos generan un círculo de impunidad, donde las víctimas no logran obtener justicia ni reparación. Este panorama refleja que la legislación ecuatoriana necesita una actualización urgente, especialmente en lo que respecta a la protección de datos, la responsabilidad de las plataformas y los delitos cometidos mediante el uso de nuevas tecnologías (Hervas Paredes, 2023).

Estos antecedentes permiten extrapolar la situación cuando ocurra con contenido creado de forma sintética, puesto que la lesión al bien jurídico persiste e incluso puede incrementarse por la forma extremadamente realista y la rápida viralización. Igualmente, la falta de una imagen real previa provoca obstáculos frente a la tipificación actual de la norma, dejando en evidencia que se necesitan reformas penales específicas y programas de respuesta rápida por parte de Fiscalía, Policía y plataformas digitales.

Desde la óptica de Simó Soler (2023), los deepfakes y, en particular, los deepnudes, operan como nuevas formas de violencia digital que reproducen patrones de cosificación y estereotipos de género. La autora indica que este tipo de conductas tienen consecuencias especialmente graves sobre mujeres y adolescentes, pues afectan su reputación, su bienestar emocional y su entorno social. Además, advierte que el impacto de estas tecnologías no solo se mide en el daño individual, sino en la normalización de prácticas digitales abusivas que perpetúan desigualdades estructurales. Por ello, plantea que los Estados deben adoptar respuestas legales específicas, que contemplen tanto la sanción penal como mecanismos de prevención y educación digital (Simó Soler, 2023).

Los medios de comunicación ecuatorianos evidenciaron que las víctimas por la difusión no consentida de contenido íntimo enfrentan procesos de revictimización, dificultades para eliminar el material y una respuesta institucional deficiente. En el plano probatorio, la trazabilidad de los archivos, la preservación de evidencias digitales y la cooperación con las plataformas tecnológicas se convierten en cuellos de botella críticos, tanto en casos de imágenes reales como en representaciones sintéticas.

Por ejemplo, en Quito, durante 2021, se denunció la existencia de grupos de Telegram y WhatsApp dedicados a compartir fotografías y videos sexuales de mujeres sin su autorización. La investigación reveló miles de archivos y participantes de distintas provincias, lo que provocó indignación social y la intervención tanto de la Defensoría del Pueblo como del Ministerio de Educación, al confirmarse la presencia de contenido de adolescentes (Diario El Universo, 2021; Defensoría del Pueblo del Ecuador, Boletín Oficial, 2021).

Como señala Paredes Castañeda (2022), las manifestaciones de violencia digital contra las mujeres se agravan debido a la persistencia del contenido en línea, la facilidad de reproducción y la falta de marcos legales eficaces que garanticen una tutela oportuna.

El autor explica que, a diferencia de la violencia tradicional, el daño digital es continuo y expansivo, porque el material circula de manera ilimitada y puede reaparecer en cualquier momento. Esta característica genera una revictimización constante, lo que exige la intervención

de legislaciones más dinámicas, capaces de equilibrar la libertad tecnológica con la protección de los derechos humanos (Paredes Castañeda, 2022).

En octubre de 2023 se conoció en la ciudad de Quito un caso de violencia sexual digital dentro de un colegio privado, donde se habría utilizado inteligencia artificial para generar imágenes de carácter sexual con los rostros de varias estudiantes de bachillerato. La denuncia fue presentada ante la Fiscalía luego de que una fundación recibiera reportes del hecho, lo que llevó al Ministerio de Educación a activar los protocolos de protección y a pronunciarse públicamente. Según reportes de medios nacionales, las imágenes fueron creadas mediante software que alteraba fotografías reales, afectando directamente la intimidad y la dignidad de las víctimas. En protesta, un grupo de estudiantes realizó un plantón frente al establecimiento educativo, exigiendo justicia y sanciones ejemplares. Aunque las autoridades confirmaron la apertura de una investigación penal, hasta la fecha no se ha revelado la identidad de los implicados ni se han informado sentencias firmes, en atención a la protección de menores de edad (El Universo, 2024).

En síntesis, los casos ecuatorianos respecto a la difusión de material íntimo real anticipan los problemas jurídicos y probatorios de los deepnudes: un daño cierto al bien jurídico de la intimidad y la dignidad, dificultades de subsunción típica y un marco penal que aún no logra responder al ritmo de los avances tecnológicos.

2.7. REFERENCIAS COMPARADAS MÍNIMAS

A nivel comparativo, varios países han logrado avanzar de manera más concreta en la construcción de respuestas normativas frente a la violencia digital, y de forma específica ante la difusión y creación de contenido íntimo no consentido generado mediante inteligencia artificial. En España, por ejemplo, la Ley Orgánica 10/2022 introdujo reformas penales que reconocen la violencia sexual digital como una forma autónoma de agresión, promoviendo además políticas públicas orientadas a la prevención, educación y reparación integral de las víctimas. En el Reino Unido, la Online Safety Act estableció obligaciones de diligencia para las plataformas digitales, imponiendo responsabilidades activas a los proveedores de servicios frente a la publicación y difusión de contenido íntimo no autorizado. Por su parte, Estados Unidos se encuentra en una etapa más fragmentada, con distintos estados adoptando sus propias regulaciones, tanto por la vía penal como civil, para sancionar la creación o difusión de deepfakes y deepnudes con fines sexuales.

El panorama internacional evidencia un avance sostenido en la regulación de estas nuevas formas de violencia digital, en claro contraste con Ecuador, donde todavía no existe una norma penal clara ni específica que permita sancionar la creación o difusión de imágenes íntimas sintéticas, dejando un vacío legal que limita la protección efectiva de los derechos fundamentales.

- España (Ley Orgánica 10/2022 y Código Penal)

En el caso español, la Ley Orgánica 10/2022 reforzó la protección frente a la violencia sexual también en los entornos digitales. Además, el Código Penal cuenta con artículos que pueden aplicarse a este tipo de casos, como el artículo 197.7, que sanciona la difusión no

consentida de imágenes íntimas, y el artículo 172 ter, que castiga el acoso o stalking, ambos útiles frente a comportamientos de hostigamiento digital vinculados a la publicación de contenido sexual no autorizado.

Como señala la Ley Orgánica 10/2022, la respuesta española frente a la violencia sexual no se limita al contacto físico, sino que incluye su manifestación digital, integrando medidas de prevención y atención a las víctimas. En conjunto, estas disposiciones conforman un modelo que combina la sanción penal con políticas públicas de educación y acompañamiento, fortaleciendo así la protección integral frente a la violencia sexual digital (Ley Orgánica 10/2022; Código Penal español, arts. 197.7 y 172 ter).

- Reino Unido (Online Safety Act, 2023)

En el Reino Unido, el modelo regulatorio es más preventivo y técnico. La Online Safety Act de 2023 impone deberes de diligencia a las plataformas digitales, exigiendo que evalúen y mitiguen los riesgos derivados de contenidos dañinos, especialmente los de carácter sexual o manipulados mediante inteligencia artificial. La norma prioriza la creación de mecanismos de reporte y eliminación rápida del contenido ilícito, complementando así las leyes penales ya existentes.

Como destaca la Online Safety Act (2023), el enfoque británico traslada parte de la responsabilidad a los proveedores de servicios, obligándolos a implementar políticas de supervisión y gestión de riesgos. Este esquema representa un avance significativo, ya que

promueve una cooperación activa entre el Estado y las empresas tecnológicas, marcando una diferencia importante respecto a sistemas más tradicionales donde toda la carga recae en la víctima (Online Safety Act, UK, 2023).

- Estados Unidos (legislación estatal)

En el caso de Estados Unidos, aún no existe una ley federal uniforme sobre los deepnudes, pero distintos estados han tomado la iniciativa con enfoques variados. En Virginia, se tipificó la difusión no consentida de imágenes sexuales sintéticas, mientras que California habilitó acciones civiles específicas para demandar la creación o distribución de deepnudes y estableció procedimientos para la eliminación del material. Por otro lado, Texas incorporó normas contra los deepfakes utilizados con fines electorales, además de regulaciones sobre pornografía no consensuada, que pueden aplicarse por analogía a imágenes generadas artificialmente.

Como explican distintos análisis legislativos, la falta de un marco federal unificado ha generado un mosaico de soluciones locales, donde cada estado combina herramientas penales y civiles para enfrentar el fenómeno. Esto demuestra un esfuerzo descentralizado, pero efectivo, por adaptar la normativa estadounidense a los nuevos riesgos digitales que surgen con la inteligencia artificial (legislación estatal de Virginia, California y Texas, 2023).

- Doctrina comparada

Desde la perspectiva doctrinal, De Hert y Papakonstantinou (2018) sostienen que la regulación de los deepfakes presenta dilemas jurídicos que giran entre la libertad de expresión, la protección de datos personales y la necesidad de una respuesta penal proporcional. Los autores plantean que la mejor alternativa sería un modelo híbrido, en el que las plataformas digitales asuman parte de la responsabilidad, mientras que el derecho penal intervenga sólo en los casos más graves, donde exista una afectación real a la dignidad o la intimidad. De esta manera, proponen equilibrar la innovación tecnológica con la protección de derechos fundamentales (De Hert & Papakonstantinou, 2018).

- Contraste con Ecuador

En Ecuador, la ausencia de una tipificación expresa sobre imágenes íntimas sintéticas mantiene un vacío jurídico evidente. Intentar aplicar el artículo 178 del COIP a casos de deepnudes implicaría incurrir en una analogía prohibida por el principio de legalidad, lo que hace inviable la sanción penal bajo la normativa actual. En contraste, el derecho comparado ofrece alternativas viables:

(i) la creación de tipos penales específicos para contenidos sexuales generados artificialmente;

(ii) la implementación de remedios civiles que permitan la reparación del daño; y

(iii) el establecimiento de deberes de diligencia y responsabilidad para las plataformas tecnológicas.

Este contraste deja en claro que Ecuador aún debe adaptar su legislación penal a los retos de la era digital, tomando como referencia los avances normativos de otras jurisdicciones que han sabido equilibrar la libertad de expresión con la protección de la intimidad y la dignidad humana.

2.8. CONCLUSIONES PARCIALES

El análisis del marco jurídico ecuatoriano permite concluir que tanto la Constitución como el Código Orgánico Integral Penal (COIP) protegen bienes jurídicos esenciales como la intimidad, la dignidad y la imagen personal. Sin embargo, dichas normas no contemplan de manera expresa la existencia de imágenes sintéticas producidas mediante inteligencia artificial, lo que genera un vacío legal frente a fenómenos como los deep nudes. En estos casos, aunque se afecta la intimidad y la identidad de la víctima, la norma penal vigente exige la existencia de una imagen real para configurar el tipo, dejando fuera a las representaciones creadas artificialmente. Como señalan Guzmán y Ramírez (2021), el ordenamiento penal ecuatoriano limita su protección a la imagen real, generando una brecha jurídica frente a la difusión de contenidos fabricados digitalmente.

Intentar aplicar las disposiciones actuales a este tipo de conductas sería jurídicamente inseguro, pues implicaría recurrir a la analogía, mecanismo prohibido en Derecho Penal y contrario al principio de legalidad consagrado en el artículo 76 de la Constitución. Esta situación no solo compromete la seguridad jurídica, sino que también evidencia la necesidad urgente de una reforma penal que incorpore expresamente este tipo de representaciones sintéticas. Tal reforma deberá

abordarse en el Capítulo II, donde se desarrollará una propuesta orientada a adecuar el sistema jurídico ecuatoriano a las nuevas formas de vulneración digital.

3. CAPÍTULO II: LIMITACIONES NORMATIVAS Y VACÍOS EN LA IMPUTACIÓN PENAL DE IMÁGENES ÍNTIMAS FALSAS EN EL MARCO JURÍDICO ECUATORIANO

El presente capítulo aborda de manera exhaustiva las limitaciones normativas y los vacíos existentes en la imputación penal de imágenes íntimas falsas, particularmente aquellas generadas mediante herramientas de inteligencia artificial (IA), como los denominados deepnudes. Este fenómeno constituye uno de los retos más complejos para el derecho penal contemporáneo, pues evidencia la rapidez con la que la tecnología transforma las dinámicas sociales y, al mismo tiempo, tensiona la capacidad de los ordenamientos jurídicos para responder de manera oportuna y eficaz.

La progresiva sofisticación de las técnicas de manipulación digital ha permitido crear imágenes hiperrealistas de carácter íntimo sin que la persona representada otorgue su consentimiento, lesionando gravemente bienes jurídicos como la intimidad, la dignidad, el honor y la autodeterminación informativa. Según explica López Jiménez (2023), “la virtualidad y el anonimato potencian la agresión simbólica y amplifican su impacto, al permitir la difusión instantánea y masiva de contenidos que afectan la esfera más reservada de la personalidad” (p.

45). Frente a esta realidad, el marco penal ecuatoriano, representado principalmente por el Código Orgánico Integral Penal (COIP), enfrenta serias dificultades para encuadrar este tipo de conductas en tipos penales existentes, los cuales fueron concebidos para hechos tangibles y pruebas materiales tradicionales.

El avance de la inteligencia artificial plantea un desafío estructural: el sistema jurídico se mueve a un ritmo mucho más lento que la innovación tecnológica. Como señala Sanz y Rodríguez (2022), “el derecho penal es un instrumento de última ratio, pensado para proteger bienes jurídicos esenciales, pero su eficacia depende de la precisión con que las normas tipifican conductas lesivas, y esto exige actualización constante ante nuevas modalidades de agresión digital” (p. 67). En el caso ecuatoriano, aunque el COIP tipifica delitos como la violación a la intimidad, la difusión no consentida de contenidos sexuales o la pornografía infantil, ninguno de estos preceptos contempla de forma expresa la generación y circulación de imágenes íntimas falsas mediante IA, generando zonas grises que pueden derivar en impunidad.

La ausencia de regulaciones específicas tiene varias consecuencias. Por un lado, limita la posibilidad de imputar responsabilidad penal a quienes producen o difunden este tipo de material, ya que las conductas no encajan de manera clara en los supuestos descritos por la ley. Por otro lado, provoca inseguridad jurídica para las víctimas, que no encuentran un cauce procesal idóneo para reclamar la reparación del daño ni para exigir la sanción de los responsables. De igual manera, los operadores de justicia —fiscales, jueces y defensores públicos— carecen de herramientas normativas y técnicas suficientes para investigar y juzgar adecuadamente estas agresiones.

El problema se agudiza cuando se considera la dimensión transnacional de la difusión de contenidos en internet. Las imágenes íntimas falsas pueden ser creadas en un país, alojadas en servidores ubicados en otro, y viralizadas globalmente en cuestión de segundos. Esta característica dificulta la aplicación territorial de las leyes penales y exige repensar los mecanismos de cooperación internacional. Experiencias comparadas, como las reformas legislativas adoptadas en el Reino Unido (Voyeurism (Offences) Act 2019) o en España (Ley Orgánica 10/2022, de garantía integral de la libertad sexual), han incorporado figuras específicas que sancionan la difusión no consentida de imágenes íntimas, incluidas aquellas manipuladas digitalmente. Sin embargo, tales avances no han sido replicados todavía en Ecuador, donde la respuesta normativa sigue siendo fragmentaria y limitada.

La doctrina penal ecuatoriana ha empezado a advertir estas lagunas. Pérez Paredes (2024) sostiene que “la protección de la intimidad debe ampliarse para incluir los supuestos en los que la imagen personal es creada artificialmente sin autorización, pues la afectación al bien jurídico es tan intensa como en los casos de difusión de material auténtico” (p. 112). En esa línea, surge la necesidad de diseñar tipos penales autónomos que contemplen la especificidad de las imágenes sintéticas, evitando forzar su encuadre en delitos concebidos para realidades analógicas.

Otro obstáculo reside en el plano probatorio. La imputación penal de imágenes íntimas falsas requiere demostrar no solo la existencia del material, sino también su carácter sintético y la intención dolosa de quien lo creó o divulgó. Esto implica peritajes informáticos avanzados, capaces de identificar metadatos, algoritmos generativos y patrones de manipulación digital. Sin embargo, en Ecuador los recursos forenses especializados en IA son escasos, lo que limita la capacidad del sistema de justicia para acreditar la autoría y autenticidad de las pruebas. La

carencia de protocolos claros para la preservación y análisis de evidencia digital agrava aún más este panorama.

Desde la perspectiva de la política criminal, la omisión legislativa frente a los deepnudes refleja un rezago en la adaptación del derecho penal a las nuevas formas de violencia digital. El legislador debe ponderar el principio de mínima intervención con la necesidad de garantizar una protección efectiva de los bienes jurídicos más sensibles, especialmente cuando se trata de agresiones que afectan desproporcionadamente a mujeres, adolescentes y colectivos vulnerables. La Relatora Especial de Naciones Unidas sobre la violencia contra la mujer (ONU, 2022) ha recomendado expresamente que los Estados tipifiquen de manera clara las prácticas de manipulación de imágenes íntimas, incorporando medidas de prevención, sanción y reparación integral.

3.1. Clasificación de limitaciones normativas

La normativa penal vigente en el Ecuador presenta múltiples limitaciones para abordar el fenómeno de las imágenes íntimas falsas generadas o modificadas mediante inteligencia artificial. Estas limitaciones se agrupan en tres grandes categorías: deficiencias en la tipificación, tensiones con los principios del derecho penal y dificultades de adaptación a las transformaciones tecnológicas.

En primer lugar, se observa que el artículo 178 del COIP, que sanciona la difusión de imágenes íntimas sin consentimiento, no contempla expresamente situaciones en las que el material difundido sea fabricado o manipulado digitalmente. Esta omisión genera un vacío sustantivo que

deja fuera de protección a víctimas cuyos derechos se ven afectados de igual manera que en los casos tradicionales de difusión de contenido real. La ausencia de una definición legal de “imagen sintética” o “imagen íntima falsa” limita el alcance de la protección penal y restringe la posibilidad de imputar responsabilidad a quienes crean o difunden este tipo de contenido.

En segundo lugar, las limitaciones se relacionan con el principio de legalidad y la prohibición de analogía *in malam partem*. El derecho penal requiere que las conductas prohibidas estén claramente definidas en la ley; sin embargo, la velocidad de los avances tecnológicos impide que las normas mantengan un ritmo adecuado de actualización. Esto plantea la pregunta de hasta qué punto puede interpretarse extensivamente la norma penal para incluir conductas no previstas explícitamente, sin comprometer las garantías fundamentales del debido proceso.

Por último, la normativa penal ecuatoriana carece de disposiciones que reconozcan las particularidades del entorno digital y de la inteligencia artificial. Las figuras clásicas de autoría y participación, así como los elementos de imputación objetiva, no siempre resultan idóneos para hechos donde el daño se produce mediante algoritmos o sistemas automáticos. Autores como Silva Sánchez (2013) señalan que el derecho penal se enfrenta a un fenómeno de expansión, obligado a intervenir en ámbitos antes ajenos a su lógica, lo que genera tensiones entre la eficacia preventiva y el respeto a los límites del *ius puniendi*. En el caso ecuatoriano, esta problemática se agrava por la falta de mecanismos que permitan perseguir penalmente a quienes, desde fuera del territorio nacional, generan o difunden imágenes íntimas falsas que afectan a ciudadanos locales.

La clasificación de estas limitaciones evidencia que no basta con pequeños ajustes normativos, sino que se requiere una reflexión profunda sobre la estructura misma del derecho penal en la era digital. El desafío radica en equilibrar la protección de los derechos fundamentales de las víctimas con la necesidad de preservar los principios garantistas que caracterizan al derecho penal moderno.

La normativa penal vigente en el Ecuador presenta múltiples limitaciones para abordar el fenómeno de las imágenes íntimas falsas generadas o modificadas mediante inteligencia artificial (IA). Estas limitaciones no solo afectan la capacidad del sistema jurídico para proteger eficazmente los bienes jurídicos implicados —intimidad, honor, dignidad y autodeterminación informativa—, sino que también comprometen la seguridad jurídica de víctimas, investigados y operadores de justicia. A partir del análisis doctrinal y normativo, estas carencias pueden agruparse en tres grandes categorías: deficiencias en la tipificación, tensiones con los principios del derecho penal, y dificultades de adaptación frente a las transformaciones tecnológicas.

3.1.1 Deficiencias en la tipificación

El primer obstáculo reside en la ausencia de una regulación expresa que contemple las imágenes íntimas falsas o “sintéticas” dentro del catálogo de conductas punibles. El artículo 178 del Código Orgánico Integral Penal (COIP) sanciona la difusión de imágenes íntimas sin consentimiento, pero su redacción presupone que el material difundido sea auténtico, es decir, que corresponda efectivamente a la persona afectada. Esta concepción clásica ignora las particularidades de los deepnudes, cuyo rasgo distintivo es la manipulación o fabricación de contenido hiperrealista sin autorización de la persona representada.

La inexistencia de una definición legal de “imagen sintética” o “imagen íntima falsa” limita el alcance de la protección penal y deja en una zona de impunidad a quienes resultan lesionados por estas prácticas. En consecuencia, los fiscales enfrentan dificultades para encuadrar la conducta en un tipo penal, y muchas veces los casos terminan archivados por falta de adecuación típica.

Ejemplo hipotético: María, estudiante universitaria en Quito, descubre que en redes sociales circula una imagen en la que aparece desnuda, aunque ella nunca posó para tal fotografía. Una investigación técnica revela que se trata de una creación obtenida mediante un programa de IA a partir de fotos tuyas disponibles en su perfil público. Cuando presenta la denuncia, la fiscalía no encuentra un tipo penal específico para imputar al autor, ya que el artículo 178 COIP exige que la imagen sea “real”. La causa termina desestimada, dejando a María sin tutela penal efectiva.

Este caso refleja cómo la falta de precisión normativa provoca que las víctimas no encuentren amparo legal, y los agresores puedan actuar con sensación de impunidad.

3.1.2 Tensiones con los principios del derecho penal

El segundo grupo de limitaciones se vincula con los principios que rigen el derecho penal, especialmente el principio de legalidad y la prohibición de analogía in malam partem. Según el artículo 76 de la Constitución ecuatoriana y el artículo 5 del COIP, nadie puede ser sancionado por una conducta que no esté descrita de manera previa, clara y expresa en la ley.

En materia de imágenes íntimas falsas, esta exigencia entra en tensión con la necesidad de proteger los derechos fundamentales frente a modalidades de agresión que no existían al

momento de redactar la norma. Si los jueces intentan aplicar el artículo 178 del COIP por analogía, corren el riesgo de vulnerar garantías básicas como el debido proceso o el principio de mínima intervención penal.

Doctrinarios como Muñoz Conde (2020) advierten que “el uso extensivo de tipos penales para abarcar conductas no previstas compromete el núcleo garantista del *ius puniendi* y puede derivar en un derecho penal de autor más que de acto” (p. 89). En otras palabras, el legislador debe ponderar cuidadosamente la creación de nuevos delitos, asegurando que la expansión del sistema penal no sacrifique las libertades individuales.

Sin embargo, la ausencia de un marco legal claro provoca que, en la práctica, los jueces deban improvisar soluciones interpretativas, generando criterios dispares y afectando la seguridad jurídica.

3.1.3 Dificultades de adaptación frente a las transformaciones tecnológicas

La tercera categoría de limitaciones deriva de la incapacidad de la normativa penal para adaptarse al ritmo de las innovaciones tecnológicas. Las imágenes íntimas falsas son producidas por algoritmos capaces de aprender, replicar rostros y cuerpos, y generar representaciones extremadamente realistas en cuestión de segundos. Estas particularidades cuestionan la idoneidad de las figuras clásicas de autoría y participación, así como los criterios de imputación objetiva desarrollados para delitos convencionales.

El COIP no contempla disposiciones específicas que regulen la responsabilidad penal por el uso de sistemas automatizados o por la intervención de múltiples agentes dispersos en distintas jurisdicciones. Esto se traduce en problemas para determinar la autoría: ¿es responsable el

programador del software, quien lo ejecuta para generar la imagen, o quien la difunde masivamente?

Además, la dimensión transnacional de la difusión en internet dificulta la aplicación territorial de las normas penales ecuatorianas. Es frecuente que los servidores donde se aloja el contenido estén ubicados en otros países, lo que exige mecanismos eficaces de cooperación internacional. En Ecuador, la cooperación en delitos informáticos aún es incipiente, y los procesos se ralentizan por falta de convenios o de personal especializado en peritajes digitales avanzados.

3.1.4 La necesidad de un replanteamiento estructural

La clasificación anterior revela que no basta con introducir pequeños ajustes al articulado del COIP. El problema es más profundo y compromete la propia estructura del derecho penal en la era digital. Siguiendo a Silva Sánchez (2013), el derecho penal experimenta un fenómeno de “expansión”, viéndose obligado a intervenir en ámbitos antes ajenos a su lógica, lo que genera tensiones entre eficacia preventiva y respeto a los límites del *ius puniendi*.

En el contexto ecuatoriano, este desafío requiere una reflexión multidimensional:

1. Tipificación clara y diferenciada de las imágenes íntimas falsas, que reconozca su autonomía respecto de la pornografía infantil o la difusión de contenido real sin consentimiento.
2. Protocolos probatorios y capacidades forenses, para garantizar que los peritajes puedan identificar con certeza el uso de IA y establecer la autoría.

3. Cooperación internacional, a fin de superar los obstáculos derivados de la ubicuidad de los contenidos en la red.
4. Capacitación permanente de fiscales, jueces y policías en delitos tecnológicos y derechos digitales.

Solo mediante una reforma integral, que combine el fortalecimiento del marco legal con la dotación de recursos técnicos y humanos, será posible ofrecer respuestas eficaces y respetuosas de los derechos fundamentales. El caso hipotético de María ilustra que la omisión legislativa actual no solo favorece la impunidad, sino que perpetúa la vulnerabilidad de quienes son objeto de agresiones digitales cada vez más sofisticadas.

3.2. Vacíos legales específicos

Los vacíos legales en torno a la regulación de las imágenes íntimas falsas generadas o alteradas mediante inteligencia artificial representan uno de los obstáculos más significativos para la protección de las víctimas. Estos vacíos impiden brindar una protección efectiva a los derechos fundamentales de las personas y ponen en evidencia la insuficiencia del Código Orgánico Integral Penal (COIP) para abordar problemáticas propias de la era digital.

Un aspecto central es la carencia de una definición normativa de 'imagen sintética' o 'deepfake'. Desde el plano dogmático, delimitar el objeto de protección penal exige precisar el alcance del término 'imagen íntima' cuando se trata de contenido fabricado o manipulado con herramientas tecnológicas. La falta de tal precisión dificulta la subsunción típica de estas conductas en las figuras tradicionales de revelación de secretos o violación de la intimidad. Autores como Floridi

(2019) y Solove (2021) advierten que el derecho debe adaptarse para responder a nuevas formas de agresión informacional que alteran la autodeterminación y dignidad de las personas.

Desde la dogmática penal, se discute si los deepfakes de carácter sexual deben considerarse dentro de los delitos contra la intimidad o si corresponde crear un tipo penal autónomo que contemple las particularidades de su producción y difusión. Mientras algunos sostienen que el principio de legalidad obliga a describir con claridad y detalle estas conductas para evitar interpretaciones extensivas, otros resaltan que la naturaleza especialmente lesiva de estos ataques justifica un tratamiento punitivo expreso, aunque ello implique innovar en las técnicas legislativas.

La experiencia comparada aporta elementos útiles para reflexionar sobre posibles soluciones normativas. En España, la Ley Orgánica 10/2022 incorporó la difusión de imágenes íntimas alteradas o creadas digitalmente como forma de violencia sexual, lo que evidencia un reconocimiento expreso del daño derivado de los deepfakes. El Reino Unido, mediante el Online Safety Act (2023), tipificó la creación y difusión de imágenes íntimas falsas sin consentimiento, diferenciando supuestos en función de la intención de causar angustia o humillación. En Estados Unidos, varios estados —como California, Texas y Virginia— han promulgado leyes específicas contra la denominada deepfake pornography, imponiendo penas agravadas cuando las víctimas son figuras públicas o menores de edad. En el ámbito europeo, el AI Act y el Digital Services Act (DSA) establecen obligaciones para plataformas y proveedores de servicios digitales, incluyendo la detección, moderación y eliminación de contenidos ilícitos.

Estos precedentes ponen de relieve que la respuesta normativa debe ser integral: no basta con crear nuevos tipos penales, sino que se requieren mecanismos preventivos, obligaciones de diligencia para intermediarios y protocolos eficaces para la remoción rápida de material ilícito. El enfoque debe combinar instrumentos penales, civiles y administrativos, así como políticas de educación digital orientadas a la prevención.

En el caso ecuatoriano, es necesario fortalecer el marco normativo del COIP con varias medidas:

1. Incluir en el artículo 178 una referencia explícita a la fabricación o alteración de imágenes íntimas mediante inteligencia artificial, aun cuando no exista una imagen real de base.
2. Incorporar agravantes cuando la conducta implique difusión masiva o automatizada, o cuando las víctimas sean menores, personas adultas mayores o integrantes de grupos vulnerables.
3. Establecer la responsabilidad de plataformas y redes sociales que, con conocimiento del carácter ilícito del contenido, no actúen diligentemente para retirarlo.
4. Crear procedimientos cautelares expeditos que permitan el bloqueo de enlaces o la eliminación de archivos, reduciendo el tiempo de exposición de las víctimas al daño.

La protección integral de las víctimas constituye otro elemento clave. Deben preverse medidas de apoyo psicológico y jurídico, así como el ejercicio del derecho al olvido digital, facilitando la eliminación de referencias en buscadores y redes. Asimismo, resulta pertinente valorar la creación de un fondo de reparación, alimentado por sanciones a infractores y plataformas negligentes, para cubrir gastos de asistencia legal y terapéutica.

En definitiva, los vacíos legales sobre imágenes íntimas falsas no son exclusivos del Ecuador,

pero su persistencia en el país genera una brecha significativa de protección. Adoptar normas claras, complementadas por políticas preventivas y medidas de apoyo a las víctimas, permitirá enfrentar de manera más eficaz el impacto de las imágenes fabricadas o alteradas mediante inteligencia artificial, alineando la respuesta penal con los desafíos de la sociedad digital contemporánea.

3.3. Retos prácticos en la imputación penal

Más allá de los problemas normativos, la imputación penal de conductas vinculadas con la creación y difusión de imágenes íntimas falsas enfrenta desafíos prácticos considerables. Uno de los más complejos es la identificación de los autores y partícipes, conforme al artículo 42 del COIP. La naturaleza descentralizada de Internet, combinada con técnicas de anonimización y el uso de redes privadas virtuales (VPN), dificulta rastrear la fuente original del contenido ilícito. En ocasiones, las imágenes son replicadas y redistribuidas tantas veces que resulta casi imposible determinar el punto inicial de la infracción.

También surgen interrogantes en torno a la participación de diferentes actores en estas conductas. Los instigadores, cómplices o coautores pueden desempeñar papeles distintos en la creación, alteración o divulgación de las imágenes, lo que complica la asignación de responsabilidad penal. A ello se suma el rol de las plataformas digitales, cuya intervención u omisión en la eliminación de contenidos puede interpretarse, en ciertos casos, como una forma de complicidad o cooperación necesaria. Sin embargo, la legislación ecuatoriana no establece con claridad los estándares de diligencia exigibles a estos intermediarios.

Otro aspecto crítico es la dimensión transnacional de estos delitos. La producción,

almacenamiento o difusión de imágenes íntimas falsas suele involucrar servidores ubicados fuera del país, lo que plantea problemas de jurisdicción y cooperación internacional. La tramitación de asistencias judiciales o exhortos internacionales puede ser lenta e ineficaz frente a la rapidez con que el contenido se replica en línea. Estos obstáculos requieren fortalecer los mecanismos de cooperación judicial y adoptar estrategias de investigación que incluyan el rastreo de datos electrónicos, análisis forense digital y colaboración con empresas tecnológicas globales.

Más allá de los problemas estrictamente normativos, la imputación penal de conductas vinculadas con la creación y difusión de imágenes íntimas falsas enfrenta desafíos prácticos significativos que comprometen la eficacia del sistema de justicia penal. Estos retos se relacionan con la identificación de los autores, la delimitación de responsabilidades entre distintos partícipes, el papel de las plataformas digitales, la obtención y preservación de la prueba electrónica, y la dimensión transnacional de los hechos. A continuación, se examinan en detalle cada uno de estos aspectos.

3.3.1 Identificación de autores y partícipes

Uno de los obstáculos centrales radica en la atribución de responsabilidad penal a los autores materiales de la creación o difusión de imágenes íntimas falsas. El artículo 42 del COIP establece que autores son quienes ejecutan directa o indirectamente la conducta típica; sin embargo, la descentralización de Internet y el uso de tecnologías que garantizan anonimato — como redes privadas virtuales (VPN), navegadores que protegen la identidad o servicios de alojamiento cifrados — dificultan rastrear la fuente original del contenido ilícito.

En muchos casos, el material se replica y redistribuye en cuestión de segundos, generando una multiplicidad de copias en distintos servidores y países. Ello complica determinar el punto inicial de la infracción y, en consecuencia, acreditar la autoría o participación en el hecho. Según Villamarín (2023), “la trazabilidad de contenidos digitales exige técnicas de investigación avanzadas, pero estas resultan inútiles si el marco legal y los recursos institucionales no permiten un rastreo eficaz en tiempo real” (p. 57).

A esto se suma que los responsables pueden operar desde cuentas falsas o identidades suplantadas, lo que exige una coordinación estrecha con proveedores de servicios de internet y redes sociales para acceder a registros de direcciones IP, datos de sesión y metadatos. Sin embargo, las solicitudes de información suelen enfrentar resistencias, demoras o negativas por parte de empresas extranjeras que priorizan la protección de datos de sus usuarios o están sujetas a legislaciones distintas.

3.3.2 Complejidad en la participación delictiva

El esquema de participación en este tipo de conductas presenta un grado de sofisticación inédito. No siempre existe un único responsable; por el contrario, la agresión puede ser el resultado de acciones encadenadas de varios sujetos: quien recopila las imágenes originales, quien las manipula mediante IA, quien las difunde en redes sociales o mensajería instantánea, e incluso quienes incentivan o financian la producción del contenido.

Esta pluralidad plantea dificultades para delimitar la responsabilidad penal conforme a las categorías de autoría, coautoría, complicidad o instigación previstas en el COIP. Por ejemplo, ¿qué grado de reproche corresponde al usuario que, sin haber generado el material, lo comparte

en grupos cerrados o foros públicos? Para Lascano (2021), “la imputación debe graduarse según el dominio del hecho y el conocimiento del carácter ilícito del contenido, pero estas variables son complejas de probar en entornos digitales donde la circulación de datos es casi automática” (p. 112).

Asimismo, surge el debate sobre la responsabilidad de las plataformas digitales. Si bien no participan directamente en la creación o difusión inicial, su intervención u omisión en la eliminación de contenidos puede incidir en la perpetuación del daño. En ausencia de estándares normativos claros sobre la diligencia exigible a intermediarios, los tribunales carecen de parámetros uniformes para evaluar si la falta de respuesta oportuna constituye cooperación necesaria o mera omisión administrativa.

3.3.3 Obtención y preservación de la prueba electrónica

La imputación penal requiere evidencia sólida que permita acreditar tanto la existencia del hecho como la participación del investigado. En delitos relacionados con imágenes íntimas falsas, la prueba suele consistir en archivos digitales, registros de actividad en redes sociales, metadatos y rastros en servidores remotos. La cadena de custodia de estos elementos es particularmente delicada, pues cualquier alteración o pérdida de información puede inutilizar el material probatorio.

En Ecuador, aunque el COIP y el Código Orgánico General de Procesos reconocen la validez de la prueba electrónica, no existen protocolos específicos para el manejo de contenidos creados mediante IA. La ausencia de peritos especializados en análisis de algoritmos generativos o en verificación de autenticidad de imágenes limita las capacidades de la fiscalía. Según un

informe de la Asociación Latinoamericana de Derecho y Tecnología (ALDT, 2024), “la escasez de laboratorios forenses con equipamiento idóneo y personal capacitado en IA constituye una de las principales barreras para el procesamiento de estos delitos” (p. 34).

Además, la velocidad con que el material puede ser eliminado o modificado en línea obliga a actuar con premura. Si la autoridad no reacciona rápidamente, la prueba puede desaparecer, reduciendo las posibilidades de éxito en el proceso penal.

3.3.4 Dimensión transnacional y cooperación judicial

La producción, almacenamiento y difusión de imágenes íntimas falsas suelen involucrar servidores ubicados fuera del país, cuentas administradas desde el extranjero o redes sociales domiciliadas en jurisdicciones con marcos regulatorios distintos. Esto plantea problemas de jurisdicción y cooperación internacional.

La tramitación de exhortos o asistencias judiciales internacionales suele ser lenta y burocrática, mientras que el contenido ilícito se replica y viraliza en segundos. La disparidad entre los tiempos procesales y la dinámica de internet favorece la perpetuación del daño. Como observa García (2022), “el carácter global de los flujos digitales exige tratados específicos y procedimientos abreviados para la obtención de datos electrónicos y la eliminación de contenidos dañinos” (p. 78).

Si bien Ecuador es parte de instrumentos como la Convención de Budapest sobre ciberdelincuencia, su implementación es todavía incipiente, y la cooperación con empresas tecnológicas globales depende muchas veces de acuerdos informales o de la buena voluntad de los proveedores. La ausencia de protocolos bilaterales o multilaterales específicos para la

manipulación de imágenes íntimas deja a las víctimas en una situación de vulnerabilidad frente a agresores que operan desde otras latitudes.

3.3.5 Necesidad de estrategias integrales

Frente a estos retos, se impone la adopción de estrategias integrales que combinen reformas normativas, fortalecimiento institucional y alianzas con el sector privado. Entre las propuestas que surgen de la doctrina y de experiencias comparadas, destacan:

1. Creación de unidades especializadas en la fiscalía y la policía, dotadas de conocimientos en inteligencia artificial, trazabilidad digital y ciberinvestigación.
2. Establecimiento de acuerdos de cooperación con empresas tecnológicas para agilizar la entrega de datos y la eliminación de contenido ilícito.
3. Desarrollo de guías y manuales sobre custodia y análisis de prueba electrónica en casos de manipulación de imágenes.
4. Capacitación permanente de jueces, fiscales y defensores en delitos informáticos y derechos digitales, para garantizar decisiones coherentes y respetuosas de las garantías fundamentales.
5. Impulso de mecanismos alternativos de reparación, como órdenes judiciales de retirada de contenido, indemnización de daños y medidas de protección para las víctimas.

La imputación penal de conductas vinculadas con imágenes íntimas falsas en Ecuador enfrenta un conjunto de desafíos prácticos que exceden el ámbito normativo. La identificación de los responsables, la delimitación de grados de participación, la obtención y preservación de la

prueba, así como la cooperación internacional, son elementos que requieren atención prioritaria. Sin avances en estos frentes, la tipificación de nuevos delitos o la reforma de los existentes podría quedar vacía de contenido, sin capacidad real de disuasión o sanción.

Como advierte Silva Sánchez (2013), “el derecho penal solo puede cumplir su función preventiva si cuenta con instrumentos eficaces de persecución y prueba; de lo contrario, se convierte en una promesa incumplida” (p. 65). Por ello, el fortalecimiento de las capacidades operativas y el diseño de marcos de colaboración público-privada resultan indispensables para garantizar que la protección jurídica frente a la manipulación de imágenes íntimas no se quede en el plano declarativo, sino que se materialice en una tutela efectiva de los derechos fundamentales.

3.4. Impacto en política criminal

El fenómeno de las imágenes íntimas falsas generadas mediante inteligencia artificial tiene un profundo impacto en la política criminal, pues desafía las bases tradicionales sobre las que se han diseñado las estrategias de persecución penal. La falta de respuestas normativas claras genera un efecto de impunidad que desalienta la denuncia por parte de las víctimas y erosiona la confianza en las instituciones encargadas de administrar justicia. Esta situación transmite un mensaje de tolerancia social frente a nuevas formas de violencia digital, que resultan particularmente lesivas para la integridad psicológica y moral de quienes las padecen.

Desde una perspectiva de política criminal, es indispensable reconocer que el uso de la inteligencia artificial en la producción de contenidos ilícitos multiplica el daño potencial y

amplifica la capacidad de difusión. Las herramientas tecnológicas permiten replicar y viralizar material en cuestión de segundos, superando la capacidad de reacción del sistema penal. Por ello, los legisladores deben considerar reformas integrales que incluyan no solo la tipificación de estas conductas, sino también estrategias preventivas, protocolos de atención a víctimas y medidas de cooperación internacional.

Zaffaroni (2011) advierte que el derecho penal debe ajustarse a las dinámicas sociales emergentes sin caer en respuestas desproporcionadas. Esto implica diseñar normas que equilibren la protección de bienes jurídicos con el respeto a los principios de proporcionalidad, legalidad y mínima intervención. En el contexto de los deepnudes, la política criminal debería orientarse a prevenir la producción y difusión de contenido falso, garantizar la reparación a las víctimas y fomentar la educación digital para reducir la tolerancia social hacia estas prácticas.

La política criminal frente a las imágenes íntimas falsas debe buscar un equilibrio entre la protección de bienes jurídicos y el respeto de las garantías fundamentales. El uso desmedido del *ius puniendi* podría derivar en un derecho penal simbólico o en restricciones excesivas a la libertad de expresión y a la innovación tecnológica.

Zaffaroni (2011) advierte que “la inflación legislativa y la expansión irreflexiva de tipos penales conllevan el riesgo de convertir al derecho penal en un instrumento de control social desproporcionado” (p. 79). Por ello, las reformas deben priorizar la proporcionalidad y la mínima intervención, delimitando con precisión los elementos típicos de las conductas prohibidas y evitando sancionar expresiones legítimas o usos lícitos de la inteligencia artificial.

Una política criminal equilibrada requiere diferenciar claramente entre quienes generan imágenes falsas con fines lesivos —extorsión, acoso, difamación o humillación— y quienes desarrollan herramientas tecnológicas sin intención de causar daño. La regulación debe enfocarse en la finalidad del acto, en el consentimiento y en el perjuicio efectivo a los derechos de la persona retratada.

3.5. Articulación de medidas preventivas, reactivas y restaurativas

El impacto de las imágenes íntimas falsas obliga a repensar los instrumentos de intervención estatal, combinando políticas preventivas, mecanismos de reacción rápida y medidas de reparación integral. Entre las acciones preventivas destacan:

- Programas de educación y sensibilización digital, que permitan a la ciudadanía reconocer los riesgos del uso indebido de la IA y promover la cultura del consentimiento.
- Campañas públicas orientadas a reducir la tolerancia social hacia la difusión de contenidos falsos, especialmente cuando involucran violencia de género o acoso en línea.
- Regulación administrativa que exija a plataformas digitales implementar sistemas de detección y eliminación de contenido manipulado, con estándares claros de diligencia.

En el plano reactivo, la política criminal debe fortalecer las unidades especializadas en ciberdelincuencia, dotándolas de recursos técnicos y personal capacitado para investigar delitos relacionados con IA. Asimismo, resulta clave desarrollar protocolos de atención inmediata a víctimas, que incluyan asesoría jurídica, apoyo psicológico y medidas de protección frente a la revictimización.

Por último, las medidas restaurativas —como la reparación económica, la eliminación definitiva de contenido y el reconocimiento público del daño— son esenciales para restituir en la mayor medida posible la dignidad e integridad de las personas afectadas.

3.6. Cooperación internacional y gobernanza digital

La dimensión global de Internet convierte a la política criminal en un asunto que trasciende las fronteras estatales. La producción y difusión de deepnudes suele involucrar servidores y cuentas administradas desde otros países, lo que plantea la necesidad de cooperación judicial y policial internacional.

Instrumentos como la Convención de Budapest sobre ciberdelincuencia ofrecen un marco de colaboración, pero su implementación en Ecuador todavía es limitada. Se requieren acuerdos bilaterales y multilaterales que agilicen la obtención de datos, la ejecución de solicitudes de bloqueo y la asistencia técnica en investigaciones forenses.

Además, es indispensable promover estándares de gobernanza digital, orientados a que empresas tecnológicas globales asuman compromisos más firmes en la prevención y erradicación de contenidos que atenten contra la intimidad personal. La política criminal, en este sentido, debe dialogar con el derecho internacional de los derechos humanos y con los principios de responsabilidad corporativa, incentivando la adopción de códigos de conducta y mecanismos de autorregulación supervisada.

3.7. Hacia un modelo integral de política criminal

El impacto de las imágenes íntimas falsas no puede abordarse únicamente mediante la tipificación de nuevas figuras delictivas. La experiencia comparada demuestra que, sin medidas estructurales, los avances legislativos quedan reducidos a declaraciones simbólicas.

Un modelo integral de política criminal para Ecuador debería considerar:

1. Reformas legislativas que tipifiquen de manera expresa la creación y difusión de imágenes íntimas falsas, diferenciando entre conductas dolosas y usos legítimos de la IA.
2. Fortalecimiento institucional mediante la capacitación continua de jueces, fiscales y policías, así como la creación de laboratorios forenses especializados en IA.
3. Protocolos uniformes de actuación, que garanticen rapidez en la eliminación de contenidos y la preservación de pruebas digitales.
4. Promoción de alianzas público-privadas, dirigidas a establecer canales ágiles de cooperación con redes sociales, buscadores y proveedores de servicios de almacenamiento en la nube.
5. Políticas de reparación y acompañamiento a víctimas, que integren asistencia psicológica, asesoría jurídica y medidas de protección.

El impacto de las imágenes íntimas falsas en la política criminal ecuatoriana exige respuestas multidimensionales. No basta con sancionar a posteriori; es necesario prevenir, educar, reparar y cooperar en el ámbito internacional. Al mismo tiempo, estas respuestas deben enmarcarse en los principios de proporcionalidad, legalidad y respeto a los derechos humanos, evitando un uso excesivo o simbólico del derecho penal.

Como señala Zaffaroni (2011), “la política criminal que olvida sus límites corre el riesgo de convertirse en un ejercicio de poder arbitrario, incapaz de brindar verdadera protección a los bienes jurídicos” (p. 83). En consecuencia, el desafío para Ecuador radica en construir una política criminal equilibrada, innovadora y sensible a las particularidades del entorno digital, capaz de garantizar que las víctimas de deepnudes encuentren no solo normas protectoras, sino también mecanismos efectivos de tutela y reparación.

3.8. Conclusiones parciales

El análisis efectuado permite concluir que el sistema penal ecuatoriano carece de herramientas suficientes para sancionar de manera eficaz la creación y difusión de imágenes íntimas falsas generadas mediante inteligencia artificial. Los vacíos legales y las limitaciones prácticas descritas contribuyen a perpetuar un clima de impunidad, en el cual las víctimas ven vulnerados derechos fundamentales como la intimidad, la dignidad, el honor y la integridad psicológica. Esta situación pone de manifiesto la urgencia de reformas legislativas que incorporen definiciones claras, tipifiquen de forma expresa las conductas vinculadas con la inteligencia artificial y establezcan responsabilidades para los distintos actores involucrados, incluidas las plataformas digitales.

Si no se adoptan medidas adecuadas, el derecho penal corre el riesgo de mantenerse rezagado frente a las formas contemporáneas de violencia digital. Por ello, resulta imprescindible que el legislador ecuatoriano, tomando como referencia experiencias comparadas y desarrollos doctrinarios, avance hacia un marco normativo que responda con eficacia a los desafíos de la era

tecnológica, sin perder de vista los principios fundamentales que orientan el ejercicio del ius puniendi.

El análisis efectuado permite concluir que el sistema penal ecuatoriano carece de herramientas suficientes para sancionar de manera eficaz la creación y difusión de imágenes íntimas falsas generadas mediante inteligencia artificial. Los vacíos legales y las limitaciones prácticas descritas contribuyen a perpetuar un clima de impunidad, en el cual las víctimas ven vulnerados derechos fundamentales como la intimidad, la dignidad, el honor y la integridad psicológica. Esta situación pone de manifiesto la urgencia de reformas legislativas que incorporen definiciones claras, tipifiquen de forma expresa las conductas vinculadas con la inteligencia artificial y establezcan responsabilidades para los distintos actores involucrados, incluidas las plataformas digitales.

A la luz de lo expuesto en los apartados anteriores, es posible extraer varias conclusiones parciales:

a) Necesidad de una respuesta normativa específica

El marco penal vigente en Ecuador no contempla de manera expresa la creación ni la difusión de deepnudes, limitándose a proteger la intimidad mediante tipos tradicionales que presuponen la existencia de imágenes auténticas. Esta omisión normativa genera un vacío de punibilidad que favorece la impunidad y desalienta la denuncia. Como indica Bustamante (2022), “la ineficacia de los instrumentos legales frente a los delitos digitales erosiona la confianza ciudadana y debilita el principio de tutela efectiva de derechos” (p. 41).

La experiencia comparada —como las reformas recientes en España (LO 10/2022) o en Reino Unido (Online Safety Act, 2023)— demuestra que la tipificación expresa de la fabricación y divulgación de imágenes íntimas falsas es indispensable para brindar seguridad jurídica y garantizar que las víctimas cuenten con mecanismos efectivos de protección.

b) Incorporación de un enfoque integral en política criminal

La sola incriminación penal resulta insuficiente para enfrentar fenómenos complejos como los deepnudes. Es imprescindible adoptar un enfoque integral de política criminal, que combine medidas legislativas, preventivas, reactivas y restaurativas.

Como señala Zaffaroni (2011), el derecho penal debe ajustarse a las transformaciones sociales “sin sacrificar los principios de proporcionalidad y mínima intervención” (p. 79). Ello implica que el legislador ecuatoriano no solo debe definir claramente las conductas prohibidas, sino también articular políticas públicas orientadas a:

- Fortalecer la alfabetización digital y la cultura del consentimiento.
- Exigir a las plataformas digitales estándares de diligencia para detectar y remover contenido ilícito.
- Crear protocolos especializados para la atención de víctimas, con asistencia psicológica, jurídica y medidas de reparación.
- Impulsar campañas de sensibilización social que desalienten la normalización de estas prácticas.

c) Reforzamiento institucional y capacidades técnicas

La eficacia del sistema penal depende de que las instituciones dispongan de recursos humanos y tecnológicos adecuados. Las unidades de investigación cibernética deben contar con capacitación permanente, herramientas de análisis forense y cooperación fluida con entidades privadas. Sin estos elementos, cualquier reforma normativa quedará en el plano simbólico.

La política criminal debe, por tanto, priorizar el fortalecimiento institucional, fomentando la creación de laboratorios forenses especializados en inteligencia artificial y la formación de operadores judiciales en materia de ciberdelincuencia y derechos digitales.

d) Cooperación internacional y gobernanza digital

Dada la naturaleza transnacional de la difusión de contenidos ilícitos, es indispensable profundizar la cooperación internacional. La adhesión y aplicación efectiva de instrumentos como la Convención de Budapest sobre ciberdelincuencia o la adopción de acuerdos bilaterales permitirán agilizar la obtención de pruebas, el bloqueo de contenido y la persecución de responsables ubicados en otras jurisdicciones.

Asimismo, la política criminal debe dialogar con los estándares de gobernanza digital y derechos humanos, promoviendo que las empresas tecnológicas asuman compromisos vinculantes en materia de prevención y retirada de material que vulnere la intimidad personal.

e) Centralidad de la víctima y reparación integral

El análisis de los efectos de las imágenes íntimas falsas evidencia que los daños trascienden lo material, impactando gravemente la dignidad, la identidad y el bienestar psicológico de quienes resultan afectados. Por ello, cualquier estrategia debe incorporar la centralidad de la víctima, garantizando su acceso a mecanismos de denuncia rápidos, apoyo emocional y medidas de reparación, incluidas la eliminación definitiva del contenido y compensaciones económicas proporcionales al daño sufrido.

Como afirma García-Pablos (2019), “la política criminal contemporánea no puede limitarse al castigo, sino que debe restaurar los derechos vulnerados y prevenir la revictimización” (p. 214).

f) Perspectiva de género y grupos vulnerables

La evidencia muestra que las mujeres, adolescentes y colectivos históricamente discriminados suelen ser los principales blancos de estas prácticas, lo que exige una perspectiva de género y un enfoque diferenciado en las medidas legislativas y políticas públicas. Las normas deben reconocer que los deepnudes constituyen, en muchos casos, una forma de violencia basada en género, articulada con dinámicas de acoso, extorsión o explotación sexual.

Integrar esta mirada permitirá diseñar respuestas que protejan especialmente a quienes enfrentan mayores riesgos de victimización.

3.8.2 Conclusión general de este capítulo

En definitiva, el estudio realizado demuestra que el sistema penal ecuatoriano enfrenta un desafío urgente ante la proliferación de imágenes íntimas falsas generadas mediante inteligencia artificial. Si no se adoptan medidas oportunas, el derecho penal continuará rezagado frente a las nuevas formas de violencia digital, comprometiendo la efectividad de la tutela de derechos fundamentales.

Es indispensable avanzar hacia un marco normativo claro, coherente y respetuoso de los principios del *ius puniendi*, acompañado de políticas públicas, cooperación internacional y fortalecimiento institucional. Solo así será posible ofrecer una respuesta adecuada al fenómeno de los deepnudes, proteger la dignidad de las víctimas y reafirmar el compromiso del Estado con la defensa de los derechos humanos en el entorno tecnológico.

4. CAPÍTULO III: JURISPRUDENCIA Y DOCTRINA PENAL INTERNACIONAL APLICABLES A LOS DEEPFAKES Y LA VIOLENCIA DIGITAL: BASES PARA UNA REFORMA PENAL ECUATORIANA

En este capítulo se aborda de forma integral, como es, el derecho penal frente al impacto de las tecnologías emergentes, en específico de la inteligencia artificial generativa utilizada en la creación de deep fakes y deepnudes. Estos fenómenos han logrado sobrepasar a los esquemas tradicionales del Derecho Penal, poniendo así a prueba la capacidad para proteger bienes jurídicos esenciales como la intimidad, dignidad y la imagen personal. A medida que estas tecnologías permiten falsificar rostros, voces y cuerpos con precisión creciente, los ordenamientos jurídicos se enfrentan al reto de equilibrar la libertad de expresión con la protección de la integridad moral y la privacidad de las personas (Organización de las Naciones Unidas [ONU], 2022).

El objetivo de este capítulo es analizar cómo las diversas jurisdicciones, doctrinas y organismos internacionales han actuado frente a este nuevo desafío, con el fin de construir una base comparativa que sirva de guía para una futura reforma penal en el Ecuador. Busca identificar las experiencias más importantes hablando del contexto normativo como de jurisprudencia que permitieron tipificar o sancionar la manipulación de contenido íntimo artificial, así mismo las lagunas legales que aún prevalecen en el contexto latinoamericano (Consejo de Europa, 2021).

Por otra parte este capítulo, examina el rol de los tratados internacionales como la Convención de Budapest sobre Ciberdelincuencia y la Convención de Belém do Pará, en la

configuración de estándares globales de cooperación judicial y protección a las víctimas de violencia digital. Este análisis demuestra que el fenómeno de los deepnudes no solo crea un problema técnico o aislado, es también una cuestión estructural relacionada con proteger los derechos humanos y la igualdad de género (Organización de los Estados Americanos [OEA], 2020).

La estructura del capítulo sigue un enfoque progresivo: inicia con un marco penal comparado que examina los avances legislativos de España, Reino Unido y los Estados Unidos, sigue con la revisión de los instrumentos penales internacionales; analiza la jurisprudencia internacional que ha trazado los fundamentos en Europa y América Latina; y finalmente presenta una síntesis doctrinal acompañada de propuestas de reforma penal en el Ecuador. Así este capítulo ofrece una visión integral sobre cómo el Derecho Penal puede adaptarse a la era digital sin olvidar los principios fundamentales de legalidad, proporcionalidad y dignidad humana.

4.1. Marco penal comparado

El derecho comparado demuestra tres enfoques importantes ante la creación y difusión de los deepfakes y deepnudes:

el modelo penal clásico, que opta por tipos penales específicos (España);

el modelo regulatorio, que impone deberes de diligencia y responsabilidad a las plataformas digitales (Reino Unido);

y el modelo mixto o estatal, que combina sanciones penales con remedios civiles en el ámbito federado (Estados Unidos).

Cada uno de estos sistemas responde a la necesidad de equilibrar el avance tecnológico con la protección de derechos fundamentales, dejando claro las diferentes conceptualizaciones acerca del derecho penal en la era digital.

- España

Este modelo se caracteriza por una respuesta penal directa. La Ley Orgánica 10/2022 y el art. 197.7 CP sanciona la difusión no consentida de imágenes íntimas, mientras que el art. 172 ter CP tipifica el acoso digital. Aunque el Código Penal no contempla expresamente las imágenes sintéticas, la doctrina propone aplicar estas normas por analogía, atendiendo al daño moral y social causado.(Referencia: Código Penal Español y LO 10/2022.)

- Reino Unido

El Reino Unido adopta un enfoque preventivo y regulatorio, centrado en la responsabilidad de las plataformas digitales. La Online Safety Act (2023) impone obligaciones de diligencia para prevenir y eliminar contenidos dañinos, complementando delitos preexistentes como la divulgación de imágenes privadas (Criminal Justice and Courts Act 2015). Este modelo prioriza la prevención y la corresponsabilidad tecnológica.(Referencia: Online Safety Act 2023 y Criminal Justice and Courts Act 2015.)

- Estados Unidos

En Estados Unidos predomina un enfoque descentralizado y flexible. Algunos estados, como Virginia, California y Texas, penalizan la creación y difusión de imágenes sexuales falsas y permiten acciones civiles. Si bien no existe una ley federal específica, la tendencia general es

reconocer la equivalencia del daño moral y psicológico causado por los deepnudes, integrando medidas penales y civiles.(De Hert & Papakonstantinou, 2018.)

4.1.1 Conclusión comparativa:

En el modelo español se destaca una rigidez penal, el británico con un enfoque preventivo y el norteamericano por su adaptabilidad normativa. Aunque tengan sus diferencias, los tres modelos coinciden en que se debe armonizar la necesidad de la legislación penal frente a los nuevos entornos digitales. Esta comparación permite ver con claridad la respuesta que efectúa cada modelo para integrar mecanismo de sanción, prevención y reparación, demostrando así un camino a seguir para la edificación del marco jurídico Ecuatoriano al referirse en casos de deepnudes y deep fakes. Todos los modelos en conjunto demuestran que la regulación eficaz es la que contiene una combinación de sanciones penales, mecanismo de reparación y responsabilidad tecnológica para garantizar la protección de la intimidad y la dignidad en el mundo tecnológico.

4.2. Instrumentos penales internacionales relevantes

El Estado ecuatoriano ratificó la Convención de Belém do Pará en 1995, asumiendo el compromiso de implementar políticas públicas orientadas a eliminar toda forma de violencia contra la mujer, incluyendo aquella que se manifiesta en espacios tecnológicos y digitales. Esta adhesión marcó un precedente importante, pues reconoció que las agresiones no siempre ocurren

en el plano físico, sino también en escenarios donde la exposición y la manipulación de la imagen femenina se vuelven un instrumento de humillación.

Aunque Ecuador no ha ratificado formalmente la Convención de Budapest sobre ciberdelincuencia, ha ido incorporando recomendaciones técnicas y mecanismos de cooperación judicial en su normativa penal y particularmente dentro del COIP y en políticas públicas de ciberseguridad y protección de datos. Esta referencia práctica demuestra que, aunque exista un desfase formal, el país ha reconocido indirectamente la importancia de estos marcos internacionales.

Por eso, integrar los dos instrumentos en la legislación penal ecuatoriana no sería solo un acto simbólico, sino una estrategia necesaria para fortalecer la persecución de los delitos cibernéticos, en especial aquellos que se derivan del uso indebido de la inteligencia artificial, y para garantizar el pleno respeto de los derechos fundamentales.

Los instrumentos penales internacionales representan el punto de partida para que los Estados puedan cooperar bajo un mismo estándar jurídico frente a la ciberdelincuencia y la violencia digital. En el caso de los deepnudes, destacan dos convenciones clave: la Convención de Budapest sobre Ciberdelincuencia (2001) y la Convención de Belém do Pará (1994).

La primera, creada por el Consejo de Europa, sentó las bases de una estructura legal común para la investigación, persecución y sanción de delitos cometidos mediante tecnologías de la información. Aunque no hace referencia directa a los deep fakes o deep nudes, sus disposiciones sobre acceso ilícito, manipulación de datos y contenido ilegal sirven como marco conceptual para abordar las nuevas modalidades delictivas que emergen del entorno digital (Consejo de Europa, 2001).

Gracias a esta convención, muchos países han podido armonizar sus sistemas penales, fortaleciendo la cooperación judicial transnacional y el intercambio de pruebas digitales. De hecho, su espíritu busca promover una colaboración constante entre Estados, generando mecanismos ágiles para rastrear delitos que, por su naturaleza digital, trascienden fronteras.

En el contexto ecuatoriano, aplicar los principios de la Convención de Budapest sería esencial para mejorar la persecución penal de conductas vinculadas al uso indebido de la inteligencia artificial. Esto permitiría, por ejemplo, una mejor preservación de evidencias digitales, la cooperación efectiva entre la Fiscalía, la Policía Judicial y los entes tecnológicos, y el establecimiento de protocolos uniformes para la identificación y sanción de quienes difundan contenido íntimo falso. En la práctica, este tratado podría convertirse en una herramienta de apoyo directo al marco penal ecuatoriano, ayudando a superar la actual dispersión normativa y dotando al país de una estructura legal más sólida frente a los delitos digitales.

Por otra parte, la Convención de Belém do Pará (1994), impulsada por la Organización de los Estados Americanos (OEA), marcó un punto de inflexión en el reconocimiento de la violencia contra las mujeres como una violación estructural de derechos humanos. Este instrumento estableció que la violencia de género también puede manifestarse en entornos digitales, exigiendo a los Estados adoptar leyes y políticas públicas que protejan la dignidad, integridad y autonomía de las mujeres frente a las nuevas formas de agresión tecnológica (Organización de los Estados Americanos [OEA], 1994).

Desde esta perspectiva, los deepnudes constituyen una forma moderna de violencia simbólica y psicológica, donde las mujeres son las principales afectadas. La manipulación de imágenes mediante inteligencia artificial refuerza estereotipos de dominación y control sobre el cuerpo femenino, reproduciendo desigualdades que se trasladan del mundo físico al digital. Por ello, la Convención de Belém do Pará insta a los Estados, incluido Ecuador, a tipificar penalmente estas conductas, desarrollar campañas de prevención y garantizar mecanismos de reparación integral a las víctimas, tanto en el ámbito judicial como en el psicológico y social (OEA, 1994).

El impacto de estas disposiciones trasciende lo simbólico, pues integran una visión humanista y tecnológica del Derecho Penal, donde la dignidad y la igualdad se entienden como ejes de protección frente a las nuevas modalidades de violencia. Así, los deepnudes dejan de ser solo un problema técnico o digital para convertirse en una cuestión estructural de derechos humanos y género.

En conjunto, la Convención de Budapest y la Convención de Belém do Pará ofrecen una visión complementaria en la lucha contra la violencia digital. Mientras la primera aporta el componente técnico y jurídico de cooperación internacional y persecución penal, la segunda introduce la perspectiva de género y derechos humanos, indispensable para entender las consecuencias sociales y morales de estas agresiones.

Para el caso ecuatoriano, unir ambos marcos normativos sería clave para avanzar hacia una legislación penal moderna, equilibrada y coherente con los retos de la inteligencia artificial.

Solo mediante la articulación de instrumentos internacionales y políticas nacionales se podrá garantizar una protección real de la intimidad, la dignidad y la seguridad digital, consolidando un sistema de justicia penal que responda de manera efectiva a los desafíos del siglo XXI (Consejo de Europa, 2001; OEA, 1994).

4.3. Jurisprudencia penal internacional

La jurisprudencia internacional ha ido ampliando su mirada frente a los delitos cometidos en entornos digitales, especialmente en aquellos que implican la difusión no consentida de contenido íntimo o la manipulación digital de imágenes. En este campo, tanto Europa como América Latina han reconocido que dichas conductas vulneran derechos fundamentales como la intimidad, la dignidad y la propia imagen, generando criterios que sirven de guía para enfrentar fenómenos recientes como los deepnudes y deep fakes. Aunque las normas no mencionen expresamente estos contenidos, los tribunales han sabido adaptar su razonamiento al contexto tecnológico, priorizando la exposición no consentida de la víctima sobre la autenticidad del material. En otras palabras, el daño jurídico no radica en si la imagen es verdadera o no, sino en el hecho de haber sido divulgada sin autorización y con capacidad de afectar la esfera privada de la persona (Tribunal Supremo de España, 2022).

- Europa

En España, el Tribunal Supremo, mediante la Sentencia 70/2022, reafirmó que la difusión de imágenes íntimas sin consentimiento constituye una forma de violencia sexual, destacando su impacto directo sobre la dignidad y la privacidad. Aunque el caso trataba sobre fotografías

reales, la fundamentación del tribunal puede aplicarse con facilidad a los deepnudes, pues el perjuicio se origina en la exposición no consentida y no en la autenticidad del contenido. El razonamiento del Supremo deja ver que el acto de publicar o compartir material sexual de otra persona y aun cuando esa persona lo haya generado originalmente, configura una vulneración grave de la intimidad y puede ser tratado como una forma moderna de violencia sexual (Tribunal Supremo de España, 2022).

En términos prácticos, la sentencia española introduce un mensaje claro: el consentimiento digital no se presume, y la voluntad de la víctima es el eje sobre el cual debe girar toda valoración penal en materia de imágenes íntimas.

Por su parte, en Alemania, el Tribunal Constitucional Federal en su decisión BVerfGE 101, 361 (2000) desarrolló una interpretación amplia del derecho general de la personalidad, reconociendo que este protege la autodeterminación de la imagen personal y la libertad de decidir cómo se representa o difunde la identidad propia. Este razonamiento ha sido clave para justificar sanciones a quienes manipulan o distorsionan fotografías de terceros, incluso si lo hacen mediante herramientas digitales avanzadas. En esencia, el tribunal señaló que toda manipulación visual que modifique la identidad de una persona sin su consentimiento afecta su esfera privada y puede dar lugar a responsabilidad civil o penal (Tribunal Constitucional Federal de Alemania, 2000).

Este criterio resulta especialmente relevante hoy, porque permite extender la protección del derecho a la imagen hacia los casos de deep fakes y deepnudes, donde el daño se produce por la falsificación o la distorsión del rostro o cuerpo de la víctima, aunque no exista una imagen original previa.

En conjunto, las decisiones europeas muestran una tendencia a reinterpretar la intimidad y la imagen personal desde una perspectiva dinámica. Los tribunales no se limitan al texto literal de la ley, sino que adaptan sus fallos a las realidades digitales, buscando que los derechos humanos mantengan su vigencia en entornos virtuales. De esta forma, el derecho penal europeo se ha transformado en un sistema capaz de responder a los riesgos tecnológicos sin perder su esencia garantista centrada en la dignidad humana.

- América Latina

En Argentina, la Cámara Nacional Civil, al resolver el Expediente 23645/2021, determinó que la divulgación no consentida de imágenes personales vulnera directamente el derecho a la intimidad y produce un daño moral que debe ser reparado mediante una compensación económica. Aunque el caso se refería a fotografías auténticas, el tribunal fue enfático en señalar que el daño radica en la exposición pública de la vida privada, no en la veracidad del material difundido. Bajo este criterio, el razonamiento puede aplicarse también a los deepnudes, pues el sufrimiento psicológico y reputacional que generan es equiparable al que produce la publicación de imágenes reales. Así, el tribunal argentino fortaleció la idea de que el derecho a la intimidad debe protegerse más allá de la autenticidad del contenido y frente a cualquier tipo de manipulación digital (Cámara Nacional Civil de Argentina, 2021).

En Chile, la Corte Suprema, mediante la Sentencia Rol N.º 126.254-2021, reconoció que la difusión de imágenes íntimas a través de medios digitales sin consentimiento constituye una forma de violencia de género, exigiendo una respuesta jurídica efectiva. En su fallo, el tribunal

subrayó que las tecnologías han ampliado los espacios de vulneración hacia las mujeres y que, por ello, las leyes deben evolucionar para responder a las agresiones mediadas por internet. Además, instó al poder legislativo a actualizar la normativa penal, incorporando una mirada de género y mecanismos de prevención. Con esta decisión, la Corte dejó sentado que la violencia digital no es solo un fenómeno social, sino una categoría jurídica que debe abordarse desde la perspectiva de los derechos humanos y la igualdad (Corte Suprema de Chile, 2021).

Las decisiones judiciales en América Latina comparten una línea común: ponen el foco en la reparación del daño psicológico y moral, reconociendo que las víctimas de violencia digital enfrentan impactos prolongados en su bienestar y reputación. Además, refuerzan la necesidad de incorporar una perspectiva de género en la interpretación judicial, considerando que la mayoría de las afectadas por la difusión de contenido íntimo —real o manipulado— son mujeres o adolescentes. En este sentido, los tribunales no solo buscan sancionar, sino también prevenir y educar, impulsando la creación de políticas públicas que promuevan la alfabetización digital y el respeto a la autonomía corporal en entornos virtuales.

- Contraste y síntesis comparada

Al comparar ambos contextos, se puede observar que Europa ha optado por una expansión progresiva del derecho a la intimidad y a la autodeterminación de la imagen, usando estos principios como base para sancionar las nuevas formas de abuso digital. En cambio, América Latina ha privilegiado un enfoque reparatorio y con perspectiva de género, centrado en la compensación del daño moral y psicológico causado a las víctimas.

A pesar de estas diferencias, ambos sistemas convergen en un punto esencial: el daño causado por los deep nudes y deep fakes no depende de su autenticidad, sino de la afectación emocional, social y moral que provocan en la víctima. Tanto las cortes europeas como las latinoamericanas reconocen que estas prácticas vulneran la dignidad humana, y que el Derecho Penal tiene el deber de responder ante la reproducción digital del abuso y la humillación.

Estas tendencias jurisprudenciales ofrecen a Ecuador un referente sólido para desarrollar una interpretación judicial moderna que combine la técnica jurídica europea con la sensibilidad social latinoamericana. Integrar ambos enfoques permitiría construir un marco penal más humano, garantista y adaptado a la realidad tecnológica actual, donde la protección de la intimidad, la imagen y la dignidad debe mantenerse firme, incluso frente a la inteligencia artificial y sus riesgos emergentes (Tribunal Supremo de España, 2022; Tribunal Constitucional Federal de Alemania, 2000; Cámara Nacional Civil de Argentina, 2021; Corte Suprema de Chile, 2021).

4.4. Doctrina penal internacional

La doctrina penal internacional ha mostrado un avance significativo en la comprensión de cómo la inteligencia artificial y la manipulación digital transforman el alcance de la tutela penal contemporánea. En la actualidad, los deep nudes y deep fakes han generado un debate que trasciende el ámbito técnico y se sitúa en el corazón del Derecho Penal, al desafiar los límites tradicionales de la tipicidad, la imputación y la protección de bienes jurídicos personales.

Diversos autores, de entre ellos Simó Soler (2023), Varela (2021), Citron (2019) y De Hert & Papakonstantinou (2018) ofrecen perspectivas complementarias que ayudan a entender la

necesidad urgente de tipificar y sancionar estas conductas como nuevas formas de atentado contra la intimidad, la dignidad y la identidad personal. En conjunto, estas visiones doctrinales reflejan una idea común: el Derecho Penal debe evolucionar hacia una adaptación digital garantista, que preserve su esencia protectora frente a los riesgos tecnológicos sin renunciar a los principios de proporcionalidad y legalidad.

a) Enfoque de violencia de género: Simó Soler y Citron

Desde una perspectiva de género, Simó Soler (2023) sostiene que los deepfakes sexuales no deben entenderse como simples montajes digitales, sino como manifestaciones contemporáneas de violencia sexual. Para la autora, estas representaciones reproducen estructuras de poder históricas que cosifican a las mujeres, trasladando al entorno virtual la misma lógica de dominación y sometimiento que caracteriza a la violencia patriarcal.

Simó Soler considera que el impacto psicológico y social que producen los deepnudes exige una respuesta penal autónoma, con tipificaciones específicas que reconozcan la gravedad moral y simbólica del daño, así como agravantes para los casos en que exista difusión pública masiva. Su planteamiento propone incorporar estas conductas al catálogo de delitos sexuales, reforzando la idea de que el cuerpo y la imagen no son objetos de manipulación, sino expresiones de la autonomía personal (Simó Soler, 2023).

De manera complementaria, Danielle Citron (2019) aborda el fenómeno desde el prisma de la violencia digital y los crímenes de odio, señalando que los deepfakes y deepnudes afectan principalmente a mujeres y minorías vulnerables. Según la autora, estas prácticas amplían el

alcance del acoso, la humillación y la discriminación en los espacios digitales, generando consecuencias reales en la vida cotidiana de las víctimas, como la exclusión social, la autocensura o la pérdida de credibilidad pública.

Citron propone un modelo híbrido de respuesta jurídica, que combine sanciones penales con mecanismos civiles de reparación y con obligaciones directas de responsabilidad para las plataformas tecnológicas. En su análisis, este tipo de violencia no solo vulnera derechos individuales, sino que erosiona valores democráticos esenciales, como la igualdad y la libertad de expresión, al convertir los entornos digitales en espacios inseguros para la participación de las mujeres (Citron, 2019).

Ambas autoras coinciden en que la violencia basada en la manipulación digital del cuerpo femenino representa una nueva frontera del Derecho Penal, en la que los Estados deben actuar con diligencia para evitar que el espacio virtual se convierta en un escenario de impunidad estructural.

b) Protección de la imagen como bien jurídico autónomo: Varela

Por su parte, Carlos Varela (2021) plantea que el derecho a la imagen debe reconocerse como un bien jurídico autónomo, independiente de la intimidad o el honor. En su análisis, las tecnologías de inteligencia artificial introducen un riesgo inédito para este derecho, al posibilitar la creación de representaciones falsas que distorsionan la identidad y la reputación de las personas.

Para Varela, la imagen no es solo un reflejo físico, sino una manifestación simbólica de la identidad personal, que cumple una función esencial en la configuración del individuo como sujeto libre y socialmente reconocido. Por ello, cualquier manipulación o reproducción sin consentimiento constituye una forma de violación de la autodeterminación.

El autor advierte que los deep nudes y deep fakes amenazan directamente ese principio, al generar una representación ficticia del cuerpo o rostro de la víctima que puede propagarse sin control, afectando su vida privada, laboral y emocional. Propone, por tanto, actualizar el catálogo de bienes jurídicos protegidos e incorporar la imagen personal como un valor penalmente tutelado por sí mismo, especialmente en la era digital, donde la identidad se proyecta constantemente en entornos virtuales (Varela, 2021).

Este enfoque refuerza la necesidad de un Derecho Penal más sensible al daño simbólico, capaz de reconocer que la manipulación digital no solo afecta el honor o la intimidad, sino que puede desintegrar la percepción misma de quién es la persona ante la sociedad.

c) Desafíos regulatorios y tecnológicos: De Hert & Papakonstantinou

En un plano más normativo y técnico, De Hert y Papakonstantinou (2018) analizan los desafíos regulatorios que plantea la inteligencia artificial para los sistemas penales contemporáneos. Según los autores, la creación y difusión de deep fakes exige marcos jurídicos más flexibles, capaces de equilibrar la libertad de expresión con la protección efectiva de la privacidad y la dignidad humana.

Argumentan que las normas tradicionales resultan insuficientes para abordar delitos tecnológicos donde el daño no proviene de un contacto físico, sino de la alteración o manipulación de datos digitales que afectan derechos fundamentales.

Los autores proponen avanzar hacia un modelo de regulación tecnológicamente consciente, sustentado en tres pilares: la sanción penal proporcional, la transparencia algorítmica y la cooperación internacional. Este enfoque permitiría una respuesta preventiva, orientada a mitigar el daño antes de que se produzca, y no solo a castigar una vez que la lesión ya sea irreversible (De Hert & Papakonstantinou, 2018).

Su aporte complementa la mirada penal con una dimensión regulatoria, recordando que el Derecho Penal no puede operar aisladamente, sino dentro de un ecosistema jurídico donde la protección de derechos se articule con políticas tecnológicas, estándares de responsabilidad y ética digital.

4.4.2 Conclusión parcial

La doctrina penal internacional coincide en que la creación y difusión de imágenes íntimas sintéticas constituye una amenaza real y creciente para los bienes jurídicos tradicionales. Los enfoques de los autores analizados permiten identificar tres dimensiones fundamentales:

La violencia de género como eje de interpretación jurídica y social, que visibiliza las asimetrías estructurales en la victimización digital.

La imagen personal como un bien jurídico autónomo, que debe gozar de protección penal específica.

La necesidad de un marco penal flexible y tecnológico, que dialogue con la inteligencia artificial y con los mecanismos de responsabilidad digital.

En definitiva, todos los autores confluyen en una misma conclusión: el Derecho Penal del siglo XXI debe ser proactivo, anticipándose a las nuevas formas de vulneración que surgen de la tecnología.

En el contexto ecuatoriano, asumir estas reflexiones significa dar un paso hacia una reforma penal moderna y garantista, capaz de sancionar con precisión, reparar con eficacia y prevenir con humanidad. Solo así se consolidará una tutela penal verdaderamente integral de la dignidad humana frente a la violencia digital (Simó Soler, 2023; Citron, 2019; Varela, 2021; De Hert & Papakonstantinou, 2018).

4.5. Propuestas de reforma para Ecuador

El marco jurídico ecuatoriano vigente protege bienes esenciales como la intimidad, la dignidad y la libertad personal, pilares fundamentales del orden constitucional. Sin embargo, no contempla disposiciones específicas que aborden la creación o difusión de imágenes sintéticas generadas mediante inteligencia artificial, dejando un vacío frente a conductas nuevas como los deepnudes o deep fakes de carácter sexual.

Esta ausencia normativa genera inseguridad jurídica tanto para las víctimas como para las autoridades judiciales, ya que estas conductas vulneran derechos fundamentales sin poder ser encuadradas con precisión dentro de los tipos penales existentes.

Las propuestas que se desarrollan a continuación parten de los principios constitucionales de dignidad humana, intimidad y libertad personal (Constitución de la República del Ecuador, 2008), y de los instrumentos internacionales de protección como la Convención de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001) y la Convención de Belém do Pará (Organización de los Estados Americanos [OEA], 1994).

El objetivo general es armonizar el Derecho Penal ecuatoriano con los nuevos desafíos tecnológicos, fortaleciendo la tutela de los derechos fundamentales frente a las formas emergentes de violencia digital y manipulación de contenido íntimo.

4.5.1 Reforma penal necesaria

El análisis comparado, doctrinal y jurisprudencial desarrollado en los apartados anteriores demuestra con claridad que Ecuador necesita una reforma penal concreta y específica para regular la creación, alteración y difusión de deepnudes y deep fakes sexuales. Esta actualización normativa debe inspirarse en los principios de legalidad, proporcionalidad y mínima intervención penal, garantizando que la sanción sea equilibrada y no abusiva, pero sí efectiva y reparadora.

No se trata únicamente de criminalizar la tecnología, sino de adaptar el Derecho Penal a una nueva realidad social en la que las imágenes sintéticas pueden causar daños tan graves como

los materiales reales. Por ello, la tipificación debe reconocer que el perjuicio radica en la afectación moral, psicológica y social de la víctima, y no en la autenticidad del contenido manipulado.

4.5.2 Tipificación expresa de los deepnudes

Una de las propuestas centrales consiste en incorporar un tipo penal autónomo en el Código Orgánico Integral Penal (COIP) que sancione la creación, modificación o difusión de imágenes, audios o videos de carácter sexual falsos o simulados elaborados mediante inteligencia artificial sin el consentimiento de la persona afectada.

La norma debe reflejar el daño que estas prácticas provocan en la reputación, la dignidad y la intimidad de las víctimas, y establecer una sanción proporcional a la gravedad del acto.

Tomando como referencia los modelos legislativos de España y Estados Unidos, una posible redacción sería:

“Quien, mediante el uso de inteligencia artificial u otra tecnología digital, cree, modifique o difunda imágenes, audios o videos de contenido sexual falso o simulado de una persona sin su consentimiento, será sancionado con pena privativa de libertad de tres a cinco años.”

(Propuesta doctrinal basada en modelos legislativos de EE. UU. y España, adaptada al contexto ecuatoriano).

Con esta disposición se cerraría uno de los vacíos normativos más críticos del COIP, permitiendo al sistema judicial sancionar conductas que hasta hoy se ubican en un limbo legal, pese a vulnerar bienes jurídicos reconocidos. Así, se garantizaría una protección más coherente de la dignidad humana y la integridad psicológica en entornos digitales.

4.5.3 Agravantes por uso de inteligencia artificial

El uso de tecnologías de inteligencia artificial como herramienta para crear o viralizar contenido sexual manipulado debe considerarse una circunstancia agravante, pues la automatización del daño y la velocidad de propagación amplifican el perjuicio a la víctima.

Esta agravante sería aplicable cuando el hecho incremente la exposición pública, intensifique el daño moral o psicológico, o se ejecute con fines de difamación, extorsión o humillación.

Una posible redacción, inspirada en la legislación comparada, podría ser:

“Se considerará agravante cuando el hecho se cometa utilizando tecnologías de inteligencia artificial o algoritmos de difusión masiva que incrementen el perjuicio ocasionado a la víctima.”

(Propuesta basada en legislación española y estadounidense sobre responsabilidad tecnológica).

Esta medida reconoce que la tecnología no solo facilita la comisión del delito, sino que también multiplica el impacto social y mediático del mismo, justificando una respuesta penal más severa en casos de mayor alcance.

4.5.4 Responsabilidad de plataformas digitales

Las plataformas digitales desempeñan un rol determinante en la difusión de contenido íntimo manipulado, ya que permiten su circulación viral sin filtros o mecanismos de denuncia eficaces. En ese contexto, se propone que Ecuador adopte un modelo de responsabilidad compartida, similar al establecido en la Online Safety Act del Reino Unido (2023), donde los proveedores de servicios tecnológicos están obligados a prevenir, detectar y retirar de manera oportuna los contenidos ilícitos.

Una redacción sugerida podría ser:

“Los proveedores de servicios digitales deberán adoptar medidas de diligencia y cooperación para prevenir y eliminar sin dilación los contenidos ilícitos generados mediante inteligencia artificial que vulneren derechos a la intimidad o a la dignidad humana.”

(Cita parafraseada, basada en la Online Safety Act del Reino Unido, 2023).

Asimismo, se debería establecer la obligación de implementar protocolos de denuncia accesibles, tiempos máximos de respuesta, mecanismos de trazabilidad y sanciones administrativas en caso de omisión. De este modo, el Derecho Penal se complementará con una

ética digital preventiva, promoviendo una cultura de responsabilidad tecnológica compartida entre Estado, plataformas y usuarios.

4.5.5 Conclusión parcial

La tipificación penal de los deepnudes en Ecuador permitiría cerrar uno de los vacíos más relevantes del Derecho Penal moderno, garantizando seguridad jurídica y protección efectiva a las víctimas frente a las nuevas formas de violencia digital.

Incorporar agravantes por el uso de inteligencia artificial y deberes de diligencia para las plataformas consolidaba una respuesta integral, en la que la sanción penal se complementa con la prevención tecnológica y la cooperación institucional.

De esta manera, el Derecho Penal ecuatoriano se alineará con los estándares internacionales de protección y con los principios constitucionales de dignidad, intimidad y libertad personal, reafirmando su papel como un instrumento de justicia social frente a los abusos tecnológicos que amenazan los derechos fundamentales en la era digital (Constitución de la República del Ecuador, 2008; Consejo de Europa, 2001; OEA, 1994).

4.6. Conclusiones parciales

El análisis exhaustivo desarrollado en este capítulo permite concluir que Ecuador enfrenta un vacío legal profundo y preocupante frente a la creación y difusión de imágenes íntimas sintéticas generadas mediante inteligencia artificial. La revisión comparada,

jurisprudencial y doctrinal demuestra que la protección penal tradicional —centrada en la existencia de una imagen real y en la tutela de la intimidad física— resulta insuficiente para responder a las nuevas formas de violencia digital que surgen en los entornos tecnológicos contemporáneos.

Este vacío normativo no sólo deja sin amparo jurídico efectivo a las víctimas, sino que también limita la capacidad del Estado para prevenir, investigar y sancionar de manera oportuna los delitos vinculados con los deepnudes y deepfakes sexuales. En otras palabras, el Derecho Penal ecuatoriano aún no ha alcanzado el ritmo acelerado de la tecnología, lo que genera una sensación de impunidad y desprotección en quienes sufren estas agresiones digitales.

La experiencia internacional ofrece lecciones valiosas. Los ordenamientos jurídicos más desarrollados, como los de Europa y América del Norte, han adoptado modelos mixtos que integran la sanción penal, la responsabilidad compartida de las plataformas digitales y mecanismos de reparación civil para las víctimas. Estos esquemas buscan un equilibrio razonable entre la libertad de expresión y la innovación tecnológica, por un lado, y la protección de bienes jurídicos fundamentales como la intimidad, la dignidad y la imagen personal por otro.

La clave radica en entender que la tecnología, si no se regula bajo un enfoque ético y jurídico sólido, puede convertirse fácilmente en una herramienta de vulneración masiva de derechos humanos, replicando en el entorno digital las mismas desigualdades estructurales existentes en la realidad (De Hert & Papakonstantinou, 2018; Citron, 2019).

Bajo este panorama, Ecuador puede apoyarse en las experiencias comparadas de España, Reino Unido y Estados Unidos para construir un marco penal moderno y coherente con su

realidad constitucional. El modelo español ofrece una estructura penal precisa que aborda la violencia sexual digital; el británico, a través de la Online Safety Act, impone deberes de diligencia y control a las plataformas; y el estadounidense combina vías penales y civiles para garantizar una respuesta integral frente a la manipulación digital.

Estas referencias no implican una copia literal, sino una adaptación inteligente al contexto ecuatoriano, tomando en cuenta la estructura institucional, los principios garantistas y las condiciones socio tecnológicas del país.

Asimismo, los instrumentos internacionales proporcionan bases normativas que deben guiar cualquier reforma. La Convención de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001) promueve la cooperación judicial y la tipificación de delitos informáticos transnacionales, mientras que la Convención de Belém do Pará (OEA, 1994) impone a los Estados la obligación de prevenir, sancionar y erradicar toda forma de violencia de género, incluyendo aquella que ocurre en espacios digitales.

Ambas constituyen pilares indispensables para diseñar un marco penal integral, donde la inteligencia artificial y las nuevas tecnologías se entiendan no solo como herramientas de riesgo, sino también como objetos de regulación responsable.

Como destacan De Hert y Papakonstantinou (2018), la actualización normativa es indispensable para salvaguardar los derechos humanos en entornos digitales, donde las tecnologías emergentes pueden transformarse en mecanismos de agresión masiva si no existen controles adecuados. En la misma línea, Citron (2019) advierte que el daño ocasionado por los deepfakes y deepnudes no depende de la autenticidad del material, sino del impacto psicológico,

moral y reputacional que genera su difusión, lo que obliga a los Estados a repensar el alcance de la tutela penal tradicional.

En consecuencia, el sistema penal ecuatoriano debe reconocer de forma expresa que las imágenes sintéticas y la manipulación digital representan una amenaza real a la integridad, la privacidad y la dignidad de las personas. Incorporar estas conductas dentro del Código Orgánico Integral Penal (COIP) permitiría cerrar vacíos normativos que hoy obstaculizan la protección de los derechos fundamentales.

Más allá de sancionar, la reforma debería consolidar una política criminal preventiva y moderna, que combine la penalización con la educación digital, la reparación simbólica y la responsabilidad tecnológica de los intermediarios.

Finalmente, una reforma penal con visión digital y enfoque de derechos humanos colocaría a Ecuador a la altura de los estándares internacionales, cumpliendo el mandato constitucional de garantizar la dignidad humana como principio rector del Estado (Constitución de la República del Ecuador, 2008) y reafirmando que el Derecho Penal, en la era de la inteligencia artificial, debe ser no solo un instrumento de castigo, sino también de protección, prevención y justicia social.

5. Conclusiones

La investigación desarrollada permite evidenciar que el ordenamiento jurídico penal ecuatoriano se encuentra en un punto de inflexión decisivo frente a los nuevos desafíos que plantea la inteligencia artificial (IA) en la protección de los derechos fundamentales.

La creación y difusión de imágenes íntimas sintéticas conocidas como deepnudes representan una forma reciente de violencia digital que atenta directamente contra bienes jurídicos esenciales como la intimidad, la imagen y la dignidad humana, pero que, hasta la fecha, carecen de una respuesta normativa clara y suficiente dentro del Código Orgánico Integral Penal (COIP).

Este vacío normativo refleja una desconexión preocupante entre el avance tecnológico y la capacidad legislativa del Estado, lo cual genera impunidad estructural y deja a las víctimas en una posición de vulnerabilidad constante.

5.1. Insuficiencia del marco penal ecuatoriano

El estudio determinó que el artículo 178 del COIP, diseñado originalmente para sancionar la difusión no consentida de imágenes reales, resulta obsoleto e insuficiente para abarcar las nuevas conductas derivadas del uso de IA generativa.

La falta de una definición legal precisa de “imagen sintética” o “imagen íntima falsa” impide adecuar estas conductas al tipo penal existente, generando vacíos sustantivos y dejando sin sanción a quienes crean o difunden este tipo de material manipulado.

En consecuencia, las víctimas se enfrentan a un panorama de impunidad digital, donde los operadores judiciales, al intentar aplicar la norma por analogía, podrían vulnerar el principio de legalidad penal consagrado en el artículo 76 de la Constitución de la República del Ecuador (2008).

Esta deficiencia demuestra la urgencia de una reforma integral del COIP, que incorpore de forma expresa los supuestos de creación, alteración o difusión digital de imágenes íntimas, diferenciándolos de los delitos tradicionales contra la intimidad, e incluyendo agravantes específicas en casos de difusión masiva, automatizada o con fines de humillación pública.

5.2. Vulneración de derechos fundamentales

Las imágenes sintéticas creadas mediante IA lesionan simultáneamente tres bienes jurídicos fundamentales:

- La intimidad, al irrumpir en la esfera privada sin consentimiento.
- La imagen, al falsificar la representación corporal y simbólica del individuo.
- Y la dignidad humana, al cosificar a la persona y exponerla al escarnio social.

La jurisprudencia constitucional ecuatoriana, particularmente las sentencias No. 003-18-SIN-CC y No. 916-22-JP/24 de la Corte Constitucional del Ecuador, refuerza la idea de que la dignidad constituye el presupuesto indispensable para el ejercicio de todos los demás derechos.

Sin embargo, la falta de adaptación normativa entre la Constitución y el COIP provoca una protección formal, pero sin eficacia material, que no logra amparar adecuadamente a las víctimas de violencia digital.

El resultado es una brecha evidente entre el discurso constitucional garantista y la realidad procesal penal ecuatoriana.

5.3. Dificultades probatorias y tecnológicas

La imputación penal por deepnudes enfrenta retos técnicos y procesales complejos. Probar la autenticidad digital, la intencionalidad dolosa o la autoría real de la imagen requiere de peritajes informáticos avanzados y peritos especializados que el Ecuador aún no posee en número ni capacidad suficiente.

Además, la naturaleza transnacional de los delitos digitales, por la ubicación de servidores en el extranjero o la difusión viral, dificulta la aplicación territorial de la ley y la ejecución de órdenes judiciales.

Frente a esto, se hace indispensable fortalecer la infraestructura forense digital del Estado, crear protocolos de cadena de custodia electrónica, y fomentar acuerdos internacionales de cooperación judicial.

Solo así el sistema penal podrá garantizar investigaciones eficaces y el respeto al debido proceso digital en delitos cometidos mediante IA.

5.4. Tendencias comparadas y estándares internacionales

El análisis comparado evidencia que España, Reino Unido y Estados Unidos han adoptado modelos diferenciados que convergen en una misma dirección: reconocer la manipulación digital del contenido íntimo como una forma grave de agresión contra la autonomía y dignidad personal.

- España, con la Ley Orgánica 10/2022, refuerza la respuesta penal frente a la violencia sexual digital.
- Reino Unido, a través de la Online Safety Act (2023), impone obligaciones activas de control y diligencia a las plataformas digitales.
- Estados Unidos, mediante legislaciones estatales diversas, combina sanciones penales y civiles frente a la difusión de contenido íntimo falso.

En el plano internacional, la Convención de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001) proporciona un marco técnico para la persecución de delitos informáticos, mientras que la Convención de Belém do Pará (OEA, 1994) introduce un enfoque de género y derechos humanos, clave para tratar los deepnudes como formas contemporáneas de violencia sexual y simbólica.

5.5. Doctrina penal y necesidad de adaptación digital

La doctrina penal moderna —representada por Simó Soler (2023), Citron (2019), Varela (2021) y De Hert & Papakonstantinou (2018)— coincide en que el Derecho Penal debe reconfigurar sus categorías tradicionales frente a la era digital.

La protección de bienes jurídicos exige una tutela penal tecnológica garantista, donde se equilibre la expansión del *ius puniendi* con los principios de proporcionalidad, legalidad y mínima intervención.

Para estos autores, la manipulación del cuerpo humano mediante IA no solo lesiona la privacidad, sino que constituye una forma de violencia simbólica y sexual, que requiere un tratamiento autónomo.

Asimismo, se plantea la necesidad de actualizar las nociones de autoría, participación y responsabilidad penal, incorporando la posible intervención de algoritmos, redes neuronales o sistemas automatizados como instrumentos comisivos de delitos.

De esta manera, el Derecho Penal no se convierte en un obstáculo al progreso tecnológico, sino en un instrumento de equilibrio y protección frente a sus posibles abusos.

5.6. Perspectiva de género y reparación integral

La evidencia obtenida confirma que la violencia digital basada en imágenes íntimas falsas afecta principalmente a mujeres y adolescentes, reproduciendo estructuras históricas de desigualdad y dominación patriarcal.

Desde un enfoque de derechos humanos y género, estas conductas deben considerarse una forma moderna de violencia sexual, en consonancia con los principios de la Convención de Belém do Pará (OEA, 1994) y las recomendaciones de ONU Mujeres (2022).

Por tanto, la respuesta estatal no puede reducirse únicamente al ámbito penal. Debe contemplar mecanismos integrales de reparación, que incluyan:

- Asistencia psicológica y jurídica especializada.
- Eliminación del contenido en línea y derecho al olvido digital.
- Medidas de protección inmediata y compensación económica.

Asimismo, las plataformas tecnológicas deben asumir deberes activos de cooperación en la detección, bloqueo y remoción de material ilícito, contribuyendo a una cultura de responsabilidad digital compartida.

5.7. Propuesta general de política criminal

El estudio concluye que Ecuador necesita una reforma penal sistémica y tecnológicamente consciente, que incluya:

- Una definición legal de imagen íntima sintética.
- Tipificación autónoma para la creación y difusión de deepnudes.
- Agravantes por difusión masiva, automatizada o dirigida a menores.
- Responsabilidad compartida de plataformas digitales.

- Protocolos técnicos para la preservación de evidencia digital.
- Medidas de reparación integral y acompañamiento para las víctimas.

Estas reformas deben formar parte de una política criminal tecnológica integral, articulada entre el legislador, el sistema judicial, las universidades y las agencias de ciberseguridad. Su enfoque debe ser preventivo, educativo y restaurativo, colocando a la víctima en el centro de la respuesta penal.

5.8. Conclusión final

En síntesis, la investigación demuestra que la ausencia de una regulación penal específica sobre imágenes íntimas sintéticas en Ecuador debilita la protección de los derechos fundamentales y perpetúa la impunidad frente a las nuevas formas de violencia digital.

El Derecho Penal ecuatoriano debe redefinirse sin perder su esencia garantista, adoptando una visión humanista, tecnológica y con perspectiva de género.

Solo a través de una reforma legislativa coherente con los estándares internacionales, acompañada de políticas públicas de educación digital, cooperación judicial y fortalecimiento institucional, el Estado podrá garantizar efectivamente la intimidad, la imagen y la dignidad de las personas en la era de la inteligencia artificial.

Así, el Derecho Penal del siglo XXI se consolidará como un instrumento de justicia equilibrada, capaz de responder a los desafíos éticos y tecnológicos del presente sin renunciar a su fin superior: la protección de la persona humana y su dignidad.

Referencias bibliográficas

- Ávila Santamaría, F. (2015). *Derecho penal: Parte general*. Quito: Editorial Jurídica.
- Cámara Nacional Civil de Argentina. (2021). *Expediente 23645/2021*. Buenos Aires, Argentina.
- Carbajo Cascón, A. (2020). La inteligencia artificial y los riesgos penales: Reflexiones sobre su regulación penal futura. *Revista Electrónica de Ciencia Penal y Criminología*, 22, 1–30. <https://www.revistascpce.es>
- Citron, D. K. (2019). *Hate crimes in the digital age*. Harvard University Press.
- Código Orgánico Integral Penal. (2014). *Registro Oficial Suplemento N.º 180 de 10 de febrero de 2014*. (Última reforma vigente).
- Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. Estrasburgo.
- Consejo de Europa. (2021). *Budapest Convention on Cybercrime – Second Additional Protocol*. Estrasburgo.
- Constitución de la República del Ecuador. (2008). *Registro Oficial N.º 449 de 20 de octubre de 2008*.
- Corte Constitucional del Ecuador. (2018). *Sentencia No. 003-18-SIN-CC*.
- Corte Constitucional del Ecuador. (2024). *Sentencia No. 916-22-JP/24*.
- Corte Suprema de Chile. (2021). *Sentencia Rol N.º 126.254-2021*. Santiago de Chile.

- De Hert, P., & Papakonstantinou, V. (2018). The legislation of deepfakes: Challenges and approaches in data protection and criminal law. *Computer Law & Security Review*, 34(4), 894–903. <https://doi.org/10.1016/j.clsr.2018.06.008>
- European Union Agency for Fundamental Rights. (2020). *Deepfakes and the law: Protecting rights in the digital age*. <https://fra.europa.eu/en/publication/2020/deepfakes-and-law>
- Floridi, L. (2019). *The logic of information: A theory of philosophy as conceptual design*. Oxford University Press.
- Guzmán, M., & Ramírez, L. (2021). La protección jurídica contra la difusión de imágenes íntimas sin consentimiento en Ecuador. *Revista Ecuatoriana de Derecho Digital*, 7(2), 45–67.
- Jakobs, G. (1995). *Derecho penal. Parte general: Fundamentos y teoría de la imputación*. Marcial Pons.
- Jescheck, H.-H., & Weigend, T. (2002). *Tratado de Derecho Penal. Parte general*. Comares.
- Lascano, F. (2021). Autoría y complicidad en los delitos tecnológicos. *Revista de Derecho Penal Contemporáneo*, (47), 109–130.
- Llana, J. (2021). Inteligencia artificial y derecho penal: Nuevos retos para la política criminal. *Revista de Derecho Penal y Criminología*, (28), 45–67. <https://doi.org/10.5944/rdpc.28.2021.29518>
- López Jiménez, M. (2023). La agresión simbólica en el entorno digital. *Revista de Derecho y Tecnología*, 5(2), 43–60.

- McCosker, A., & Wilken, R. (2020). Fake me harder: Deepfakes, legal responses and the problem of trust. *International Journal of Law and Information Technology*, 28(3), 215–237. <https://doi.org/10.1093/ijlit/eaz008>
- Muñoz Conde, F. (2020). *Derecho penal: Parte general*. Tirant lo Blanch.
- Naciones Unidas – Oficina del Alto Comisionado para los Derechos Humanos. (2021). *Informe sobre derechos humanos y tecnologías emergentes*.
<https://www.ohchr.org/Documents/Issues/DigitalAge/ReportTechEmerging.pdf>
- Naciones Unidas – Oficina del Alto Comisionado para los Derechos Humanos. (2022). *Informe de la Relatora Especial sobre la violencia contra la mujer y las nuevas tecnologías*.
- Organización de los Estados Americanos (OEA). (1994). *Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (Convención de Belém do Pará)*. Belém do Pará, Brasil.
- Organización de los Estados Americanos (OEA). (2020). *Informe sobre violencia digital y derechos humanos*. Washington, D.C.
- Paredes Castañeda, D. (2022). La violencia digital y sus implicaciones penales: una mirada desde el derecho penal colombiano y comparado. *Revista Derecho Penal Contemporáneo*, (47), 113–135. <https://revistas.unilibre.edu.co/index.php/dpc>
- Pérez Paredes, J. (2024). *La protección penal de la intimidad en la era digital*. Editorial Jurídica Nacional.
- Roxin, C. (2010). *Derecho penal: Parte general. Fundamentos del derecho penal y teoría del delito*. Tirant lo Blanch.

- Sanz, J., & Rodríguez, P. (2022). Desafíos del derecho penal ante la inteligencia artificial. Universidad de Salamanca.
- Silva Sánchez, J. M. (2013). *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales*. Civitas.
- Simó Soler, E. (2023). Retos jurídicos derivados de la inteligencia artificial generativa: deepfakes y violencia contra las mujeres. *InDret*. <https://indret.com>
- Solove, D. J. (2021). *Understanding privacy in the digital age*. Yale University Press.
- Tribunal Constitucional Federal de Alemania. (2000). *BVerfGE 101, 361*. Karlsruhe, Alemania.
- Tribunal Supremo de España. (2022). *Sentencia 70/2022*. Madrid, España.
- Trujillo Cabrera, C. (2023). El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial. *InDret*. <https://indret.com>
- Varela, C. (2021). La protección del derecho a la imagen frente a las tecnologías de inteligencia artificial. *Revista Chilena de Derecho y Tecnología*, 10(1), 101–125. <https://doi.org/10.5354/0719-2584.2021.63601>
- Villamarín, J. (2023). *Peritajes digitales y trazabilidad penal en Ecuador*. Universidad Andina Simón Bolívar.

ANEXOS



Declaratoria de Autoría y Responsabilidad

Eduardo Alejandro Granja Rosero portador(a) de la cédula de ciudadanía N° **0932017635**. Declaro ser el autor de la obra: **“Responsabilidad penal por la difusión de imágenes íntimas no consentidas generadas con inteligencia artificial en Ecuador”**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **19 de noviembre de 2025**

Eduardo Alejandro Granja Rosero

C.I. 0932017635



Vinicio Alejandro Calles Cadena portador(a) de la cédula de ciudadanía N°1400714422. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **“Responsabilidad penal por la difusión de imágenes íntimas no consentidas generadas con inteligencia artificial en Ecuador”** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, 18 de noviembre de 2025

F: 

Vinicio Alejandro Calles Cadena

C.I. 1400714422