LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, Asunción, Paraguay.
ISSN en línea: 2789-3855, 2025, Volumen VI

Protección de derechos sobre la propia imagen, datos personales e intimidad frente a los deepfakes

Protection of rights over one's own image, personal data, and privacy against deepfakes

Anyel Marina Ponce González
e1350576565@live.uleam.edu.ec
https://orcid.org/0009-0006-2530-2648
Universidad Laica Eloy Alfaro de Manabí
Ecuador

Javier Andrés Espinoza Suárez
Javier.espinoza@uleam.edu.ec
https://orcid.org/0009-0000-8126-4400
Universidad Laica Eloy Alfaro de Manabí
Ecuador

Anthony Posso Loor
e1314617224@live.uleam.edu.ec
https://orcid.org/0009-0003-0444-8208
Universidad Laica Eloy Alfaro de Manabí
Ecuador

DOI: https://doi.org/10.56712/latam.v6i3.3947

Artículo recibido: 05 de mayo de 2025
Aceptado para publicación: 19 de mayo de 2025.
Conflictos de Interés: Ninguno que declarar.

NÚMERO 3

DOI: https://doi.org/10.56712/latam.v6i3.3947

Protección de derechos sobre la propia imagen, datos personales e intimidad frente a los *deepfakes*

Protection of rights over one's own image, personal data, and privacy against deepfakes

Anyel Marina Ponce González
e1350576565@live.uleam.edu.ec
https://orcid.org/0009-0006-2530-2648
Universidad Laica Eloy Alfaro de Manabí
Ecuador

Javier Andrés Espinoza Suárez
Javier.espinoza@uleam.edu.ec
https://orcid.org/0009-0000-8126-4400
Universidad Laica Eloy Alfaro de Manabí
Ecuador

Anthony Posso Loor
e1314617224@live.uleam.edu.ec
https://orcid.org/0009-0003-0444-8208
Universidad Laica Eloy Alfaro de Manabí
Ecuador

Artículo recibido: 05 de mayo de 2025. Aceptado para publicación: 19 de mayo de 2025.
Conflictos de Interés: Ninguno que declarar.

Resumen

El presente artículo tiene como objetivo analizar la capacidad del marco legal ecuatoriano para proteger los derechos a la imagen, la intimidad y los datos personales frente al uso de tecnologías de deepfake. Estas tecnologías, basadas en inteligencia artificial, permiten manipular imágenes, voces y videos de manera altamente realista, lo que plantea riesgos éticos, legales y sociales significativos. La investigación se desarrolló a través de una metodología documental y sociojurídica, basada en la recopilación y análisis de fuentes bibliográficas, normativas y jurisprudenciales, con el fin de identificar las limitaciones del ordenamiento jurídico vigente. Entre los principales hallazgos, se evidenció que, aunque Ecuador cuenta con normas generales como la Constitución, el COIP y la Ley de Protección de Datos Personales, no existen disposiciones específicas que regulen el fenómeno de los deepfakes. Esta ausencia dificulta la protección efectiva de los derechos afectados y contrasta con los avances legislativos observados en países como Francia, Estados Unidos y la Unión Europea. Se concluye que es urgente reformar y adaptar la legislación ecuatoriana para enfrentar los desafíos que plantea esta tecnología emergente, garantizando así la autodeterminación digital y la protección integral de los derechos fundamentales en la era digital.

Palabras clave: deepfake, privacidad, derechos de imagen, protección de datos

Abstract

This article aims to analyze the capacity of the Ecuadorian legal framework to protect the rights to image, privacy, and personal data against the use of deepfake technologies. These AI-based tools enable the highly realistic manipulation of images, voices, and videos, raising significant ethical, legal,

and social concerns. The research was carried out using a documentary and socio-legal methodology, based on the collection and analysis of bibliographic, normative, and jurisprudential sources, to identify the limitations of the current legal system. Among the main findings, it was noted that although Ecuador has general regulations such as the Constitution, the Comprehensive Organic Criminal Code (COIP), and the Personal Data Protection Law, there are no specific provisions addressing the deepfake phenomenon. This absence hinders the effective protection of affected rights and contrasts with legislative progress observed in countries such as France, the United States, and the European Union. It is concluded that there is an urgent need to reform and adapt Ecuadorian legislation to face the challenges posed by this emerging technology, thus ensuring digital self-determination and comprehensive protection of fundamental rights in the digital age.

Keywords: deepfake, privacy, image rights, data protection

Cómo citar: Ponce González, A. M., Espinoza Suárez, J. A., & Posso Loor, A. (2025). Protección de derechos sobre la propia imagen, datos personales e intimidad frente a los deepfakes. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 6 (3), 276 – 288. https://doi.org/10.56712/latam.v6i3.3947*

INTRODUCCIÓN

El término “ultrafalso”, “mentiras profundas” o deepfakes se refiere a una forma de distorsionar la imagen

de una persona utilizando herramientas tecnológicas avanzadas, por lo que para comprender la terminología, es necesario entender que la palabra "profundo” alude a algo muy hondo o abismal, es decir, que llega hasta el fondo, aunque también puede referirse a aquello que se adentra en algo hasta su extremo, por lo que no necesariamente implica una dirección hacia abajo (Cerdán & Padilla, 2019), de este modo, al referirse al término en español “mentiras profundas” indica que es aquella que alcanza los extremos de la recreación de lo real, siendo casi imposible determinar su falsedad o veracidad.

Etimológicamente se puede definir a las Deepfakes como aquella tecnología que mediante inteligencia artificial (IA) se pueden modificar videos o imágenes a partir de audios, imágenes y videos previamente obtenidos (L. Institute, 2024). Los Deepfakes son creados a partir de patrones los cuales son procesados por la inteligencia artificial lo que permite la reproducción y creación de lo que se desee (L. Institute, 2024).

Para dar creación a una Deepfake se necesita la unión de dos elementos:

Deepvoice: Tecnología mediante la cual clonan una voz o unen la voz original de un individuo para crear una secuencia artificial.

Deepface: Tecnología dentro de la cual superponen el rostro del individuo y falsifican sus gestos, consiguiendo resultados extremadamente realistas.

Como se puede denotar la unión de ambas es lo que conocemos como Deepfake, no obstante, estas herramientas pueden tener un buen uso y a su vez un mal uso debido a que por medio de las deepvoice se pueden dar extorsiones, y por el lado de las deepface se puede dar la suplantación de la identidad y otros tipos de delitos los cuales pueden desencadenarse con el uso malicioso de esta herramienta.

Siguiendo el orden de ideas, un estudio reciente llevado a cabo por la revista científica PNAS determinó que los rostros generados sintéticamente son prácticamente indistinguibles de los reales, incluso para personas que han sido capacitadas para identificar imágenes falsas tienen dificultades para distinguir entre contenido real y Deepfakes (Groh, Epstein, & Picard, 2021).

Lo antes expuesto conduce a una importante interrogante: ¿Son los Deepfakes una forma de libre expresión o una tecnología para cometer delitos no debidamente sancionados? La respuesta más idónea para esta pregunta tiende a recaer en la subjetividad debido a que al ser una tecnología de libre acceso, esta puede ser usada de distintas formas, por ello la respuesta a dicha pregunta tendrá distintas interpretaciones de acuerdo al uso que se le dé a esta, por ejemplo, para un editor de imágenes o videos este tipo de herramientas resulta muy útil, dado que permite insertará una persona dentro de una imagen o video en los que originalmente no aparecía, sin embargo, también existen personas las cuales usan este tipo de herramientas con fines malintencionados, como acosar, suplantar identidad, entre otro tipo de acciones con claras intenciones dolosas.

Si bien dentro de la normativa ecuatoriana este tipo de delitos son sancionados, no tienden a hacerlo de la manera pertinente, dado que este tipo de delitos que se realizan a partir de esta tecnología se pueden considerar nuevos dentro del Ecuador y a la vez en el mundo.

Las preocupaciones son principalmente de tipo ético, político, legal y tecnológico, a causa de que se fundan en el hecho de que los deepfakes minan la credibilidad de los documentos audiovisuales,

principalmente videos, como medios de información o certificación de hechos, poniendo en entredicho su veracidad o generando riesgos de desinformación, difamación o chantaje. (Bañuelos, 2020).

Como se ha hecho previa mención, la falta u la necesidad de sanciones o leyes las cuales sancionen directamente las Deepfakes son muy carentes o no suelen darse para todo el mundo, por un lado tenemos La ley Elvis la cual prohíbe a las personas que por medio de inteligencia artificial modifiquen o imiten la voz de un artista sin su permiso, con esto se busca garantizar la seguridad de la voz y la imagen de los artistas (Rábago, 2024), también han existido sanciones para las Deepfakes en tiempos de campaña electoral en Estados Unidos, sin embargo, no existe hasta la actualidad una ley especifica para tipificar las deepfakes, si bien ya existen países los cuales están comenzando a sancionar y a crear leyes especificas para esto, Ecuador por su parte se esta quedando muy atrás, lo único que salvaguarda la integridad y los derechos de una persona afectada por esta tecnología se encuentra dentro de la Constitución de la República del Ecuador, el Código Orgánico Integral Penal y la Ley de Protección de Datos personales, sin embargo, a pesar de que existen diversas normativas que protegen múltiples derechos que se vulneran por esta tecnología, ninguno de estos instrumentos incorpora el uso de deepfakes como un delito específico, lo que hace que la defensa en casos donde se utiliza esta tecnología sea más compleja.

Por lo antes expuesto, esta complejidad surge porque el delito no está contemplado de manera específica, dentro del Código Orgánico Integral Penal establece varios artículos que, aunque pueden aplicarse a ciertos aspectos de los deepfakes, carecen de especificidad, por ejemplo, el artículo 103, que sanciona la producción y difusión de materiales visuales que exploten la imagen de niños y adolescentes, aunque crucial, no abarca el espectro más amplio de las manipulaciones que afectan a adultos, por otro lado, el artículo 154, sobre la intimidación, y el artículo 212, que tipifica la suplantación de identidad, también presentan limitaciones en su aplicabilidad a los deepfakes, dado que estas prácticas a menudo ocurren en un entorno digital que complica la identificación y el enjuiciamiento de los infractores (COIP, 2024).

Asimismo, la Ley de Protección de Datos Personales, en su artículo 7, establece que el tratamiento de datos personales debe ser legítimo y contar con el consentimiento del titular, sin embargo, la naturaleza de los deepfakes, que a menudo utilizan imágenes y voces sin autorización, plantea interrogantes sobre la efectividad de esta norma en la protección de los derechos individuales (LOPDP, 2021). La jurisprudencia vinculada al habeas data refuerza la necesidad de un marco legal que reconozca explícitamente el impacto de las tecnologías emergentes en la intimidad y la imagen de las personas

Es importante plantear la interrogante: ¿Es el deepfake tan reciente como para que no existan leyes que lo regulen? Las Deepfakes comenzaron a cobrar relevancia en 2018, principalmente por su uso en videos de contenido sexual, no obstante, los indicios se remontan a 2014 (Cerdán & Padilla, 2019).

El desarrollo de los deepfakes está vinculado a importantes avances en inteligencia artificial y redes neuronales, así como a aplicaciones prácticas que han suscitado controversia. A continuación, se destacan momentos clave que marcaron el origen y la popularización de esta tecnología:

En 2014 Ian Goodfellow, un estudiante de doctorado de la Universidad de Montreal, abordó de forma pionera la generación de imágenes con el enfoque de redes neuronales degenerativas adversas, GAN. Goodfellow entrenó dos redes neuronales con una misma base de datos de imágenes para luego crear otras nuevas. Enfrentó las dos redes para que identificaran qué imágenes eran reales y cuáles eran ficticias como un juego digital del gato y el ratón.

En 2017 un usuario anónimo de Reddit utilizó el deep learning para intercambiar las caras de actrices famosas con las de las actrices originales en escenas de películas para adultos.

En el 2017 comenzaron a verse deep fakes de famosos. Especialmente populares fueron las falsificaciones de Emma Watson y Natalie Portman. También se han hecho videoclips de la ex primera dama Michelle Obama; de la hija del expresidente Donald Trump, Ivanka Trump; o de la duquesa de Cambridge, Kate Middleton (ESIC, 2021).

El primer modelo de red neuronal generaba imágenes nuevas a partir de la base de datos que había aprendido creando, por ejemplo, un gato con dos colas. El segundo modelo detectaba las imágenes ficticias, y así el primero aprendía de sus propios errores y generaba gatos con una única cola, por lo que poco a poco se iban creando imágenes cada vez más realistas y difíciles de distinguir (ESIC, 2021).

En sus orígenes, estas redes neuronales cometía una gran cantidad de fallos, como bicicletas con dos manillares o caras con las cejas fuera de su sitio. Ahora mismo son capaces de crear con una alta verosimilitud una imagen completa a partir de una parte de esta: por ejemplo, el cuerpo de un gato a partir de su cabeza (ESIC, 2021).

Es por ello que el eje central de este artículo radica en evaluar la capacidad del marco legal ecuatoriano para proteger los derechos sobre la propia imagen, los datos personales y la intimidad frente al uso de deepfakes, por lo que, se realizará un análisis crítico del marco normativo vigente, identificando sus limitaciones y proponiendo la extensión de las normas existentes para abordar eficazmente las vulneraciones derivadas de esta tecnología, además, se explorará el concepto de consentimiento informado en el uso de imágenes y datos personales en relación con los deepfakes, argumentando la necesidad de adaptar y reformar la legislación para reflejar las realidades de un mundo digital en constante evolución. Este análisis se enmarca en la urgencia de establecer un marco jurídico que no solo garantice la protección de los derechos individuales, sino que también promueve la autodeterminación digital, salvaguardando así la dignidad y la privacidad de los ciudadanos ecuatorianos en la era de la información.

METODOLOGÍA

La investigación es principalmente de carácter documental o bibliográfica, la naturaleza de esta técnica de investigación consiste en la identificación, recopilación y análisis de los documentos seleccionados que proporcionen hechos u eventos asociados al material de estudio, para la obtención de aquellos documentos se complementa con la investigación bibliográfica dado que la esencia de dicha investigación radica en el conjunto de técnicas y estrategias que se utilizan para localizar e identificar documentos los cuales contienen la información necesaria para la investigación (Hernández, Fernández, & Baptista, 1997).

Del mismo modo, la investigación se caracteriza por ser socio jurídica, dado que se centra en el análisis de cómo las normas jurídicas afectan y son afectadas por los comportamientos, valores y estructuras sociales, este tipo de investigación busca entender las dinámicas sociales y su impacto en la aplicación y evolución del derecho, así como explorar cómo las leyes pueden ser utilizadas para promover cambios sociales y mejorar la justicia (Bernal, Díaz, & Padilla, 2017).

RESULTADOS Y DISCUSIÓN

En el ámbito nacional, la Corte Constitucional del Ecuador ha abordado, aunque de manera indirecta, la protección de la imagen personal, específicamente, en el Caso No. 2064-14-EP (2021), la Corte reconoció que el rostro y otros aspectos identificativos de una persona constituyen datos personales protegidos, pues son representaciones directas de la identidad de un individuo, este fallo reitera lo dispuesto en el artículo 66, numeral 18 de la Constitución, donde se garantiza el derecho al honor y buen nombre, así como la protección de la imagen y voz de la persona, en donde a partir de este pronunciamiento, se estableció que cualquier uso no autorizado de imágenes personales puede

constituir una vulneración de derechos fundamentales, lo que sienta un precedente para el manejo de casos relacionados con la manipulación digital de contenido, como los deepfakes.

A partir de lo expuesto, se evidencia que los primeros intentos en Ecuador por abordar aspectos relacionados de manera indirecta con el fenómeno de los deepfakes surgieron apenas en 2021, lo que pone de manifiesto las limitaciones del marco normativo nacional, en contraste, diversas jurisdicciones internacionales han adoptado medidas específicas para enfrentar las implicaciones legales de esta tecnología, por un lado, la Unión Europea, mediante el Artificial Intelligence Act, establece un marco regulatorio para tecnologías de inteligencia artificial, clasificando los deepfakes como un riesgo significativo para los derechos fundamentales, esta normativa exige que las aplicaciones de IA utilizadas para manipular datos visuales garanticen la transparencia y que los usuarios sean informados cuando se encuentren frente a contenido generado artificialmente (Ley de Inteligencia Artificial UE, 2024).

En Francia, se ha adoptado una legislación que prohíbe expresamente la creación y difusión de deepfakes no consensuados, en donde no solo penaliza la manipulación de imágenes y voces sin autorización, sino que también amplía la protección a casos en los que la difusión maliciosa de contenido falso cause daño a la reputación o a la privacidad de las personas (H. Lovells, 2024), lo que representa un avance al incluir tanto el daño real como el potencial, y al establecer mecanismos procesales claros para las víctimas.

En Estados Unidos, estados como California han legislado específicamente contra los deepfakes en contextos electorales y de explotación sexual, la ley californiana criminaliza la creación y uso de deepfakes diseñados para influir en elecciones o para dañar reputaciones, reflejando una preocupación por el impacto sociopolítico de esta tecnología (Karsondas, 2024). En el Reino Unido, se han dado pasos similares, particularmente en la protección contra deepfakes de naturaleza sexual, estableciendo sanciones que buscan disuadir estas prácticas y proporcionar herramientas legales más efectivas para las víctimas (Karsondas, 2024).

El Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha subrayado que el desarrollo de tecnologías de inteligencia artificial, incluidos los deepfakes, debe estar alineado con los principios de derechos humanos, lo que enfatiza la autodeterminación digital, la transparencia y el consentimiento informado como pilares esenciales para mitigar el impacto de estas tecnologías sobre la privacidad y la imagen personal (Naciones Unidas , 2023).

El Comité Jurídico Interamericano, como parte de su labor en la protección de los derechos humanos en América, ha impulsado la creación de un marco normativo común para la protección de los datos personales en la región, lo que busca garantizar que los datos sean tratados de manera legítima y con el consentimiento explícito de las personas, evitando su uso para fines no autorizados, en este sentido, el Comité resalta que los datos personales deben ser recolectados con fines específicos y legítimos, y deben ser protegidos con medidas de seguridad adecuadas, además, subraya la importancia de que las legislaciones permitan a los individuos acceder y corregir sus datos personales, especialmente aquellos que pueden ser considerados sensibles y causar daños significativos si se utilizan de forma inapropiada (Comité Interamericano, 2017).

Estos principios adquieren especial relevancia en el contexto de los deepfakes, dado que las tecnologías utilizadas para crear y difundir contenido manipulado pueden vulnerar la privacidad e identidad de las personas al alterar imágenes y audios sin su consentimiento, por ello, el Comité ha propuesto que los países miembros de la Organización de Estados Americanos (OEA) adopten un marco regulatorio homogéneo para proteger los derechos de las personas frente al uso indebido de sus datos personales, promoviendo la cooperación internacional y asegurando la circulación segura de los datos en la región (Comité Interamericano, 2017).

Desde una perspectiva académica, autores han señalado que los deepfakes presentan un desafío sin precedentes al combinar el poder de la inteligencia artificial con la capacidad de alterar la percepción de la realidad, lo que demanda un marco normativo que abarque tanto los daños directos como los potenciales que puedan derivarse de estas manipulaciones, algo que países como Francia y Estados Unidos ya están implementando (Talas & Kearney, 2019).

Estas experiencias internacionales ponen de relieve la necesidad de normativas específicas que aborden directamente el impacto de los deepfakes, ampliando el alcance de las leyes tradicionales para adaptarse a los desafíos tecnológicos actuales, en comparación, el marco ecuatoriano, limitado a disposiciones generales sobre protección de datos personales y derechos de imagen, resulta insuficiente para atender los casos más complejos derivados de esta tecnología emergente

A pesar de que Ecuador ha dado pasos importantes en la protección de los derechos de la imagen, datos personales e intimidad, aún existe un vacío normativo significativo en cuanto a la regulación directa y específica de los deepfakes, pues las disposiciones actuales, aunque ofrecen un marco general para la protección de derechos fundamentales como el derecho al honor y a la propia imagen, no abordan con claridad ni especificidad el impacto de las tecnologías emergentes, como los deepfakes, sobre estos derechos.

La falta de una legislación específica sobre el uso y manipulación de contenido digital mediante inteligencia artificial coloca a Ecuador en una posición vulnerable frente a los desafíos tecnológicos y sus implicaciones en los derechos fundamentales, mientras que otras jurisdicciones internacionales, como la Unión Europea, Francia y Estados Unidos, ya han adoptado normativas detalladas sobre el tema, Ecuador no cuenta con un marco legal que contemple las particularidades de la creación, difusión y uso de deepfakes.

Este vacío normativo impide que las víctimas de manipulación digital, como el uso no consensuado de su imagen o voz en contenido falso, cuenten con las herramientas legales adecuadas para protegerse, de este modo, el país se encuentra en una situación en la que los derechos de las personas a su propia imagen, intimidad y datos personales no están suficientemente protegidos frente a los avances tecnológicos que permiten crear y difundir contenido manipulado, en consecuencia, se revela de manera urgente la creación de leyes que aborden de manera directa los retos que los deepfakes representan para los derechos humanos en Ecuador.

Retomando el postulado dentro del ámbito nacional, La Corte Constitucional del Ecuador ha abordado e impulsado de manera explícita la protección de datos de carácter personal, dentro de la Sentencia No. 110-21-IN/22, dentro de la misma la corte ha determinado que existe una protección constitucional de los datos personales y que su tratamiento requiere del consentimiento expreso inequívoco del titular o un mandato legal, en esta misma sentencia se señala que el acceso a un dato personal por parte de un tercero podría interpretarse y ser considerado como tratamiento de datos, esto en concordancia con el artículo 66 de la Constitución el cual reconoce y garantiza a las personas de aspectos tales como el numeral 19 que manifiesta el derecho a la protección de datos de carácter personal dentro del cual se incluyen el acceso y la sobreinformación de datos a la par de correspondiente protección; como se ha podido denotar la Corte Constitucional en reiteradas ocasiones ha hecho moción respecto a la protección de datos de carácter personal mas sin embargo carecemos de una regulación directa, es decir de delitos en los cuales la protección de datos en este caso el rostro no poseen una regulación específica, es por ello que delitos como los Deepfakes en el marco normativo ecuatoriano carecen de una sanción o una pena directa.

Al existir la carencia de una sanción se ha empezado a producir con mayor frecuencia las Deepfakes dentro del Ecuador, si bien una parte de ellas son utilizadas para hacer sátira y contenidos los cuales no tienen una repercusión penal, ya se han presentado casos dentro de los cuales si recae una

repercusión penal, para ejemplo de ello se presenta el caso que sucedió en un colegio católico de la ciudad de Quito dentro del cual dos jóvenes estudiantes del primer año de bachillerato utilizaron fotografías de 24 estudiantes de género femenino con el afán de crear imágenes y videos de tipo sexual mediante el uso de inteligencia artificial, como se puede denotar existe la intención de querer hacer un daño ya que no solo fue la manipulacion de fotografias de 24 estudiantes sino que a partir de ello mediante la inteligencia artificial se llegó a difundir alrededor de 700 contenidos entre imágenes y videos, las víctimas llegaron a conocer de dicho contenido debido a que este se empezó a compartir entre todo el colegio (Loaiza, 2023).

Por lo antes expuesto, el jueves 5 de octubre de 2023, alrededor de las 15:00 horas, la Fiscalía anunció el inicio de una investigación de oficio por el presunto delito de pornografía con utilización de niños, niñas y adolescentes (Loaiza, 2023), tipificado en el artículo 104 del Código Orgánico Integral Penal (COIP), aunque dicho artículo menciona la comercialización de este tipo de contenido, omite un aspecto crucial: la creación del material en cuestión.

El texto del artículo establece que: "La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda" será sancionada, pero en ningún momento menciona expresamente a "la persona que cree" dicho contenido, esta omisión es especialmente relevante en el contexto de los Deepfakes, ya que este tipo de material suele generarse a partir de imágenes extraídas de redes sociales, sin necesidad del consentimiento pleno de las víctimas.

Adicionalmente, muchas plataformas digitales se deslindan de responsabilidad a través de sus políticas de privacidad, por ejemplo, en los términos de uso de Facebook, los usuarios otorgan una "licencia internacional, libre de regalías, sublicenciable, transferible y no exclusiva para alojar, usar, distribuir, modificar, publicar, copiar, mostrar o exhibir públicamente y traducir su contenido", lo que implica que cualquier imagen compartida en la plataforma puede ser almacenada, copiada y distribuida por terceros.

Dado el creciente uso de Deepfakes para la creación de contenido ilícito, resulta fundamental que la normativa penal reconozca y sancione adecuadamente estos delitos, aunque el COIP contempla la penalización de ciertos actos relacionados con la pornografía infantil, su formulación actual es ambigua y no aborda de manera específica los nuevos riesgos derivados del uso de inteligencia artificial en la manipulación de imágenes, por ello, se vuelve necesario actualizar y extender el marco legal para garantizar una protección efectiva frente a este tipo de delitos en expansión.

Si bien existe un vacío normativo en torno a esta tecnología, es sustancial reconocer que su uso no se limita únicamente a personas naturales, dado que las personas jurídicas también han implementado Deepfakes y herramientas de inteligencia artificial con fines comerciales, políticos y publicitarios, recurriendo a la modificación o suplantación parcial o total de la identidad de individuos o colectivos.

No obstante, el impacto de esta tecnología puede afectar a terceros de manera significativa, un caso que ilustra esta problemática es la controversia generada en Ecuador en torno a la influencer virtual Nina Tapuy, creada mediante inteligencia artificial, mientras algunos celebran este avance tecnológico, otros lo consideran un acto de robo de identidad y racismo, ya que la influencer fue diseñada con rasgos indígenas sin consentimiento de las comunidades a las que supuestamente representa.

En este sentido, la activista indígena Nina Gualinga expresó su rechazo ante el uso de imágenes sin autorización:

> *"No hemos dado consentimiento de utilizar fotos de personas de nuestra familia o de nuestro pueblo, como lo están haciendo. Y lo más probable es que la gente detrás de esta cuenta no conozca ni los nombres, ni a qué nacionalidad pertenece, peor aún la historia de las personas en*

las fotos que utilizan para generar este personaje de IA. Por favor, den de baja a esta cuenta" (El Comercio, 2024)

Por lo tanto, se evidencia la necesidad de extender ciertas normativas para abordar directamente la creación y difusión de contenido manipulado mediante inteligencia artificial, encontrándose normativa relevante a extender en la Ley del Consumidor y el Código Orgánico Integral Penal:

Tabla 1

Propuesta de Extensión de Normativa

Normativa Original	Normativa con Extensión
Código Orgánico Integral Penal (COIP) Art. 212.- Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.	Código Orgánico Integral Penal (COIP) Art. 212.- Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. Se considera suplantación de identidad la alteración, modificación o recreación de la imagen, voz o apariencia de una persona a través de herramientas tecnológicas con el fin de inducir a error, causar daño o generar beneficios indebidos.
Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.- La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.	Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.- La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años. Se considerará agravante el uso de técnicas de manipulación digital para la creación, alteración o simulación de material ilícito con el fin de aparentar la participación de menores de edad.
Art. 185.- Extorsión.- La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. La sanción será de cinco a siete años si se verifican alguna de las siguientes circunstancias: 1. Si la víctima es una persona menor a dieciocho años, mayor a sesenta y cinco años, mujer embarazada o persona con discapacidad, o una persona que padezca enfermedades que comprometan su vida. 2. Si se ejecuta con la intervención de una persona con quien la víctima mantenga relación laboral, comercio u otra similar o con una persona de confianza o pariente dentro del	Art. 185.- Extorsión.- La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. La sanción será de cinco a siete años si se verifican alguna de las siguientes circunstancias: 1. Si la víctima es una persona menor a dieciocho años, mayor a sesenta y cinco años, mujer embarazada o persona con discapacidad, o una persona que padezca enfermedades que comprometan su vida. 2. Si se ejecuta con la intervención de una persona con quien la víctima mantenga relación laboral, comercio u otra similar o con una persona de confianza o pariente dentro del

cuarto grado de consanguinidad y segundo de afinidad. 3. Si el constreñimiento se ejecuta con amenaza de muerte, lesión, secuestro o acto del cual pueda derivarse calamidad, infortunio o peligro común. 4. Si se comete total o parcialmente desde un lugar de privación de libertad. 5. Si se comete total o parcialmente desde el extranjero.	cuarto grado de consanguinidad y segundo de afinidad. 3. Si el constreñimiento se ejecuta con amenaza de muerte, lesión, secuestro o acto del cual pueda derivarse calamidad, infortunio o peligro común. 4. Si se comete total o parcialmente desde un lugar de privación de libertad. 5. Si se comete total o parcialmente desde el extranjero. 6. Si la intimidación se realiza mediante la difusión de contenido audiovisual manipulado con el fin de afectar la reputación, inducir al miedo o generar coacción sobre la víctima.
Art. 154.- Intimidación. - La persona que amenace o intimide a otra con causar un daño que constituya delito a ella, a su familia, a personas con las que esté íntimamente vinculada, siempre que, por antecedentes, aparezca verosímil la consumación del hecho, será sancionada con pena privativa de libertad de uno a tres años.	Art. 154.- Intimidación. - La persona que amenace o intimide a otra con causar un daño que constituya delito a ella, a su familia, a personas con las que esté íntimamente vinculada, siempre que, por antecedentes, aparezca verosímil la consumación del hecho, será sancionada con pena privativa de libertad de uno a tres años. Se considerará agravante la utilización de contenido audiovisual alterado o manipulado con el fin de generar pánico, coacción o desprestigio.
Ley Orgánica de Defensa del Consumidor Art. 7.- Infracciones Publicitarias. - Comete infracción a esta Ley el proveedor que a través de cualquier tipo de mensaje induce al error o engaño en especial cuando se refiere a: 1. País de origen, comercial o de otra índole del bien ofrecido o sobre el lugar de prestación del servicio pactado o la tecnología empleada; 2. Los beneficios y consecuencias del uso del bien o de la contratación del servicio, así como el precio, tarifa, forma de pago, financiamiento y costos del crédito; 3. Las características básicas del bien o servicio ofrecidos, tales como componentes, ingredientes, dimensión, cantidad, calidad, utilidad, durabilidad, garantías, contraindicaciones, eficiencia, idoneidad del bien o servicio para los fines que se pretende satisfacer y otras; y, 4. Los reconocimientos, aprobaciones o distinciones oficiales o privadas, nacionales o extranjeras, tales como medallas, premios, trofeos o diplomas.	Ley Orgánica de Defensa del Consumidor Art. 7.- Infracciones Publicitarias. - Comete infracción a esta Ley el proveedor que a través de cualquier tipo de mensaje induce al error o engaño en especial cuando se refiere a: 1. País de origen, comercial o de otra índole del bien ofrecido o sobre el lugar de prestación del servicio pactado o la tecnología empleada; 2. Los beneficios y consecuencias del uso del bien o de la contratación del servicio, así como el precio, tarifa, forma de pago, financiamiento y costos del crédito; 3. Las características básicas del bien o servicio ofrecidos, tales como componentes, ingredientes, dimensión, cantidad, calidad, utilidad, durabilidad, garantías, contraindicaciones, eficiencia, idoneidad del bien o servicio para los fines que se pretende satisfacer y otras; y, 4. Los reconocimientos, aprobaciones o distinciones oficiales o privadas, nacionales o extranjeras, tales como medallas, premios, trofeos o diplomas. 5. La manipulación digital de imágenes, videos o audios que distorsionen la realidad con el propósito de inducir al engaño sobre la autenticidad de una persona, producto o servicio.

CONCLUSIONES

Entorno a la metodología utilizada para recopilar información dentro del presente artículo, hemos podido determinar las siguientes conclusiones:

Ecuador, al igual que muchas naciones, enfrenta el auge de delitos derivados de la inteligencia artificial, como los deepfakes, los cuales representan una seria amenaza para la privacidad, la identidad y la seguridad digital de las personas, a nivel internacional, países como Francia, Estados Unidos y la Unión Europea han implementado regulaciones específicas para mitigar los riesgos asociados a esta tecnología, mientras que en Ecuador el marco legal sigue siendo insuficiente.

Aunque la Constitución, el Código Orgánico Integral Penal y la Ley de Protección de Datos Personales contemplan la protección de derechos fundamentales, carecen de normas específicas que tipifiquen y sancionen de manera efectiva estas conductas, esta laguna jurídica genera incertidumbre y limita las herramientas de defensa para las víctimas, dado el impacto creciente de los deepfakes, resulta urgente que el país adapte su legislación, estableciendo mecanismos claros de prevención y sanción, alineados con estándares internacionales, con el fin de garantizar una tutela efectiva de los derechos fundamentales y preservar la confianza en el entorno digital.

REFERENCIAS

Bañuelos, J. (2020). Deepfake: la imagen en tiempo de la posverdad. Ciudad de México: Revista Panamericada de Comunicación. doi:https://doi.org/10.21555/rpc.v0i1.2315

Bernal, D., Díaz, E., & Padilla, A. (2017). Retos éticos de la investigación sociojurídica: una revisión a partir de buenas prácticas en artículos publicados. Obtenido de https://revistas.urosario.edu.co/xml/733/73355497005/html/index.html#:~:text=La%20investigaci%C3%B3n%20sociojur%C3%ADdica%20tiene%20como,Arango%20Paj%C3%B3n%2C%202013%2C%20p

C. Constitucional del Ecuador. (2021). CASO No. 2064-14-EP. Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

Cerdán, V., & Padilla, G. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. Ediciones complutense. Obtenido de https://revistas.ucm.es/index.php/HICS/article/view/66293/4564456552459

COIP. (2024). Código Orgánico Integral Penal, COIP. Quito: LEXIS. Obtenido de https://www.lexis.com.ec/biblioteca/coip

Comité Interamericano. (2017). LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES. Obtenido de https://www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_CJI-doc_541-17_corr1.pdf

El Comercio. (junio de 8 de 2024). EL COMERCIO. Obtenido de Polémica por el nombre de influencer ecuatoriana creada con Inteligencia Artificial: https://www.elcomercio.com/tecnologia/influencer-virtual-ecuador-polemica-nina-gualinga.html

ESIC. (Julio de 2021). ESIC Business & Marketing School. Obtenido de https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros#:~:text=C%C3%B3mo%20se%20crea%20un%20deep%20fake&text=Utiliza%20las%20denominadas%20redes%20neuronales,ese%20objeto%2C%20rostro%20o%20imagen.

Groh, M., Epstein, F. C., & Picard, R. (2021). Deepfake detection by human crowds, machines, and machine informed crowds. PNAS. doi:https://doi.org/10.1073/pnas.211001311

H. Lovells. (15 de julio de 2024). Francia prohíbe las falsificaciones no consentidas. Obtenido de https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes

Hernández, R., Fernández, C., & Baptista, P. (1997). METODOLOGÍA DE LA INVESTIGACIÓN. Obtenido de https://www.uv.mx/personal/cbustamante/files/2011/06/metodologia-de-la-investigaci%C3%83%C2%B3n_sampieri.pdf

Hogan Lovells. (15 de julio de 2024). Francia prohíbe las falsificaciones no consentidas. Obtenido de https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes

Karsondas, A. (14 de agosto de 2024). YOTI. Obtenido de Leyes sobre deepfakes: regulaciones globales en la era digital contra el uso sexual explícito y criminal de deepfakes: https://www.yoti.com/blog/deepfake-laws/

L. Institute. (2024). Lisa Institute. Obtenido de https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-

amenazas#:~:text=Los%20Deepfakes%20o%20%22falsedades%20profundas,parezcan%20originales%2C%20aut%C3%A9nticos%20y%20reales.

Ley de Inteligencia Artificial UE. (2024). Ley de Inteligencia Artificial (reglamento (UE) 2024/1698). Obtenido de artificialintelligenceact

Ley Orgánica de Defensa del Consumidor. (2011). Ley Orgánica de Defensa del Consumidor. Obtenido de https://www.gob.ec/sites/default/files/regulations/2018-09/Documento_Ley-Org%C3%A1nica-Defensa-Consumidor.pdf

LISA Institute. (2024). Lisa Institute. Obtenido de https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas#:~:text=Los%20Deepfakes%20o%20%22falsedades%20profundas,parezcan%20originales%2C%20aut%C3%A9nticos%20y%20reales.

Loaiza, Y. (5 de octubre de 2023). Infobae. Obtenido de https://www.infobae.com/america/america-latina/2023/10/05/estudiantes-de-un-colegio-de-quito-utilizaron-fotografias-de-sus-companeras-para-crear-contenido-sexual-con-inteligencia-artificial/

LOPDP. (2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Naciones Unidas . (12 de julio de 2023). Naciones Unidas Derechos Humanos Oicina del Alto Comisionado. Obtenido de https://www.ohchr.org/es/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner

Rábago, R. (2 de Abril de 2024). VOZ. Obtenido de https://voz.us/es/tecnologia/240402/11653/ley-elvis-tennessee-primer-estado-protege-artistas-amenazas-inteligencia-artificial.html

Talas, T., & Kearney, M. (2019). Diving into the deep end: regulating deepfakes online. Obtenido de https://www.austlii.edu.au/au/journals/CommsLawB/2019/24.pdf