Vol.8 No.2 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.2.2024.1950-1970

The criminalisation of Deepfake Pornography in Ecuador and the age of artificial intelligence

La tipificación del delito Deepfake Pornográfico en Ecuador y la era de la inteligencia artificial

Autores:

Valverde-Ramos, Mishell Sthefanny
UNIVERSIDAD BOLIVARIANA DEL ECUADOR
Maestrante en Derecho Procesal
Durán – Ecuador
msvalverder@ube.edu.ec
https://orcid.org/0009-0006-6804-7560

Armijos-González, Marlon Jeovanny
UNIVERSIDAD BOLIVARIANA DEL ECUADOR
Maestrante en Derecho Procesal
Durán – Ecuador
mjarmijosg@ube.edu.ec
https://orcid.org/0009-0005-1106-5437

Ph.D. Martínez-Pérez, Odette
UNIVERSIDAD BOLIVARIANA DEL ECUADOR
Docente Tutor
Durán – Ecuador
omartinezp@ube.edu.ec
https://orcid.org/0000-0001-6295-2216

Fechas de recepción: 03-ABR-2024 aceptación: 13-MAY-2024 publicación: 15-JUN-2024
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Con el avance de la inteligencia artificial y el surgimiento de nuevas formas de manipulación audiovisual, el fenómeno de los deepfakes pornográficos representa en la actualidad una amenaza inminente en el mundo digital. Ante esta realidad, la presente investigación buscó, desde un enfoque cualitativo y utilizando los métodos lógico, exegético, comparativo, de revisión bibliográfica y de casos, así como el hipotético-deductivo, responder a la interrogante de si será necesaria la configuración legal del tipo penal de deepfake pornográfico en la parte especial del Código Orgánico Integral Penal de Ecuador, con el fin de garantizar la seguridad ciudadana a través los principios de legalidad y tipicidad.

Los hallazgos obtenidos muestran que esta modalidad delictiva emergente necesita una respuesta legal eficaz que, además de sancionar a los infractores, permita reparar las graves consecuencias derivadas de estos actos y prevenir que nuevas vulneraciones sigan ocurriendo. Se evidencia así la urgencia de tipificar los deepfakes pornográficos como un delito específico dentro del ordenamiento jurídico ecuatoriano, dotando a las autoridades de herramientas sólidas hacer frente a esta forma de violencia sexual digital.

Palabras clave: Inteligencia artificial; Violencia digital; Regulación jurídica; Ciberdelito; Manipulación audiovisual

Abstract

With the advancement of artificial intelligence and the emergence of new forms of audiovisual manipulation, the phenomenon of pornographic deepfakes currently poses an imminent threat in the digital world. Faced with this reality, the present research sought, from a qualitative approach and using logical, exegetical, comparative, bibliographic review, and case methods, as well as the hypothetical-deductive method, to answer the question of whether it will be necessary to legally configure the crime of pornographic deepfake in the special part of the Ecuadorian Comprehensive Organic Criminal Code of Ecuador, in order to guarantee public safety through the principles of legality and typicity.

The findings obtained show that, indeed, this emerging criminal modality needs an effective and legal response that, in addition to sanctioning offenders, allows for the repair of the serious consequences derived from these acts and prevents further violations from occurring. This highlights the urgency of typifying pornographic deepfakes as a specific crime within the Ecuadorian legal system, providing authorities with solid tools to confront this form of digital sexual violence.

Keywords: Artificial intelligence; Digital violence; Legal regulation; Cybercrime; Audiovisual manipulation

Introducción

Las herramientas de inteligencia artificial (IA) surgieron con el propósito de simplificar la vida de las personas y brindar soluciones eficientes a una variedad de problemas. Inicialmente, se concibieron con un propósito en su mayoría positivo. No obstante, a medida que fueron evolucionando, se alejaron de esta idea original y empezaron a ser utilizadas de manera malintencionada.

De ahí que, la violencia sexual en la actualidad no se limita al ámbito presencial, sino que ha extendido sus raíces a dimensiones más allá de las convencionales, incorporando la tecnología y más específicamente, la inteligencia artificial. Dando lugar a nuevas modalidades delictivas dentro de las cuales se encuentra la conocida como "deepfake pornográfico".

En pocas palabras, el deepfake pornográfico se concreta mediante la utilización y manipulación de videos o imágenes de una persona, los cuales son cargados en un sistema de inteligencia artificial, todo esto con la intención de crear contenidos que implican desnudos u otras acciones de carácter sexual, sin que el individuo afectado haya participado en la producción de dicho material.

La creciente incidencia de esta nueva modalidad de ciberviolencia sexual es preocupante, ya que puede acarrear consecuencias negativas para quienes la sufren. Su impacto se magnifica aún más en Ecuador, donde se han registrado limitados avances en la regulación de delitos que tienen lugar directamente en el entorno digital, dejando así a las víctimas en un estado de total indefensión.

Ante tal escenario, el presente artículo tiene por objetivo abordar y analizar la problemática del deepfake pornográfico en el marco de la creciente influencia de la inteligencia artificial. En este sentido, se plantea la hipótesis de que una correcta tipificación del delito de deepfake pornográfico en la parte especial del Código Orgánico Integral Penal (COIP) de Ecuador contribuirá a garantizar la seguridad ciudadana mediante la aplicación de los principios de legalidad y tipicidad.

Por consiguiente, la importancia de investigar esta problemática radica en la necesidad de comprender a profundidad el fenómeno de los deepfakes pornográficos y la amenaza que representa el uso indebido de las inteligencias artificiales. A medida que su utilización y avance tecnológico se acelera, es crucial que se desarrollen mecanismos de prevención, regulación y respuesta efectiva. Esto permitirá salvaguardar los derechos, proteger de manera oportuna a las potenciales víctimas y a sentar bases legales sólidas para abordar estas cuestiones emergentes.

Aproximación al delito y tipo penal de deepfake pornográfico y su irrupción en la era de la inteligencia artificial

La sociedad contemporánea se encuentra inmersa en un constante proceso de transformación, caracterizado por la necesidad de realizar cambios en los diversos sectores, a fin mantenerse al ritmo de los avances tecnológicos. En este contexto, la inteligencia artificial (IA), siendo una disciplina científica de reciente incorporación, ha generado un impacto profundo en nuestra vida diaria, afectando no solo la manera en que interactuamos con la tecnología, sino también ejerciendo influencia en la forma en que nos comunicamos, trabajamos, tomamos decisiones, entre otros aspectos.

En términos generales, las inteligencias artificiales se constituyen como sistemas capaces de razonamiento y automatización de tareas intelectuales. Como indica Porcelli (2020), el propósito fundamental de la inteligencia artificial es desarrollar algoritmos capaces de resolver problemas cotidianos que los seres humanos enfrentan y resuelven de manera rutinaria (p. 57). De modo que, la esencia de esta tecnología radica en su habilidad para aprender, adaptarse y realizar funciones que tradicionalmente requerirían la intervención humana, ofreciendo de esta manera soluciones eficientes a una amplia gama de situaciones.

Sin lugar a dudas, la proliferación de las inteligencias artificiales y los programas diseñados para mejorar los diversos aspectos de nuestras vidas han generado numerosos beneficios. No obstante, es esencial reconocer que este avance también ha suscitado problemáticas emergentes que afectan de manera sustancial y que les conciernen a las ciencias jurídicas. Siendo que, dentro de estas cuestiones, destaca el fenómeno conocido como deepfake.

En sus inicios, los deepfakes se utilizaban con frecuencia con propósitos humorísticos, abarcando desde la esfera política hasta el entretenimiento, e incluso aspectos sentimentales. Sin embargo, con el transcurso del tiempo, su aplicación se ha extendido hacia esferas más complejas. Antes de profundizar en este tema, es fundamental definir qué se entiende por deepfake.

Si abordamos la cuestión desde una perspectiva lingüística se puede determinar a breves rasgos dicho fenómeno. La palabra deepfake se deriva de la combinación de dos vocablos en inglés: "deep" que es igual a profundo y "fake" que significa falso. Siendo que "deep" hace referencia al aprendizaje profundo o deep learning, que involucra la utilización de redes neuronales artificiales de distintos niveles para llevar a cabo tareas de análisis y procesamiento de información de manera avanzada. Por otro lado, "fake" se emplea para señalar que el producto de este tipo de aprendizaje consiste en la creación de contenido que aparenta ser auténtico, pero que en realidad es generado o manipulado.

Para ahondar más en la comprensión de la naturaleza de los deepfakes, es esencial hacer referencia a la investigación de Boté y Vállez (2022), quienes explican que estos combinan diversos tipos de contenido multimedia, como imágenes, videos y audios, entrelazándolos para fabricar videos falsos. Su propósito principal es engañar al espectador al manipular la apariencia o acciones de un individuo, e incluso generando animaciones completamente artificiales. Este proceso implica una personalización detallada mediante tecnología audiovisual avanzada que opera en múltiples niveles, tales como la reproducción facial, la modulación vocal, el sincronismo de labios y las posturas corporales (p. 26).

Con aquella definición, es posible deducir las características fundamentales de los deepfakes. Estos se constituyen como una meticulosa fusión de elementos multimedia que no solo alteran la apariencia visual, sino que también modifican aspectos sonoros como la voz, con el objetivo de capturar de manera verosímil tanto la dimensión auditiva como el habla específica de la persona.

Además, los deepfakes utilizan algoritmos de inteligencia artificial sofisticados llamados redes neuronales generativas adversarias (GANs) que permiten al sistema ingerir datos multimedia, entrenarse y generar contenido. Esta capacidad de perfeccionar la ilusión mediante la combinación de elementos visuales y auditivos contribuye a la creación de un producto final convincente y engañoso.

En este punto, conviene destacar que, si bien es cierto que antes del surgimiento de las inteligencias artificiales ya existían imágenes o videos adulterados y creados mediante programas informáticos, gran parte de estas manipulaciones eran ejecutadas por individuos con conocimientos especializados, limitando de esta forma su producción a una escala pequeña. No obstante, en la actualidad, la elaboración de deepfakes no requiere necesariamente un amplio dominio de la edición ni experiencia. En muchos casos, su creación se ha simplificado a un punto tal que puede llevarse a cabo con tan solo un clic a través de diversos servicios web, algunos de los cuales son gratuitos.

Es precisamente la relativa facilidad en la creación de deepfakes lo que ha propiciado que se extiendan más allá de su finalidad original. Uno de los usos más preocupantes es su aplicación en la producción de material íntimo de carácter sexual, conocido como deepfakes pornográficos. Estos utilizan inteligencia artificial para crear pornografía sintética usando como protagonistas a cualquier individuo cuyas imágenes personales, ya sean con ropa o sin ella, se encuentren disponibles en redes sociales (Gieseke, 2020). Esta cuestión no solo afecta a figuras públicas, como ocurrió en los primeros casos registrados en Reddit en 2017, sino también a cualquier individuo, quien podría convertirse en víctima.

Así, la creación de numerosos deepfakes pornográficos en los cuales aparecen personas realizando actos de naturaleza sexual que terceros podrían considerar verdaderos, aunque no

lo sean, nos sitúa en una época peligrosa. Cualquier individuo podría obtener estas imágenes o vídeos con el propósito de extorsionar a las víctimas, amenazando con hacer sexpreading, es decir, difundirlos públicamente si no cumplen con ciertas demandas. Así mismo, este tipo de prácticas se podría convertir en una herramienta poderosa para aquellos que buscan vengarse de sus ex parejas o lucrarse con dicho contenido pornográfico falso.

Tampoco se debe subestimar las devastadoras consecuencias que los deepfakes pornográficos pueden acarrear a las víctimas. Además del evidente daño psicológico y emocional, estas manipulaciones pueden derivar en una serie de trastornos graves, incluyendo ansiedad, depresión, una disminución significativa en la autoestima, entre otros.

En los casos más extremos, estas afecciones podrían incluso conducir a situaciones de riesgo como ideas o intentos de suicidio. En realidad, el impacto nocivo que generan estas manipulaciones con inteligencia artificial trasciende lo meramente pasajero o superficial, dejando cicatrices emocionales duraderas y profundas en las víctimas, afectando su bienestar integral y calidad de vida a largo plazo.

Además de lo anterior, los deepfakes pornográficos representan un grave peligro para la reputación e imagen de las víctimas. Dado que se tiende a otorgar mayor credibilidad a las evidencias visuales, existe un alto riesgo de que este material falso sea considerado verídico por la sociedad. Esto puede conducir a la estigmatización de los individuos implicados, con consecuencias significativas tanto en su vida personal como profesional. Puede afectar sus relaciones personales, oportunidades de trabajo e incluso exponerlos a situaciones de humillación, acoso y hostigamiento en diferentes entornos. Tal situación podría generar en las víctimas una sensación de vulnerabilidad y falta de control, pues deben afrontar las consecuencias a pesar de no haber incurrido en ninguna conducta reprochable.

Por estas razones, este novedoso método de manipulación audiovisual debe ser abordado desde una perspectiva jurídica, ya que se ha convertido en una amenaza delictiva de gran potencial, no solo en Ecuador, sino también a nivel mundial.

Casos emblemáticos de deepfake pornográfico a nivel internacional y en Ecuador

La utilización de los deepfakes pornográficos, en primer término, se originó para representar a celebridades realizando ciertas acciones de carácter sexual con el objetivo de generar entretenimiento de este nivel para el público. Nombres destacados en este ámbito incluyen a celebridades como Scarlett Johansson, Taylor Swift, Emma Watson y Megan Fox, quienes fueron falsamente representadas en cientos de videos e imágenes que se encuentran en el ciberespacio.

Sin embargo, en la actualidad la situación ha evolucionado, ya que no solo las celebridades son víctimas de esta práctica. Se han documentado numerosos casos en los que individuos comunes, así como figuras del ámbito político y social, han sido afectados por la generación de dicho contenido pornográfico falso. Una simple búsqueda de la palabra deepfake en la sección de noticias arroja diversos resultados que exponen la creciente prevalencia de esta problemática.

Ejemplos recientes destacan la experiencia de QTCinderella y Sweet Anita, dos streamers de Twitch que descubrieron imágenes y videos alterados en los que aparentaban ser las protagonistas, siendo comercializados en plataformas de suscripción mensual. Otro caso relevante es el de Nina Jankowicz, ex Directora Ejecutiva de la Junta de Gobernanza de Desinformación del Departamento de Seguridad Nacional de los Estados Unidos (DHS), quien se percató de la circulación de deepfakes pornográficos, en los que aparecía, a través de una alerta de Google. Jankowicz compartió su experiencia en el artículo "No debería tener que aceptar estar en pornografía deepfake", denunciando el impacto negativo que tuvo en su vida y criticando a los políticos que ignoran esta problemática urgente.

Greta Thunberg, la activista sueca, también fue víctima de una grabación pornográfica falsa de dieciséis segundos que se viralizó en varias redes sociales y páginas web. Sobre esto, muchos argumentan que fue difundido con la intención de menoscabar su compromiso contra el calentamiento global. Otro ejemplo destacado es el de una estudiante universitaria de 23 años que, en 2020, descubrió deepfakes pornográficos de ella en Facebook. A pesar de denunciar la situación, las leyes en su país carecían de regulaciones específicas, lo que la llevó a emprender su propia investigación. Descubrió que no era la única víctima en su comunidad universitaria, y su historia inspiró el documental "Otro Cuerpo", donde se protege su identidad mediante un alias.

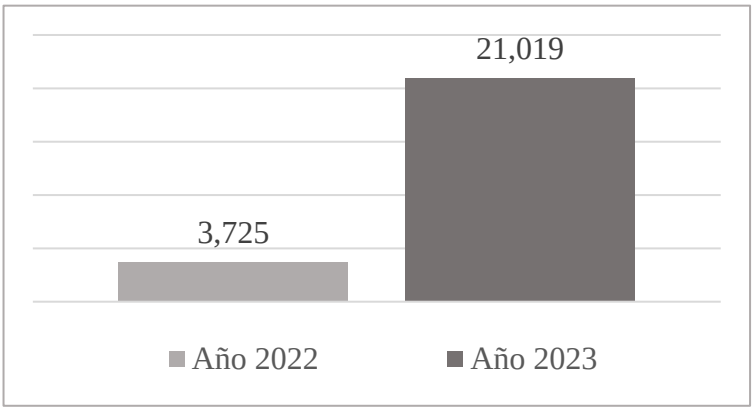
En Ecuador, uno de los casos más destacados se desenvolvió en un colegio de la capital, donde dos estudiantes fotografiaron a compañeras y estudiantes de otros niveles. Ellos utilizaron esas imágenes para crear contenido de naturaleza sexual, que incluía alrededor de setecientas imágenes y videos. Este material fue difundido ampliamente dentro de la institución educativa, exponiendo a las estudiantes afectadas a la situación. Como consecuencia, los padres de las adolescentes presentaron una denuncia formal ante la Fiscalía General del Estado, cuyo proceso judicial está próximo a desarrollarse.

Estos casos son solo ejemplos de una problemática que parece no tener fin. Las cifras revelan que este tipo de situaciones van en aumento, producto del mayor acceso a estas herramientas de manipulación de imágenes y videos. Según el informe "Estado de los Deepfakes 2023: Realidades, amenazas e impacto", esta forma de manipulación audiovisual ha experimentado un alarmante incremento del 464% en comparación con años anteriores. Siendo el 2023 un

año récord en la producción de videos de deepfake pornográfico (Home Security Heroes, 2023).

Figura 1

Número de pornografía deepfake

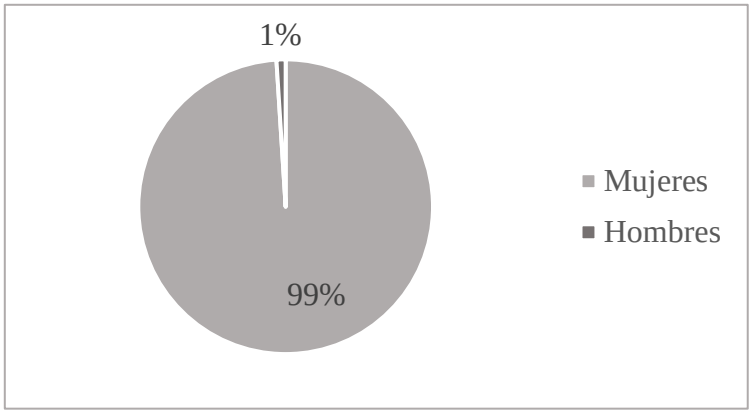


Fuente: Elaboración propia con base a los datos de Home Security Heroes, 2023.

Además, según los datos de dicho informe, se evidencia que las mujeres son el blanco más vulnerable y atacado por esta modalidad, representando el mayor porcentaje de víctimas (Home Security Heroes, 2023).

Figura 2

Tendencia de deepfakes pornográficos por género en el año 2023



Fuente: Elaboración propia con base a los datos de Home Security Heroes, 2023.

Ante las evidencias presentadas, resulta innegable que el género femenino se encuentra mayormente afectado por la problemática de los deepfakes pornográficos. El hecho de que gran parte de este tipo de contenido esté centrado en ellas refleja una realidad preocupante de desigualdad de género. Esta situación no solo perpetúa estereotipos perjudiciales y

contribuye a la objetualización y cosificación de las mujeres, sino que además permite que se sigan fomentando conductas misóginas y normalizando la violencia sexual en los entornos virtuales.

Es preciso indicar que, si bien los datos expuestos no eximen a los hombres de ser víctimas de esta forma de manipulación digital, ya que cualquier individuo es susceptible a ello, es más frecuente encontrar este tipo de contenido enfocado en mujeres. Esto posiblemente como una manifestación de la persistente discriminación y opresión hacia el género femenino que enfrentan en los diversos ámbitos de la sociedad.

A la luz de estos hechos, se pone de manifiesto una vez más la necesidad de abordar la problemática desde un enfoque jurídico y de perspectiva de género, pues no se debe subestimar las diversas consecuencias negativas que acarrean los deepfakes pornográficos y aún más si consideramos que en muchas ocasiones, resulta difícil eliminar por completo las imágenes que se encuentran en la red.

Estudio comparado internacional sobre el tratamiento legal del delito de deepfake pornográfico: Lecciones aprendidas

En los últimos años, se ha observado un creciente interés en las conductas derivadas del uso de las tecnologías, un hecho que se refleja en el fortalecimiento de los marcos jurídicos a nivel nacional e internacional. En este contexto, la capacidad de las inteligencias artificiales para llevar a cabo acciones que bordean la ilegalidad ha generado inquietud y se ha convertido en tema recurrente de debates.

Uno de los primeros países en abordar jurídicamente la creciente problemática de los deepfakes pornográficos fue Estados Unidos. Aunque es relevante destacar que a nivel federal han existido diversos intentos de regular este fenómeno, como la Ley de Prohibición de Deepfakes Maliciosos de 2018 - S.3805 y la Ley de Responsabilidad de Deepfakes de 2019 - H.R.3230, ninguno ha tenido éxito, lo que ha dejado en gran medida la responsabilidad en manos de los Estados.

Para ser más precisos, en California se promulgó la Ley de la Asamblea 602, la cual establece que cualquier persona que divulgue material explícito modificado sin el consentimiento de la persona representada en dicho contenido será sancionada económicamente. La sanción impuesta oscilará entre al menos $1,500 y no más de $30,000 dólares americanos. Sin embargo, en caso de que la acción se haya realizado con malicia, la sanción puede ascender hasta $150,000 dólares americanos. Además de las sanciones económicas, también se pueden imponer daños punitivos, honorarios y costos de abogados, así como la aplicación de medidas cautelares para proteger a la víctima (Assembly Bill 602, 2019).

Así también, Nueva York ha promulgado Ley del Senado S5959D, la cual, en su segunda parte, establece un significativo avance en la protección de los derechos de las víctimas de deepfakes pornográficos que han sido divulgados sin su consentimiento. La norma les otorga el derecho a emprender acciones legales privadas, reforzando la protección de sus derechos individuales relacionados con su nombre y reputación, mediante la imposición de reparaciones económicas según cada caso. Las reclamaciones deben presentarse en un plazo máximo de 3 años desde la publicación del material sexual, pero este plazo se reduce a 1 año después de que la víctima descubra la divulgación del contenido explícito (Senate Bill S5959D, 2019).

De igual forma, en Virginia se implementaron sanciones rigurosas en relación con la problemática del deepfake pornográfico. Estas modificaciones afectaron secciones específicas de la legislación penal, concretamente los artículos 18.2-386.1 y 18.2-386.2. Dichas disposiciones prohíben la creación, comercialización o distribución sin licencia de imágenes o videos generados mediante inteligencia artificial en los cuales una persona sea representada realizando actos de naturaleza sexual, sin el previo consentimiento del individuo afectado. Así bien, tales acciones son consideradas delitos de Clase 1, lo que implica que la penalización puede alcanzar un máximo de doce meses de privación de libertad y una multa de hasta $2,500 dólares americanos (Code of Virginia, 2019).

Finalmente, otro Estado que ha tomado medidas en contra de este fenómeno es Georgia, que enmendó la Parte 3 del Artículo 3 del Capítulo 11 del Título 16 del Código Oficial. Esta modificación se llevó a cabo con el propósito de incorporar la prohibición de transmitir o publicar imágenes de desnudez o conducta sexualmente explícita de un adulto, abarcando tanto imágenes videográficas reales como las falsificadas. Bajo esta enmienda, la sanción se categoriza como delito menor de índole alta o grave, con condenas que varían desde uno hasta cinco años de privación de libertad. Así mismo, se contempla la imposición de una multa que podría alcanzar hasta los $100.000 dólares americanos, pudiendo aplicarse ambas sanciones según las circunstancias del caso (Code of Georgia, 2022).

A diferencia de Estados Unidos, en Corea del Sur existen disposiciones a nivel nacional que regulan el fenómeno del deepfake pornográfico. La Ley de Prevención de la Violencia Sexual en su artículo 14 inciso 2 establece que cualquier individuo que, distribuya, edite o sintetice material visual con el propósito de suscitar deseo sexual o vergüenza en contra de la voluntad de la víctima del material, será sancionado con una pena de prisión de hasta cinco años o una multa de hasta 50 millones de wones. Esta pena se incrementará a siete años si se utilizan las redes de información para cometer el delito y se aumentará hasta la mitad en caso de reincidencia (Seongbogryeok cheobolbeo, 2023).

Así mismo, en China los esfuerzos por regular el fenómeno de deepfake pornográfico han sido varios, destacando el Reglamento para la Gestión Profunda de los Servicios de Información en Internet. Esta normativa exige obtener consentimiento previo para compartir contenido generado por inteligencia artificial, así como incluir una marca de agua que indique la edición del material. Además, los proveedores de servicios de generación de contenido deben comprometerse a no procesar información personal y cumplir con reglas como la evaluación de algoritmos, autenticación de usuarios y transparencia en la creación de videos.

Los infractores de estas disposiciones pueden enfrentar penas privativas de libertad, determinadas según la gravedad de los hechos y el daño causado. Adicionalmente, las víctimas tienen la opción de iniciar procesos civiles para obtener compensaciones por los perjuicios sufridos (Reglamento para la Gestión Profunda de los Servicios de Información en Internet (Hùliánwǎng xìnxī fúwù shēndù héchéng guǎnlǐ guīdìng, 2022).

Como se ha podido observar, la problemática asociada al deepfake se aborda de diferentes maneras en las legislaciones jurídicas objeto de análisis. Algunas de estas normativas catalogan el deepfake pornográfico como una infracción de menor gravedad, sancionándola mediante la imposición de multas, mientras que otras adoptan una postura más severa, calificándolo como un delito que conlleva tanto una pena privativa de libertad como una sanción monetaria.

Se debe notar también que los países del continente asiático están más avanzados en el tratamiento de esta problemática, abordándola no solo desde la perspectiva del individuo que comete la acción, sino también involucrando a terceros. Esto podría deberse a que están mucho más avanzados en el desarrollo tecnológico que otros países. Con todo, es claro que las sanciones implementadas tienen como objetivo no solo mitigar este tipo de actos, sino también reducir las consecuencias asociadas.

De igual forma, ha de tenerse presente que, pese a que parecen escasos los intentos de tipificar el deepfake pornográfico, los ejemplos mencionados anteriormente constituyen solo una parte del panorama. Diversos países han iniciado la implementación de medidas para hacer frente a los desafíos que plantea esta nueva modalidad, aunque estas acciones se encuentran aún en sus primeras etapas.

A nivel supranacional, se encuentra la legislación de la Unión Europea sobre Inteligencia Artificial, cuyo objetivo principal es regular que los sistemas de inteligencia artificial sean utilizados de manera confiable y segura, respetando los derechos fundamentales de las personas y evitando los factores de riesgo a los que podrían estar expuestas. Este marco normativo, que regirá en varias jurisdicciones, se espera que se establezca de manera estándar en los próximos años.

Así también, a nivel individual, se han propuesto varias medidas de regulación jurídica. En concreto, en España se ha propuesto un proyecto de Ley Orgánica destinado a regular las simulaciones de imágenes y voces de personas generadas mediante inteligencia artificial. Este proyecto contempla reformas en diversas leyes existentes, incluyendo el Código Penal. Un caso similar es el de México, donde se presentó un proyecto para reformar el Código Penal, cuyo propósito es sancionar con penas de dos a ocho años de prisión a aquellas personas que, mediante inteligencia artificial, modifiquen videos o audios con el objetivo de perjudicar la moral.

Además de los países mencionados, otras naciones, como Alemania, Canadá, Chile, India y el Reino Unido, también están considerando la adopción de medidas similares, con el fin de fortalecer sus estructuras legales y salvaguardar a sus ciudadanos ante el potencial uso indebido de esta innovadora tecnología. Todo esto es crucial, dado que refleja el creciente reconocimiento a nivel mundial de la importancia de abordar jurídicamente los deepfakes pornográficos.

Tabla 1

Comparativa internacional de marcos jurídicos sobre deepfake pornográfico

País	Región Estado	Marco legal	AÑO	Clasificación jurídica	Sanción
Estados Unidos	California	Ley de la Asamblea 602	2019	Infracción	Multas económicas que conllevan daños punitivos y honorarios
	Nueva York	Ley del Senado S5959D	2019	Infracción	Multas económicas determinadas conforme al caso
	Virginia	Código Penal, Artículos 18.2-386.1 y 18.2-386.2	2019	Delito de Clase 1	Pena privativa de libertad de hasta un año y multa de hasta $2.500
	Georgia	Código Oficial, Parte 3 del Artículo 3, Capítulo 11, Título 16	2022	Delito de índole alta o grave	Pena privativa de libertad de uno a cinco años y multas de hasta $100.000
Corea del Sur	Nacional	Ley de Prevención de la Violencia Sexual Art. 14.2	2023	Delito	Pena privativa de libertad de hasta siete años y multa de hasta ₩50,000,000

China	Nacional	Reglamento para la Gestión Profunda de los Servicios de Información en Internet	2022	Delito	Penas privativas de libertad según la gravedad del perjuicio y compensaciones civiles

Fuente: Elaboración propia.

Material y métodos

En el presente estudio se optó por una metodología de carácter cualitativo para profundizar en la problemática del deepfake pornográfico. Para tal propósito, se recurrió a diversas técnicas y enfoques metodológicos.

En primera instancia, se acudió al método lógico, el cual posibilitó determinar la trascendencia que ha adquirido la inteligencia artificial en el escenario global actual, así como el alcance de la modalidad delictiva del deepfake pornográfico. Este abordaje sentó las bases para comprender la magnitud y el impacto de dicho fenómeno.

De manera complementaria, se efectuó una exhaustiva revisión documental y un análisis minucioso de casos emblemáticos relacionados con el deepfake pornográfico, tanto en el ámbito nacional como internacional. Dicha revisión abarcó artículos académicos, estudios especializados e informes técnicos, lo que permitió vislumbrar las implicaciones jurídicas y sociales de esta modalidad digital, además de determinar su nivel de incidencia delictiva y propagación.

A su vez, uno de los pilares metodológicos fue la aplicación de los enfoques exegético y comparativo. A través del primero, se examinaron detalladamente los distintos marcos normativos y jurisdicciones que abordan el deepfake pornográfico a escala global. Por su parte, el enfoque comparativo posibilitó identificar similitudes, diferencias y perspectivas adoptadas por diferentes naciones, brindando una visión panorámica sobre el tratamiento legal de este fenómeno. Con esto se pudo resaltar buenas prácticas y lecciones aprendidas en diversos contextos.

Finalmente, se recurrió al método hipotético-deductivo, planteando la hipótesis de que una adecuada tipificación del delito de deepfake pornográfico en el Código Orgánico Integral Penal (COIP) garantizaría la seguridad ciudadana mediante la aplicación efectiva de los principios de legalidad y tipicidad. Esta hipótesis fue sometida a prueba a través de la investigación realizada.

Resultados y discusión

Es innegable que los deepfakes pornográficos representan una amenaza creciente que causa un daño significativo a las víctimas y produce consecuencias devastadoras. Prueba de ello son los casos previamente expuestos y las acciones tomadas por las diferentes jurisdicciones para frenar su proliferación masiva. Ante esta preocupante realidad surge la interrogante: ¿Será necesaria una configuración legal del tipo penal de deepfake pornográfico en la parte especial del Código Orgánico Integral Penal (COIP) de Ecuador para garantizar la seguridad ciudadana en virtud de los principios de legalidad y tipicidad?

Para responder a esta cuestión, es crucial considerar varios aspectos fundamentales. Si bien algunos sectores podrían argumentar que no es necesaria una regulación penal específica sobre los deepfakes pornográficos, bajo el supuesto de que los tipos penales vigentes podrían adecuarse a estas nuevas modalidades delictivas virtuales, no podemos ignorar que en este punto, nuestro ordenamiento jurídico no brinda una protección adecuada a las personas cuyas imágenes o videos de índole sexual han sido creados o manipulados mediante inteligencia artificial y luego distribuidos sin su consentimiento.

Bajo este panorama, una regulación jurídica clara y actualizada sobre los deepfakes pornográficos permitiría a Ecuador anticiparse a esta nueva forma de violencia digital, pues el país ya se encuentra inmerso en esta ola. Al reconocer que la violencia evoluciona y busca nuevas formas de ejercer control, es responsabilidad de las autoridades públicas implementar medidas políticas y legales apropiadas para prevenir su manifestación (Simó Soler, 2023).

Adicionalmente, es importante destacar que en la práctica jurídica ecuatoriana se observa una tendencia preocupante de subsumir varios hechos en las infracciones jurídicas existentes, aun cuando estos no cumplen con todos los elementos que las caracterizan. Este enfoque conlleva a una interpretación extensiva de la ley y pone en peligro principios fundamentales como la legalidad, la tipicidad y la seguridad ciudadana.

Como bien señalan Robles-Lessa et al. (2020) la actuación de los deepfakes en el ciberespacio clama por una regulación legal específica que garantice la seguridad de lo que se divulga a la sociedad a través de Internet, que es una herramienta habitual presente en la vida cotidiana de la comunidad mundial, se diría incluso indispensable en la contemporaneidad (p. 485). Por lo tanto, es crucial que Ecuador aborde de manera directa y precisa esta modalidad de manipulación audiovisual mediante un marco normativo adecuado.

Dilucidado esto, es pertinente abordar qué criterios deben tenerse en cuenta al diseñar y proponer un tipo penal para los deepfakes pornográficos. Resulta necesario considerar que algunos de ellos, en virtud de su elevado nivel de sofisticación técnica y los procedimientos

empleados en su elaboración, logran un grado de verosimilitud mucho más convincente para la percepción humana en comparación con otros. Tal es el caso de los denominados "shallowfakes", que constituyen deepfakes pornográficos de naturaleza menos realista, en los cuales el carácter artificioso o falso resulta evidente a simple vista.

En lo concerniente a estos últimos, cabe preguntarse si deberían estar regulados de la misma manera que el resto de deepfakes pornográficos. Para responder a esto, habría que considerar que los shallowfakes si bien por su propia naturaleza pueden no resultar tan persuasivos para la sociedad, el mero hecho de su existencia y la intención subyacente detrás de su creación, que es exhibir a individuos en actos sexuales sin su consentimiento, es motivo suficiente para que todos los deepfakes pornográficos, sin distinción alguna, sean susceptibles de penalización jurídica. Esto en razón de que, aun cuando su falta de realismo sea evidente, su sola presencia puede ocasionar humillaciones, menoscabo a la dignidad y otras consecuencias perjudiciales para las víctimas representadas.

Otra cuestión de suma importancia radica en que hoy por hoy, existen sofisticados sistemas de inteligencia artificial que una vez entrenados posibilitan la generación íntegra de un cuerpo falso a partir de la imagen facial auténtica de una persona, con el objeto de simular su participación en actos de naturaleza sexual. Así mismo, estas tecnologías permiten realizar mixturas entre rostros verdaderos o manipulados y cuerpos reales, propios o ajenos, retratando de igual manera a los individuos involucrados en conductas de carácter sensible. En este último supuesto, surge la compleja interrogante de determinar qué sujeto o sujetos ostentarían legitimación activa para efectuar las acciones legales pertinentes: si la persona cuyo rostro es exhibido, si aquella a cuyo cuerpo se alude dentro de la manipulación, o bien ambas.

En este sentido, el Tribunal Supremo de Suiza abordó la cuestión de la identificabilidad en el fallo 5A_553/2012 del 14 de abril de 2014, un caso relacionado con fotomontajes. El tribunal determinó que el rostro es uno de los rasgos más distintivos, por lo que no basta con que la persona se reconozca a sí misma, sino que debe ser identificable por otros individuos. Considerando esto, podría conferirse la aptitud para activar los mecanismos de tutela jurídica a quienes puedan verse perjudicados por tales conductas, es decir, cuando la representación de la persona dentro del deepfake pornográfico sea susceptible de identificación por otros. Sin embargo, esta cuestión debe analizarse detenidamente al momento de su regulación jurídica, con el fin de respetar todos los derechos fundamentales involucrados de manera equilibrada.

Una vez resueltas dichas incertidumbres, es pertinente abordar la inclusión explícita de los deepfakes pornográficos en el Código Orgánico Integral Penal (COIP). Se vislumbran dos vías posibles: la primera, integrarla en conjunto con una regulación ya existente; y la segunda,

crear un tipo penal específico que se dedique de forma exclusiva a esta manifestación derivada de la inteligencia artificial. En cualquier caso, es indispensable que su regulación se encuentre enmarcada dentro de los delitos contra la integridad sexual y reproductiva o dentro de los delitos contra el derecho a la intimidad personal y familiar.

Ahora bien, en lo que concierne a la determinación de la pena a imponer a los infractores de deepfake pornográfico, ésta deberá guardar la debida proporcionalidad y coherencia sistemática con otros ilícitos de similar entidad contemplados en nuestra norma penal actual, atendiendo a la gravedad de las conductas, las consecuencias que éstas generan en los bienes jurídicos tutelados y las eventuales circunstancias agravantes que pudieren concurrir, como la condición de persona vulnerable de la víctima.

A su vez, deviene indispensable que la regulación atienda a los diversos eslabones de la cadena delictiva involucrada. Podría darse el caso de que la persona que crea la imagen o video de índole sexual manipulado mediante inteligencia artificial sea distinta a aquella que proceda a su carga y distribución en diversos medios y plataformas. Por lo tanto, al establecer el marco normativo de este delito, se deberá analizar si las acciones de creación y de compartir los deepfakes pornográficos serán sancionadas de la misma forma o tendrán penas diferenciadas.

En definitiva, una propuesta normativa para la tipificación del delito de deepfake pornográfico en nuestro ordenamiento jurídico deberá responder a todos los supuestos previamente expuestos, pues de esta forma se podrá conformar una visión integral del problema que supone esta modalidad delictiva virtual y, a su vez, de las consecuencias negativas que se generan en la actualidad y se prevén en los próximos años.

A su vez, la regulación específica de la modalidad delictiva de los deepfakes pornográficos representaría un avance transcendental en el combate contra la violencia sexual en el entorno digital y la protección de los derechos de las víctimas. Al introducir un tipo penal que recepcione de manera expresa esta particular acción, se proveería a los operadores de justicia de un instrumento legal robusto y contundente para emprender acciones persecutorias y aplicar sanciones de forma efectiva.

No obstante, es menester enfatizar que abordar esta problemática no puede limitarse únicamente a una respuesta de carácter jurídico, sino que se requiere la articulación coordinada de diversos sectores tales como el tecnológico, educativo, psicológico, entre otros. Ello con el fin de que, además de contar con un marco normativo que sancione de manera efectiva el ilícito, se puedan desarrollar estrategias integrales y multidisciplinarias que permitan prevenir la proliferación de estas conductas delictivas, al tiempo que se brinde apoyo integral y protección adecuada a las víctimas desde un enfoque de derechos humanos.

Por consiguiente, se vuelve imperativo implementar políticas estrictas y articular acciones a fin de prevenir la proliferación de deepfakes pornográficos en redes sociales y sitios web. Por ello, es necesario el desarrollo e implementación de tecnologías avanzadas de detección de contenido manipulado, que permitan remover de manera efectiva este tipo de materiales del ciberespacio, evitando así la revictimización constante de las personas afectadas. Así mismo, es preciso desplegar campañas de concientización y educación digital que alerten sobre los riesgos y consecuencias de estas prácticas, fomentando un uso ético y responsable de las nuevas tecnologías.

Para finalizar, además de todo lo mencionado, resulta indispensable la capacitación de los distintos profesionales del sistema judicial, como jueces y fiscales, en el manejo de estos nuevos desafíos, puesto que de nada servirá una norma que proteja a las víctimas ante esta nueva problemática, cuando los encargados de aplicarla carezcan de los conocimientos y herramientas necesarias para abordar adecuadamente estos casos complejos en el contexto del mundo globalizado actual.

Conclusiones

Debido al acelerado avance tecnológico y la creciente sofisticación de las inteligencias artificiales, han surgido diversas modalidades delictivas que suponen una grave amenaza para los derechos fundamentales y la integridad sexual de las personas. El fenómeno de los deepfakes pornográficos representa, sin duda alguna, uno de los desafíos más inquietantes y complejos que enfrenta la sociedad en la actualidad. Sus efectos devastadores sobre las víctimas son prácticamente irreparables, pues se trata de una problemática novedosa y cambiante para la cual aún no se cuenta con un marco jurídico sólido y una respuesta legal efectiva, dejando a quienes lo sufren en un estado de total vulnerabilidad e indefensión.

Lo que resulta aún más preocupante es el incremento exponencial de casos de deepfakes que se constata tanto a nivel nacional como global, alimentado por cada nueva interacción en línea. Sobre esto, es particularmente alarmante que el contenido manipulado mediante deepfakes afecte de manera desproporcionada al género femenino, convirtiéndolo en el colectivo más vulnerable frente a esta práctica que representa una forma de opresión y cosificación contra las mujeres, perpetuando así la discriminación y violencia de género que han sufrido durante siglos.

Ante la cruda realidad que esto representa, diversas naciones han implementado regulaciones específicas a nivel estatal y federal con el objetivo de prevenir y sancionar estas conductas ilícitas en el entorno cibernético. Dichas regulaciones centran su atención tanto en los infractores como en los servicios que permiten crear y difundir este tipo de contenido manipulado.

Por ello, tomando en consideración que Ecuador también se ve afectado por este fenómeno y que requiere proteger de manera efectiva los derechos de las víctimas, así como avanzar en

la lucha contra los delitos digitales, resulta imprescindible contar con una regulación jurídica sobre los deepfakes pornográficos dentro del Código Orgánico Integral Penal (COIP). De esta manera, se dotaría a los operadores jurídicos del país de herramientas sólidas para afrontar esta modalidad delictiva digital de forma contundente.

Sin embargo, no basta con una regulación punitiva. Se necesita un enfoque multidisciplinario que involucre políticas públicas integrales, educación digital y un profundo conocimiento de las dinámicas tecnológicas, con el fin de superar esta agresión digital que parece no tener fin y que amenaza con agravar aún más la brecha de género ya existente.

Referencias bibliográficas

Asamblea Nacional del Ecuador. (2014, 10 de febrero). Código Orgánico Integral Penal. Registro Oficial del Gobierno del Ecuador No.180. https://www.lexis.com.ec/biblioteca/coip

Assembly Bill No. 602 [Ley de la Asamblea No. 602], 2019, (Estados Unidos). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

Bañuelos Capistrán, J. (2020). Deepfake: la imagen en tiempos de la posverdad. Revista Panamericana de Comunicación, 2(1), 51-61. https://www.redalyc.org/pdf/6649/664970407007.pdf

Boté, J., y Vállez, M. (2022). Aplicaciones de DeepFakes.: manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad. Revista Complutense de Educación, 45(1), 25-32. https://dialnet.unirioja.es/servlet/articulo?codigo=8253826

Code of Georgia [Código de Georgia]. [CG]. §§ 16-11-90 — 16-11-92, 1981 (Estados Unidos). https://n9.cl/jrw9n

Code of Virginia [Código de Virginia], [VA Code], § 18.2-386.2, 1919, (Estados Unidos). https://n9.cl/nmon6

Gieseke, A. P. (2020). "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography ["La Nueva Arma de Elección": La Actual Incapacidad de la Ley para Abordar Adecuadamente la Pornografía Deepfake]. Vanderbilt Law Review, 73, 1479-1515. https://n9.cl/ku4g6

González-Véliz, C., & Cuzcano-Chavez, X. (2024). Desafíos y dimensiones de la desinformación en ALAC deepfakes y la urgencia de proteger los derechos de las mujeres. ResearchGate. https://n9.cl/l5q1e

Home security heroes. (2023). 2023 State of Deepfakes: Realities, threats, and impact [Estado de Deepfakes 2023: Realidades, amenazas e impacto]. https://www.homesecurityheroes.com/state-of-deepfakes/#key-findings

Hùliánwǎng xìnxī fúwù shēndù héchéng guǎnlǐ guīdìng [Reglamento para la Gestión Profunda de los Servicios de Información en Internet], 11 de diciembre de 2022 (China). https://n9.cl/8fq8d

Martínez, V. C., y Castillo, G. P. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. Historia y Comunicacion Social, 24(2), 505-520. https://doi.org/10.5209/hics.66293

Porcelli, A. (2020). La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos. Derecho global. Estudios sobre derecho y justicia, 6(16), 49-105. https://doi.org/10.32870/dgedj.v6i16.286

Pulido, I. G. (2023). El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes. Ius Et Scientia, 2(9), 157-180. https://doi.org/10.12795/iestscientia.2023.i02.08

Robles-Lessa, M., Boechat Cabral, T., y Fachetti Silvestre, G. (2020). Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço [Deepfake: inteligencia artificial y algoritmo que causa riesgos a la sociedad en el ciberespacio]. Derecho y Cambio Social, 61, 475-487. https://dialnet.unirioja.es/servlet/articulo?codigo=7525024

Senate Bill S5959D [Ley del Senado S5959D], 2019, (Estados Unidos). https://www.nysenate.gov/legislation/bills/2019/S5959

Seongbogryeok cheobolbeo [Ley de Prevención de la Violencia Sexual], [Ley No. 19743], 24 de octubre de 2023, (Corea del Sur). https://www.law.go.kr/법령/성폭력범죄의처벌등에관한특례법

Simó Soler, E. (2023). Retos jurídicos derivados de la Inteligencia Artificial Generativa: Deepfakes y violencia contra las mujeres como supuesto de hecho. InDret Criminología, 493-515. https://doi.org/10.31009/InDret.2023.i2.11

Tribunal Supremo de Suiza (2014, 14 de abril). Sentencia No. 5A_553/2012. (Suiza). https://perma.cc/BX37-4QYT

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.