ISSN 2953 - 6421

Deepfakes Pornográficos: Impacto jurídico-probatorio y social en el Ecuador

Pornographic Deepfakes: Legal-evidential and social impact in Ecuador

Para citar este trabajo:
Sinaluisa, F., Romero, W., y Freire, N., (2024) Deepfakes Pornográficos: Impacto jurídico- probatorio y social en Ecuador. *Reincisol*, 3(6), pp. 2912-2934. https://doi.org/10.59282/reincisol.V3(6)2912-2934

Autores:

Franklin Geovanny Sinaluisa Sagñay
Universidad Nacional de Chimborazo
Ciudad: Riobamba, País: Ecuador
Correo Institucional: franklin.sinaluisa@unach.edu.ec
Orcid https://orcid.org/0009-0001-8040-8086

Wendy Pilar Romero Noboa
Universidad Nacional de Chimborazo
Ciudad: Riobamba, País: Ecuador
Correo Institucional: wendy.romero@unach.edu.ec
Orcid https://orcid.org/0009-0007-3579-2588

Nelson Franciso Freire
Universidad Nacional de Chimborazo
Ciudad: Riobamba, País: Ecuador
Correo Institucional: nffreire@unach.edu.ec
Orcid https://orcid.org/0009-0006-6747-1140

RECIBIDO: 29 agosto 2024 **ACEPTADO**: 29 septiembre 2024 **PUBLICADO:** 2 octubre 2024

Resumen

Los “Deepfakes” pornográficos representan un fenómeno creciente de videos o imágenes falsificados generados por inteligencia artificial, es el resultado directo de los avances tecnológicos, trasgrediendo de manera directa al derecho a la intimidad, con la generación de videos de contenido sexual sin consentimiento de la víctima. Estas manipulaciones iniciaron en el año de 2017, fueron evolucionando provocando riesgos legales inherentes en particular con los derechos de intimidad de las mujeres. El estudio se realizó con un método investigación, de enfoque cualitativo, de tipo documental, bibliográfico, dogmática, descriptiva, comparativo que contiene un diseño no experimental. Se enfoca, en comparar legislaciones diversas y así comprender las dificultades probatorias y desafíos jurídicos contemporáneos en Ecuador, pues esto representa un obstáculo legal y conlleva graves consecuencias en el futuro. En los hallazgos encontrados se establece que efectivamente los “deepfakes” vulnera el derecho a la intimidad, afectando la privacidad de las personas y su reputación, así también se resalta la dificultad probatoria, la cual plantea desafíos significativos para identificar el origen y atribución de responsabilidad, debido a escasa normativa ecuatoriana, y la falta de peritos especializados en la IA, lo cual resáltala necesidad urgente de abordar esta problemática desde un punto de vista legal y tecnológico.

Palabras claves: Deepfake pornográfico; Derecho de intimidad; Pornografía; Víctimas mujeres; Pornografía no consensuada; Inteligencia artificial.

Abstract

Pornographic “Deepfakes” represent a growing phenomenon of falsified videos or images generated by artificial intelligence, is the direct result of technological advances, directly transgresses the right to privacy, with the generation of videos of sexual content without the consent of the victim. These manipulations started in the year of 2017, were evolving causing inherent legal risks in particular with the privacy rights of women. The study was conducted with a research method, qualitative approach, documentary, bibliographic, dogmatic, descriptive, comparative containing a non-experimental design. It focuses on comparing different legislations in order to understand the evidentiary difficulties and contemporary legal challenges in Ecuador, since this represents a legal obstacle and entails serious consequences in the future. The findings establish that “deepfakes” indeed violate the right to privacy, affecting the privacy of individuals and their reputation, as well as highlighting the evidentiary difficulty, which poses significant challenges to identify the origin and attribution of responsibility, due to scarce Ecuadorian regulations, and the lack of specialized experts in AI, which highlights the urgent need to address this issue from a legal and technological point of view.

Keywords: Pornographic deepfake; Privacy rights; Pornography; Female victims; Non-consensual pornography; Artificial Intelligence.

INTRODUCCIÓN

El término "Deepfake" se origina en Hollywood en el año 2017, siendo un acrónimo de "Fake" (falso) y "Deep" (profundo). Los vídeos producidos mediante la utilización de inteligencia artificial, que emplean algoritmos para crear secuencias audiovisuales inventadas y superponer digitalmente el rostro de una persona al cuerpo de otra persona en un vídeo sexualmente explícito (Somers, 2020) representan un problema importante.

Estos vídeos muestran a personas realizando acciones que no infringen el derecho a la privacidad; sin embargo, cuando se utilizan en contextos perjudiciales, como el contenido pornográfico manipulado que se difunde en Internet, aproximadamente el 96% de las víctimas son mujeres. En consecuencia, dentro del marco legal de Ecuador, existe una deficiencia en las regulaciones diseñadas para sancionar a las personas responsables de la producción de «Deepfakes» pornográficos.

El derecho a la privacidad, es un derecho fundamental protegido por las disposiciones constitucionales sin embargo, se encuentra en peligro debido a los continuos avances de la tecnología, en particular de la inteligencia artificial. La preocupación principal radica en las violaciones del derecho a la privacidad en las que incurren quienes difunden información auténtica (Martínez, 2000).

Para abordar esta cuestión es necesario realizar un examen jurídico y social exhaustivo de los «Deepfakes» y sus repercusiones en la vida personal de las víctimas. Este documento profundiza en los desafíos desde una perspectiva legal, analizando casos reales y haciendo comparaciones con los sistemas legales de otras jurisdicciones. La aparición de las copias falsas con contenido pornográfico representa un enorme desafío para los marcos legales y legislativos de Ecuador, y ha suscitado investigaciones críticas sobre la legalidad de estas prácticas tecnológicas novedosas, la ausencia de medidas reguladoras eficaces que regulen las «falsificaciones profundas» y las complejidades asociadas a la recopilación de pruebas digitales. Estos factores plantean impedimentos legales, lo que complica la determinación de la autenticidad del contenido y la responsabilidad del autor. El objetivo principal de esta investigación es comprender estas implicaciones y

proponer vías para reformar el Código Orgánico Integral Penal (COIP) en relación con este fenómeno.

Es imperativo explorar cómo otros sistemas legales abordan este tema para evaluar su viabilidad en el contexto ecuatoriano. La percepción pública también ejerce una influencia considerable en la formulación de leyes que salvaguarden la privacidad, lo que refuerza los argumentos en contra de los vídeos o imágenes manipulados. Los «deepfakes» pornográficos se consideran similares a la pornografía tradicional no consentida debido a su impacto negativo en la difusión, lo que hace que dicha conducta sea censurable (Cerdán & Padilla, 2019).

Dada la incesante evolución de la tecnología, la sofisticación y la accesibilidad de los «deepfakes» están a punto de aumentar. En consecuencia, el método principal para identificar y rastrear a las personas responsables de actividades delictivas en línea depende de discernir la dirección IP (Protocolo de Internet). Este enfoque permite identificar el numeración única del dispositivo, lo que facilita la determinación del origen y el destinatario de la actividad, en particular el responsable del hecho, por lo que es una herramienta crucial en los procedimientos legales para aliviar los problemas probatorios en este ámbito.

MATERIALES Y METODOS

La investigación se desarrolló en Ecuador con el objetivo de analizar a través de un estudio jurídico-doctrinal y comparativo, la aplicación de una normativa que regule los “deepfakes”. Se emplearon varios método: el jurídico- doctrinal, que consisten en analizar de la literatura jurídica para respaldar posturas de autores, sobre los deepfakes. “La doctrina jurídica explica del por qué una norma jurídica es válida dentro de una sociedad” (Heocke, 2011). Jurídica-descriptivo, que permitió describir las características fundamentales de los “deepfakes”, aplica de manera pura, el método analítico a un tema jurídico, se trata de descomponerlo en tantas partes como sea posible (Rivera, 2007). El jurídico-comparativo, en la cual se examina distintas legislaciones como son México, Estados Unidos, España, Ecuador. Permite describir mediante la comparación de leyes, derechos reconocidos por otros países, en tanto compara los fenómenos jurídicos (Villabela, 2012).

El enfoque de la investigación se la realizó con un enfoque cualitativo, contiene un diseño no experimental, de tipo documental, bibliográfico, descriptiva. Busca comprender y explicar los "deepfake" desde diversas perspectivas. Pues se trata de una investigación exploratoria en virtud que es una actividad nueva y novedosa, y necesita identificar perspectivas legales y principios jurídicos esenciales, para tipificar los "deepfakes".

Dentro de la etapa de recolección de datos, se utilizó como técnicas de investigación la encuesta semiestructurada con la escala de Likert, la cual fue aplicada a abogados penalistas, fiscales y jueces en la ciudad de Riobamba

Población y muestra

La población está constituida por: Fiscales, Jueces de la Unidad Judicial Penal, Defensores Privados especializados en víctimas, quienes a diario necesitan estar actualizados con los nuevos desafíos legales, y la aparición de nuevos actos delictivos, se utilizó un muestreo no probabilístico de conveniencia, en vista de que se encuesta a personas conocedores de la materia con un total de 15 involucrados.

RESULTADOS Y DISCUSIÓN

"Deepfake" pornográfico como una nueva problemática social.

Los" Deepfake" pornográficos aparecieron en el año 2017, son videos que consisten en la creación de videos falsos, extremadamente realista, en la cual un rostro de una persona, es incrustado en el cuerpo de otra persona realizando una actividad pornográfica, denominada "cambio de caras".

El término «deepfake» proviene de la fusión de los términos ingleses «fake» (que denota falsedad) y «deep», derivados del concepto de «Deep Learning», una metodología de inteligencia artificial que emplea algoritmos que permite a una computadora adquirir conocimiento y modelar de forma autónoma características faciales (Hao, 2022).

Los vídeos manipulados, comúnmente denominados «vídeos ultra falsos», se realiza mediante la alteración automatizada de imágenes, videos y sonidos generados por la IA (Somers, 2020). El objetivo de estos vídeos es generar réplicas digitalizadas de cualquier persona, independientemente de su estado público o no pública.

La aparición de los “deepfakes” pornográficos se puede atribuir a la aplicación de la inteligencia artificial y a la utilización de la técnica de «aprendizaje profundo» para entrenar redes neuronales capaces de producir y manipular artificialmente vídeos, imágenes y audio. El proceso implica introducir imágenes de dos personas en un algoritmo de aprendizaje profundo para facilitar el intercambio de sus rostros (Rössler et al, 2019).

Deepfake en la legislación Ecuatoriana

El art 66 numeral 19 de la Constitución, la cual garantiza el derecho a la protección de datos de carácter personal su acceso, tomar decisiones sobre su datos, la distribución y difusión, en tal virtud requiere la autorización del titular ([CRE], 2008, art.11. núm. 19).

La [CRE] de 2008 reconoce y protege el derecho a la intimidad, “Artículo 66.- Derecho de libertad (...) núm. 20: Se le reconoce y garantiza a todas las personas el derecho a la intimidad personal y familiar” ([CRE], 2008, art. 66, numeral. 20). La Constitución busca reconocer y establecer un marco legal la protección de la intimidad frente a posibles intromisiones,

El [COIP], su art. 178 menciona será sancionada con una pena privativa de libertad de uno a tres años, la persona que sin contar con el consentimiento, reproduzca, grabe, publique datos personales, difunda, información contenida en un soporte informático (Asamblea Nacional, 2023, art. 178). Esta medida legal busca proteger la intimidad de las personas y garantizar la seguridad de la información en diversos medios, ya sea fisicos o digitales.

En Ecuador existe una garantía constitucional que se utiliza para el control de la propia información denominada Habeas Data en el Art. 92 inc. 3ero de la [CRE], que de manera tácita expresa: La persona titular de los datos, podrá solicitar, eliminación, actualización, ratificación, anulación o de datos, autorizado por la ley o por el titular ([CRE], 2008, art. 92, inc. 3ero).

La Ley Orgánica de Protección de Datos Personales: tiene como objeto proteger la información personal, acceder y determinar el manejo de sus datos, y proporcionar las garantías adecuadas. Con el fin de establecer, anticipar y desarrollar derechos, deberes y medidas de protección (LOPD] 2021, art.1).

Derecho comparado del deepfake pornográfico

En Estados Unidos, específicamente en el estado de Virginia, se han implementado leyes contra la "pornografía no consensual", se incluye los “deepfakes” pornográficos Las sanciones pueden incluir hasta un año de cárcel y multas de hasta 2.500 dólares. Además, existe una cooperación internacional a través del Convenio de Budapest sobre la Ciberdelincuencia, en que varios países incluyendo Estados Unidos (Capcha, 2024).

En España, se ha enmendado el artículo 3144 del Código Penal para incluir una definición de los deepfakes, considerándolos como "ultrafalificaciones". Las sanciones pueden alcanzar hasta 9 años de prisión. La Ley 13/2022 General de Comunicación Audiovisual aborda la difusión de deepfakes, que se considera una transgresión grave si se realiza sin el consentimiento explícito de las personas afectadas (Corte General, 2022).

En México, el artículo 199 octies del Código Penal Federal establece el delito de violación a la intimidad sexual, que incluye la divulgación de imágenes íntimas sin consentimiento. La sanción es de tres y seis años de cárcel y el pago de multas (Vargas, 2023).

Creación de deepfake

1. Recopilación de Datos: La fase inicial se recopila la mayor cantidad de datos, este proceso es importante para establecer bases para la generar video falsificado, implica la búsqueda y obtención de diversas imágenes o videos que representen a una persona en particular” (Sadonil, 2022).

2. Procesamiento: La etapa del proceso implica la preparación de los datos recopilados para su posterior entrenamiento, aquí se realizan diversas tareas tales como: recortar las imágenes para focalizar la atención en los rostros, el ajuste del color y la iluminación, para mejorar la calidad visual y homogeneizar los datos.

3. Entrenamiento de la Red: El entrenamiento de la Red Generativa (GANs) es un elemento crucial para buscar lograr un equilibrio entre la generación de contenido y la capacidad de discernir la autenticidad, esta etapa se centra en el la recopilación y procesamiento de datos, una vez completados estos dos pasos, la GANs se pone

en marcha, generando el desafío de distinguir las imágenes falsas de las reales (Toral, 2022).

4. Generación de "deepfake": Con red neuronal entrenada, el autor obtiene las imágenes o videos de cualquier persona y realizar la interposición de rostros, generando videos falsos, con abstracciones faciales y movimientos de la víctima (Gómez et al, 2022).

Rastreo del origen de los deepfake

Los "deepfakes" representan un desafío al sistema judicial respecto al rastreo de su origen, así como las técnicas de generación de contenido falso dificultan una identificación precisa del origen y la atribución de responsabilidad. En consecuencia, surge la necesidad de profesionales que sean expertos en la realización de investigaciones en línea y que posean conocimientos en el campo de la ciberinteligencia (inteligencia artificial), lo que conlleva a determinar que el Ecuador posee escasos expertos en éste ámbito.

Igual que un mensaje los "deepfakes" se compone de 3 parámetros que son: un lugar de partida, un lugar de llegada y mensaje o contenido el mensaje, entonces lo que se debe descubrir no solo son el contenido del delito sino también el origen o la fuente en la que se generó. En el caso que las computadoras, dispositivo móviles que trasfieren eso datos, tenemos un equipo un dirección IP de salida y una dirección IP de llegada de ser el caso (Cabello, 2017).

La dirección IP está definida como la identificación numérica que esta designada en cada dispositivo que esté conectado a internet, la dirección IP, es utilizada para determinar el origen y el destino de un delito en línea, hablando del campo penal, las autoridades judiciales utilizan esta detección para rastrear la actividad maliciosa de una persona y vincularla a un delito, se puede conocer varias características de dispositivo que se usó, como por ejemplo: la empresa a la que pertenece, color del dispositivo, tamaño, componentes, y otros detalles específicos. Pero de manera primordial lo que pretende encontrar es la titular de la IP (Arnedo, 2014).

Los proveedores de Internet y los administradores redes sociales, también están preparados para identificar los cuales están preparados para identificar a los

usuarios de internet que han asignado direcciones IP de manera fija o dinámica, además no solo cuentan con este dato, sino también almacena el número de identificación, fecha y hora, duración de la asignación de la IP, inclusive cuando el actor utilizó un teléfono.

Hay veces que los “deppefake” son manejadas a través de lo que se conoce como “cuentas espejo”, es decir estoy en Ecuador y manejo servidor través Europa y la misma se conecta con Asia y regresa a Ecuador, las cuentas se refledeppfakejan entre sí, seguir estas cuentas espejo es un camino que resulta complejo y se necesita el apoyo internacional para encontrar al autor del hecho. Análisis de memoria del dispositivo: el análisis de la memoria RAM, destaca toda información relevante sobre las actividades que fueron realizados en el dispositivo al momento de cometer delito.

Pericia de análisis de video y fotografía

La experiencia en el análisis de vídeo y fotografía es crucial. El auge de los vídeos “deepfake” subraya la necesidad de contar con herramientas para verificar la autenticidad del contenido, dados los avances tecnológicos que permiten manipular de forma convincente los vídeos y audios (Anderson, 2018). El autor hace hincapié en la facilidad de crear y difundir contenido manipulado a través de las redes sociales o sitios web. Algunos “deepfakes” muestran imperfecciones que los manipuladores se esfuerzan por corregir, como diferencias sutiles en las expresiones faciales, la posición de la cabeza, la iluminación y los contornos borrosos.

El parpadeo en un “deepfake” parece menos pronunciado en comparación con los vídeos auténticos, ya que el algoritmo no consigue replicarlo de forma convincente y rápida como lo haría un humano (Ehrenkranz, 2018, p. 175). También se observan discrepancias en el parpadeo entre los vídeos “deepfake” y los de personas reales.

Los desajustes entre las características corporales y las de la persona genuina sirven como indicadores adicionales de falsedad. Los «deepfakes» suelen centrarse en los primeros planos faciales para minimizar la edición y reducir el riesgo de errores.

Estos vídeos suelen ser de corta duración, de unos pocos segundos, debido al considerable esfuerzo que se requiere para dominar el algoritmo. El contenido increíble en vídeos excesivamente cortos también puede sugerir su naturaleza "deepfake".

En muchos "deepfakes", el algoritmo se esfuerza por sincronizar el sonido con los movimientos de los labios, lo que subraya la importancia de tener varias voces para ayudar a la detección (Vives, 2019). Además, analizar minuciosamente los detalles sutiles de la grabación puede resultar revelador, ya que ralentizar la reproducción del vídeo puede provocar alteraciones repentinas de la imagen o cambios de fondo que indiquen que se trata de un "deepfake".

Desafío probatorio

Los obstáculos legales relacionados con la presentación de pruebas ante los tribunales en relación con la tecnología "deepfake" son complejos. Autenticar y preservar la integridad de las pruebas plantea un gran desafío debido a la naturaleza sofisticada de las manipulaciones realizadas mediante la tecnología deepfake, lo que dificulta diferenciar entre vídeos o imágenes auténticas y alteradas. La ausencia de una legislación específica en este ámbito crea lagunas legales e incertidumbre a la hora de abordar los casos de ciberdelincuencia.

Los registros de dirección IP proporciona información acerca del dispositivo que utilizo para acceder al internet que puede ser útil para establecer una conexión entre el responsable de la actividad ilegal, entonces se resalta que la evidencia digital es una herramienta importante para la imputación de delitos informáticos.

La pericias informáticas son fundamentales para determinar la veracidad de los contenidos digitales, pues se necesita de peritos informáticos, especializados en identificación de anomalías. La evidencia digital debe ser obtenida conforme a lo establece la ley para ser materializada al proceso judicial, la cual se debe garantizar la cadena de custodia y el debido proceso.

Tabla 1.

Resultados del cuestionario aplicado a Fiscales, Jueces de la Unidad Judicial Penal, Defensores Privados especializados en víctimas.

Preguntas	Variable	Familiarizado	Neutral	No familiarizado	Poco familiarizado	
1.- ¿Está familiarizado con el concepto de "deepfakes" y su uso en contextos legales?	Concepto "deepfake"	6,67%	33,33%	20,00%	40,00%	
		De acuerdo	**En desacuerdo**	**Neutral**	**Totalmente de acuerdo**	**Totalmente en desacuerdo**
2. ¿Considera que el uso de "deepfakes" está en aumento en los casos que involucran vulneración del derecho de intimidad?	Aumento	0,33333333	0,06666667	0,33333333	0,2	0,06666667
3. **¿Usted cree urgente la necesidad de incorporar regulaciones legales que aborden la problemática de los "deepfake" en el Ecuador?**	Incorporar	60,00%	0%	0%	33,33%	6,67%
4**. ¿Considera que la tecnología actual proporciona herramientas suficientes para detectar y autenticar "deepfake"?**	Proporcionar	33,33%	40,00%	20,00%	6,67%	0%
5**. ¿Considera que el sistema judicial mantiene desafíos importantes en la autenticidad de un contenido de "deepfake"?**	Desafíos	53,33%	13,33%	20,00%	13,33%	0%

6. **¿En su opinión, cree que los "deepfakes" representan una amenaza significativa para el derecho de intimidad de las personas?**	Amenaza	46,67%	13,33%	6,67%	33,33%	0%
7. **Usted cree que las víctimas han sufrido consecuencias emocionales o psicológicas debido a la difusión de "deepfakes"**	Consecuencias	40,00%	0%	6,67%	46,67%	6,67%
8. **¿Considera que la legislación actual en el Ecuador aborda adecuadamente los casos de "deepfakes" y su relación con la vulneración del derecho de intimidad?**	Abordar	13,33%	6,67%	20,00%	6,67%	53,33%
9. **¿Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos?**	Enfrentar	46,67%		20,00%	6,67%	26,67%
10 **¿Usted considera que se debe establecer como un tipo penal especifico al "deepfakes", en nuestro Código Orgánico Integral Penal?**	Tipo penal	20,00%	6,67%	0%	6,67%	66,67%

Nota: *Encuesta realizada a: Fiscales Especializados de Violencia de Género de la ciudad de Riobamba, Jueces de la Unidad Judicial Penal y Defensores en libre ejercicio especializados en víctimas.*
Autor*: Franklin Geovanny Sinaluisa Sagñay*

El resultado obtenido con la aplicación de los instrumentos de investigación, infiere con la realidad de la problemática del surgimiento de nuevos delitos tecnológicos "deepfakes" pornográfico. Se observa que el 40% de los encuestados indicaron estar poco familiarizados, seguido por un 33.33% que se mostraron neutrales en su conocimiento sobre el tema. Solo el 6.67% indicó estar completamente familiarizado, mientras que el 20% restante manifestó no estar familiarizado con el concepto. Es así que 7 de casa 10 latinoamericanos desconocen, qué es un "deepfake".

Sobre la percepción de un aumento en los casos de "deepfake" entre los encuestados en el ámbito del derecho. Aunque no hay un consenso claro, se observa que aproximadamente el 53.33% de los participantes están en desacuerdo o neutral con respecto al aumento de los casos de "deepfake", mientras que el 33.33% expresó estar de acuerdo o totalmente de acuerdo. Esta distribución sugiere una división en la percepción del aumento de casos de "deepfake" dentro de la comunidad jurídica.

La necesidad y la aceptación de la incorporación de regulaciones legales relacionadas con el tema en cuestión. Aproximadamente el 93.33% de los encuestados expresaron estar de acuerdo o totalmente de acuerdo con la idea de implementar regulaciones legales, mientras que solo el 6.67% indicó estar en desacuerdo. Basándome en la tabla proporcionada, hay una clara tendencia hacia la reforma del Código Orgánico Integral Penal (COIP) para abordar el tema del "deepfake". Se observa un énfasis en la tipificación de este delito, así como en la responsabilidad y las sanciones asociadas con él.

La percepción y utilización de herramientas para detectar "deepfake" dentro del ámbito legal. Aproximadamente el 80% de los encuestados expresaron estar de acuerdo o totalmente de acuerdo con la existencia y utilidad de estas herramientas, mientras que solo el 20% indicó estar en desacuerdo. Esta tendencia sugiere una creciente conciencia y aceptación dentro de la comunidad jurídica sobre la importancia de contar con herramientas especializadas.

Sobre el desafío que representa la autenticidad del contenido de los "deepfakes" en el ámbito del derecho, aproximadamente el 66.67%, expresó estar de acuerdo o totalmente de acuerdo con este desafío, un porcentaje considerable, el 33.33%,

manifestó estar en desacuerdo o neutral al respecto. Esta variabilidad en las respuestas sugiere una falta de consenso dentro de la comunidad jurídica.

Los “deepfakes” representan una amenaza contra el derecho a la intimidad. Se observa una clara tendencia hacia la preocupación en este sentido, con el 86.67% de los encuestados expresando estar de acuerdo o totalmente de acuerdo con esta afirmación. Esta alta proporción sugiere una percepción generalizada dentro de la comunidad jurídica sobre la amenaza que los “deepfakes”.

En relación al reconocimiento de las consecuencias emocionales o psicológicas que las víctimas experimentan como resultado de los “deepfakes”. Aproximadamente el 93.34% de los encuestados expresaron estar de acuerdo o totalmente de acuerdo con esta afirmación, mientras que solo el 6.67% indicó estar en desacuerdo o neutral al respecto.

Aproximadamente el 80% de los encuestados expresaron estar en total desacuerdo o en desacuerdo con la afirmación de que Ecuador aborda adecuadamente estos casos. Esto sugiere una falta de confianza generalizada en la efectividad de las medidas existentes para enfrentar los “deepfakes” dentro del contexto legal ecuatoriano.

La falta de confianza en la preparación de la justicia ecuatoriana para enfrentar delitos informáticos. Un total del 73.34% de los encuestados expresaron estar en desacuerdo o totalmente en desacuerdo con la afirmación, mientras que solo el 6.67% indicó estar totalmente de acuerdo. Esta tendencia refleja una preocupación respecto a la capacidad del sistema judicial ecuatoriano para abordar efectivamente los delitos informáticos.

La tendencia hacia la creación de un tipo penal específico para abordar los “deepfakes”. Aproximadamente el 86.67% de los encuestados expresaron estar de acuerdo o totalmente de acuerdo con esta medida, mientras que solo el 13.33% indicó estar en desacuerdo. Esta fuerte inclinación sugiere establecer una legislación específica para abordar los delitos relacionados con los “deepfakes”.

La perspectiva de propuesta de reforma es la siguiente: Art. 178.- Violación a la intimidad: La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, genere con Inteligencia

Artificial, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (Asamblea Nacional,2023) .

Tabla 2

Análisis de derecho comparado del "deepfake" y su aplicabilidad en el Ecuador.

Dimensión / Atributo	Estados Unidos	España	México	Ecuador
Legislación específica sobre "deepfake"	En el estado de Virginia define a los "*deepfakes*" pornográficos, como vídeos o imagenes manipuladas con herramientas digitales (Divulgadores del misterio, 2019).	La Ley 13/2022 General de Comunicación Audiovisual aborda la difusión de deepfakes, que se considera una transgresión grave si se realiza sin el consentimiento explícito de las personas afectadas (Corte General, 2022).	Artículo 199 octies Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual, sin su consentimiento, su aprobación o su autorización (Cámara de Diputados, 2021).	No hay legislación específica sobre deepfake, pero se pude aplicar el articulado de violación a la intimidad
Protección de datos personales	Ley de privacidad es equilibrar la necesidad del gobierno de almacenar información sobre las personas con los derechos de las personas a ser protegidas contra las invasiones injustificadas	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales derechos de las personas a la protección y tratamiento de sus datos personales (Jefatura de Estado, 2018).	Ley Federal de Protección de Datos Personales ejerce sus derechos de acceso, rectificación, cancelación, de datos.	La Ley Orgánica de Protección de Datos Personales, en su artículo 1, señala que su objeto y finalidad es el garantizar el ejercicio del derecho a la protección de datos personales (Asamblea Nacional,2021)
Sanciones y penas	En Virginia hasta un año de cárcel y 2.500 dólares	Ley General de Comunicación Audiovisual,	En el Código Penal Federal sanciona entre	No hay legislación específica sobre

	de multa (Flusche, s.f).	sancionada con multas de entre los 60.000 y los 600.000 euros. (Marcus,2024)	tres y seis años de prisión y multas de entre 54,000 y 109,000 pesos (Morales, 2021).	"deepfakes" , pero se podría aplicar leyes relacionadas con la vulneración del derecho a la intimidad, que tiene como sanción un pena de 3 años de prisión
Cooperación internacional	Convenio sobre la ciberdelincuencia (STE 185)	Convenio sobre cibercriminalidad o Convenio de Budapest	Convenio sobre cibercriminalidad o Convenio de Budapest	Convenio sobre cibercriminalidad o Convenio de Budapest

***Autor**: Franklin Geovanny Sinaluisa Sagñay*

Respecto al derecho comparado sobre el "deepfakes", España, Estados Unidos, México y Ecuador, han aborda el tema desde diferentes enfoques. En España, la propuesta de Ley de Inteligencia Artificial, que se refiere a mitigar los riesgos de la creación de "deepfake" pornográficos, introduce enmiendas legales para la protección del derecho a la intimidad, privacidad y la reputación, estableciendo medidas para eliminar contenido falso y encontrar al responsable de dicho acto.

En Estados Unidos, la legislación varía entre estados, referente a la difusión del "deepfake" pornográfico, ya que a nivel federal existen otras leyes que establecen las definiciones y sanciones para este delito. En México tiene una ley que relacionada a la violencia contra la mujer denominada Ley Olimpia la cual lucha contra la violencia y acoso digital, penalizando la distribución de contenido sexual íntimo sin consentimiento, con sanciones severas así como su respectiva reparación integral. Finamente el Ecuador no tiene normativa específica sobre "deepfake", pero se pude aplicar el articulado de violación a la intimidad.

CONCLUSIÓN

Numerosas doctrinas coinciden en la interpretación de los "deepfake",en los que la inteligencia artificial se utiliza para desarrollar algoritmos que permiten la creación de abstracciones faciales y la generación de patrones audiovisuales, lo que resulta en vídeos engañosos, lo que enfatiza la urgente necesidad de abordar este tema desde un punto de vista legal y tecnológico.

Los desafíos que presentan los "deepfake" en cuanto a la identificación de su origen y la asignación de responsabilidades son particularmente pronunciados en el ámbito judicial, lo que pone de relieve la complejidad de las mismas. Rastrear el origen y la dirección IP es un mecanismo crucial para establecer la precisión, la legitimidad y la responsabilidad de dicho contenido, ya que ayuda a identificar el dispositivo responsable de generar y difundir el material fabricado. Los conocimientos informáticos desempeñan un papel fundamental a la hora de verificar la autenticidad del contenido mediante metodologías especializadas que implican analizar minuciosamente la estructura de los archivos, identificar irregularidades y descubrir manipulaciones, lo que facilita la extracción de datos de los dispositivos electrónicos.

Dada la compleja naturaleza y las consecuencias de las llamadas "deepfake" en el marco legal ecuatoriano, es imprescindible tomar medidas urgentes para mejorar la capacidad del sistema para detectar, gestionar y juzgar los casos relacionados con esta tecnología. Esto requiere la formación y especialización de especialistas informáticos en inteligencia artificial y análisis facial, junto con la revisión de los protocolos y estándares para garantizar la aceptación de la evidencia digital en el sistema legal ecuatoriano.

En términos de análisis jurídico comparado, la legislación y las estrategias implementadas en los Estados Unidos, España y México en relación con los "deepfake" ilustran notables similitudes y distinciones en sus enfoques sobre este tema. Mientras que los Estados Unidos y España han introducido leyes específicas que prohíben los "deepfake" en contextos como la pornografía no consentida, México y Ecuador carecen de medidas legislativas explícitas que aborden este tema en particular.

REFERENCIAS BIBLIOGRÁFICAS.

Anderson, K. E. (2018). *Getting acquainted with social networks and apps: combating fake news on social media* [Familiarizarse con las redes sociales y las apps: combatir las noticias falsas en los medios sociales]. Library Hi Tech News, 35(3), 1-6. https://doi.org/10.1108/lhtn-02-2018-0010

Arnedo, B. (11 de marzo de 2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. https://reunir.unir.net/handle/123456789/2828

Asamblea Nacional. (2021). Constitución de la República del Ecuador. Corporación de Estudios y Publicaciones.

Asamblea Nacional. (2021). Ley Orgánica de Protección de Datos Personales. Corporación de Estudios y Publicaciones. Lexis Finder. https://www.finanzaspopulares.gob.ec/wpcontent/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asamblea Nacional. (2023). Código Orgánico Integral Penal. Lexis Finder. https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

Cabello, G. (2017). *Geolocalization through IP addresses* [Geolocalización a través de direcciones IP]. Revista de Derecho de la UNED (RDUNED), 0(20), 283. https://doi.org/10.5944/rduned.20.2017.19492

Cámara de Diputados. (2021). iniciativa que reforma el artículo 199 octies del Código Penal Federal, a cargo de la diputada María Jesús Aguirre Maldonado, del grupo parlamentario del pri. México. http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/03/asun_4318201_20220301_1646182113.pdf

Capcha, E. (2024). *Legisladores de Estados Unidos buscan combatir la pornografía deepfake*. Infobae. https://www.infobae.com/estados-unidos/2024/05/24/legisladores-de-estados-unidos-buscan-combatir-la-pornografia-deepfake/

Divulgadores Del Misterio. (4 de julio de 2019). En Estados Unidos están empezando a legislar contra los 'deepfakes', y así está la normativa al respecto en España. Divulgadores del Misterio. https://divulgadoresdelmisterio.net/en-estados-unidos-estan-empezando-a-legislar-contra-los-deepfakes-y-asi-esta-la-normativa-al-respecto-en-espana/

Ehrenkranz, M. (16 de junio de 2018). *Hay un truco infalible para detectar si un vídeo ha sido manipulado por una IA Deep Fake: fíjate en los ojos*. Gizmodo En Español. https://es.gizmodo.com/hay-un-truco-infalible-para-detectar-si-un-video-ha-sid-1826888894

Gómez, A., Feijóo, C. & Salazar, I. (2021) Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital. Deep fakes e inteligencia artificial. *"El Profesional de la Informacion"*, 30(2), 1-24. https://doi.org/10.3145/epi.2021.mar.16

Corte General. (2022). Ley General de Comunicación Audiovisual, España.

Hoecke, M. (2014). Doctrina jurídica: ¿Qué método (s) para qué tipo de disciplina? *Ciencia Jurídica*, 3(6), 127-148. https://doi.org/10.15174/cj.v3i2.115

Hao, K. (2022). What is machine learning? [¿Qué es el aprendizaje automático?]. MIT Technology Review. https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/

Cerdán, V., & Padilla, G. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. Historia y Comunicación Social, 24(2), 505.

https://link.gale.com/apps/doc/A612031130/IFME?u=anon~4eadf41e&sid=googleScholar&xid=0b6194d4

Estrada, J. C. (s. f). El Derecho A La Intimidad Y Su Necesaria Inclusión Como Garantía Individual. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Flusche, A. (s.f). Clasificaciones de delitos menores y graves en Virginia. https://www.andrewflusche.com/blog/virginia-felony-misdemeanor-classifications/

Jefatura de Estado. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/eli/es/lo/2018/12/05/3

Marcus, P. (2024). Sandra Golpe, Pablo Motos, Resines... Crecen las estafas con 'deep fakes': serán sancionadas hasta con 600.000€. https://www.vozpopuli.com/espana/deep-fake-sancion-propuesta-sumar.html

Morales, F. (2024). Deepfakes: Sancionarán con cárcel la difusión de imágenes porno creadas con IA. https://www.eleconomista.com.mx/politica/Deepfakes-Sancionaran-con-carcel-la-difusion-de-imagenes-porno-creadas-con-IA-20240216-0094.html

Rivera, W. (2005). *Investigación Jurídica* [Diapositivas de PowerPoint]. Issuu. https://issuu.com/wrivera/docs/investigacion_juridica

Rossler, A. et al. (2019). FaceForensics: Learning to Detect Manipulated Facial Images [Cómo detectar imágenes faciales manipuladas]. 1-11. https://openaccess.thecvf.com/content_ICCV_2019/html/Rossler_FaceFo

rensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.html

Sadornil, D. (2022). XVII Reunión española sobre criptología y seguridad de la información. RECSI 2022. Editorial Universidad de Cantabria: Santander; pp. 251. https://books.google.es/books?hl=es&lr=&id=V4qREAAAQBAJ&oi=fnd&pg=PA205&dq=Recopilaci%C3%B3n+de+Datos:+La+fase+inicial+de+la+creaci%C3%B3n+de+los+%E2%80%9Cdeepfakes%E2%80%9D+&ots=YWHkHwv-RQ&sig=fFJLVjYRYIQgoTBPE9qud6qLqZ0#v=onepage&q=recopilaci%C3%B3n&f=false

Sastre, T. (2022). Deepfakes: creación de nuevas caras a partir de imágenes de famosos. *Universidad Abierta de Cataluña*. http://hdl.handle.net/10609/146181

Somers, M. (2020). *Deepfakes, explained* [Deepfakes, explicado]. Massachusetts Institute of Technology. https://www.researchgate.net/publication/368330820_Deepfake_Cuando_la_inteligencia_artificial_amenaza_el_Derecho_y_la_Democracia

Vives, S. (2019). Posverdad. La nueva guerra contra la verdad y cómo combatirla. De Mattew d'Ancona, Alianza Editorial, 2019. Clivatge Estudis I Tesitimonis del Conflicte I el Canvi Social, 7. https://doi.org/10.1344/clivatge2019.7.8

Conflicto de intereses

Los autores indican que esta investigación no tiene conflicto de intereses y, por tanto, acepta las normativas de la publicación en esta revista.

Con certificación de: