UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

Título

"Deepfakes", dificultades probatorias y su incidencia en la vulneración al derecho de intimidad"

Trabajo de investigación previo la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador

Autor:

Franklin Geovanny Sinaluisa Sagñay

Tutor:

Mgs. Wendy Pilar Romero Noboa

Riobamba- Ecuador

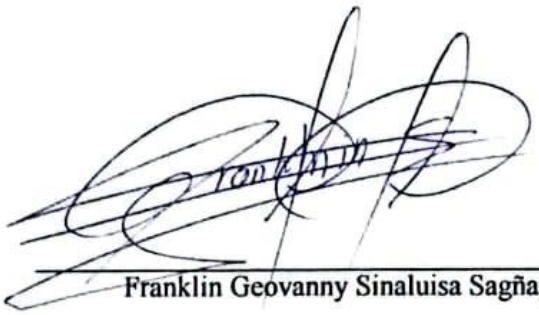
2024

DECLARATORIA DE AUTORÍA

Yo Franklin Geovanny Sinaluisa Sagñay, con cédula de identidad 060475403-6, autor del presente trabajo de investigación que tiene como título: "Deepfakes dificultades probatorias y su incidencia en la vulneración al derecho de intimidad", declaro de manera libre y voluntaria que la protección, contenidos, criterios, opiniones y conclusiones desarrollados en la misma, son de mi absoluta responsabilidad.

De la misma forma, debo manifestar que cedo a la Universidad Nacional de Chimborazo, y de una manera no exclusiva, los derechos para su uso, distribución, divulgación y/o reproducción total o parcial, por los diferentes medios físicos o digitales; mediante la cual no podrá obtener beneficios económicos. Las posibles reclamaciones de terceros respecto a los derechos de autor de la obra mencionada, será de mi responsabilidad; librando de posibles obligaciones a la Universidad Nacional de Chimborazo.

En Riobamba, de 17 julio del 2024



Franklin Geovanny Sinaluisa Sagñay

CI. 0604754036

AUTOR

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Msc. Wendy Pilar Romero Noboa , catedrática de la Universidad Nacional de Chimborazo, adscrito a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación de título "Deepfakes, dificultades probatorias y su incidencia en la vulneración al derecho de intimidad", por la autoría de Franklin Geovanny Sinaluisa Sagñay, por lo que se autoriza ejecutar los trámites legales de su sustentación.

Es todo en cuanto puedo informar en honor a la verdad, en Riobamba, 6 días del mes de Marzo de 2024.

Msc. Wendy Pilar Romero Noboa

TUTOR

CERTIFICADO DE LOS MIEBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para evaluar del trabajo de investigación "Deepfakes, dificultades probatorias y su incidencia en la vulneración al derecho de intimidad", realizado por Franklin Geovanny Sinaluisa Sagñay con cédula de identidad 060475403-6, bajo la tutoría de la Mgs. Wendy Romero; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente de ha evaluado el trabajo de investigación y escuchada la sustentación por parte de sus autores; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a los 05 días del mes de agosto del 2024.

Mgs. Gabriela Medina

PRESIDENTE DEL TRIBUNAL DE GRADO

Dr. Nelson Freire

MIEMBRO DEL TRIBUNAL DE GRADO

Dra. Rosita Campuzano

MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICADO ANTIPLAGIO

Con entendimiento

DECANATO DE LA FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

Riobamba, 27 de junio del 2024
Oficio No. 513-DFCPA-UNACH

Magister
Alianne Araujo Pirela
COORDINADOR DE GESTION DE BIBLIOTECA
Presente

De mi consideración:

El Decanato de la Facultad de Ciencias Políticas y Administrativas en virtud de las atribuciones que le confiere el Estatuto de la Universidad Nacional de Chimborazo en su Art. 150, literal a) expresa: "Decano, máxima autoridad académica de la Facultad, responsable de la gestión estratégica";

Que, el Estatuto de la Universidad Nacional de Chimborazo, en su Art. 152, numeral 17, determina que es atribución del decano de la Facultad resolver las solicitudes de personal académico, administrativo y estudiantes que no sean competencia expresa de órganos de mayor jerarquía"

Por cuanto existe el informe de la Sra. Subdecana Oficio No. 0259-SD-FCPA-UNACH-2024 referente a la no publicación completa en el repositorio de tesis del Señor Franklin Sinaluisa Sagñay

RESUELVE

Resolución No. 513-DFCPA-UNACH.- Oficiar a la Coordinadora de Gestión de Bibliotecas, a fin de solicitar la no publicación completa en el repositorio de tesis de la Universidad Nacional de Chimborazo, el informe final del Proyecto de Investigación (Tesis) **"DEEPFAKES, DIFICULTADES PROBATORIAS Y SU INCIDENCIA EN LA VULNERACIÓN AL DERECHO DE INTIMIDAD"**, como autor el Sr. Franklin Geovanny Sinaluisa Sagñay, estudiante de la Carrera de Derecho, bajo la tutoría de la Mgs. Wendy Pilar Romero Noboa, por cuanto el presente trabajo de investigación es la base de un artículo académico, en tal virtud solo se publique un resumen.

Sin otro particular, me suscribo de Usted.

Atentamente,

JOSE ORLANDO GRANIZO CASTILLO

Dr. José Orlando Granizo Castillo
DECANO DE LA FACULTAD

Elaborado: Marilyn L

DEDICATORIA

A mi familia que son la luz de mi vida y la razón de mi existencia. A mi madre por su apoyo y su amor inmenso, sus sacrificios y su infinita paciencia, así como su afán, abnegación y su incondicional apoyo moral, que hicieron posible la culminación de mi carrera universitaria, de igual manera, el apoyo emocional de mis hermanas Itzel y Nora, quienes me alentaban día a día, en la consecución de mis estudios. A ti Nadia, por tu amor, comprender mi ausencia en varios momentos y alegrarte por mis triunfos, tu paciencia y aliento constante que ha sido fundamental para mantenerme enfocado y motivado para la culminación de este proyecto.

Una vez más agradezco, por hacer posible esta etapa de aprendizaje, la cual me capacita para un futuro mejor, y que siempre pondré a disposición del bien de las personas que me rodena, y sobre todo buscando la justicia y la verdad en el ejercicio de mi profesión, adhiriéndome a los valores y principios inculcados por mi madre, por eso y mucho más, Dios os Pague.

AGRADECIMIENTO

Quiero expresar mis más sinceros agradecimientos a todas las personas que contribuyeron de una manera muy significativa al cumplimiento de este proyecto. En primer lugar gradecer a mi tutora la Msc. Wendy Pilar Romero Noboa, que con entusiasmo, su orientación y vastos conocimientos hicieron posible este evento importante, así como su paciencia infinita a lo largo de este arduo trabajo. Los consejos y retroalimentación fueron fundamentales para dar forma y realizar las observaciones necesarias para mejora el trabajo.

Además quiero agradecer a todos los profesores que con su colaboración, asesoramiento, conocimientos y experiencia, realizaron su aporte y enriquecieron este proyecto, logrando ampliar las perspectivas del tema, como no también agradecer a mis compañeros de estudio que con sus palabras de aliento han hecha llevadera la travesía académica, y sobre todo dejó constancia de mi enorme agradecimiento a la Universidad Nacional de Chimborazo, el ama mater de futuras generaciones de profesionales.

Por último, pero no menos importante agradezco a mi familia que me apoyo con la decisión de convertirme en un profesional del Derecho, que con su constancia y motivación, además del sacrificio realizado por mi madre, que hicieron posible y realidad uno de mis más grandes anhelados sueños.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Los “deepfakes” son videos o imágenes falsas creadas con inteligencia artificial que incurre en una violación a la intimidad y la privacidad. Este acto surge en el año 2017 específicamente para hacer videos sexuales falsos, sin consentimiento de la persona. El derecho de intimidad, es un derecho fundamental la cual protege la vida privada de cada individuo. El presente proyecto de investigación, trata de la falta de tipificación en Ecuador sobre los “deepfakes” así como su relación con las dificultades probatorias que esto conlleva. Se realizó con un método investigación, de enfoque cualitativo, de tipo documental, bibliográfico, dogmática, descriptiva, que contiene un diseño no experimental. Es preocupante que los “deepfakes” invadan la privacidad e intimidad usando datos encontrados en redes sociales o en cualquier sitio web (big data). El derecho comparado ayuda a estudiar legislaciones para dar perspectivas de reforma que puedan resolver este problema de forma efectiva, y determinar su aplicabilidad en posibles casos futuros, que sucedan en el Ecuador. En efecto la falta de tipificación de este acto afecta directamente al derecho de intimidad de las personas en futuros casos, por lo que se resalta la necesidad de implementar en Código Orgánico Integral Penal, normativas para prevenir y sancionar estas manipulaciones digitales maliciosa, también implementar las herramientas y métodos de investigación para contra el origen y al responsable de la creación de los “ deepfake”, así como señalar la falta de peritos especializados en Inteligencia Artificial. Se analiza un caso real, así como legislaciones diferentes para entender los retos legales actuales y así proponer soluciones jurídicas fiables.

Palabra clave

Deepfake pornográfico, víctimas mujeres, derecho de intimidad, inteligencia artificial, privacidad.

ABSTRACT

The "deepfakes" are fake videos or images created with artificial intelligence that incurs a violation of privacy and intimacy. This act arose in 2017 specifically to make fake sex videos without the consent of the person. The right to privacy is a fundamental right that protects the private life of each individual. The present research project deals with the lack of typification in Ecuador on "deepfakes" and its relationship with the evidentiary difficulties that this entails. It was carried out using a qualitative, documentary, bibliographic, dogmatic, descriptive, and descriptive research method, which contains a non-experimental design. It is worrying that "deepfakes" invade privacy and intimacy using data found in social networks or on any website (big data). Comparative law helps to study legislation to give perspectives on reform that can solve this problem effectively and determine its applicability in possible future cases in Ecuador. The lack of criminalization of this act directly affects the right to privacy of individuals in future cases, so it highlights the need to implement the Organic Criminal Code, regulations to prevent and punish these malicious digital manipulations, also implement the tools and methods of investigation to find the origin and the responsible for the creation of the "deepfake," as well as pointing out the lack of experts specialized in Artificial Intelligence. A real case is analyzed, and different legislations are examined to understand the current legal challenges and propose reliable legal solutions.

Keywords: Pornographic deepfake, female victims, privacy rights, artificial intelligence, privacy.

Reviewed by:

Lic. Eduardo Barreno Freire. Msc.

ENGLISH PROFESSOR

C.C. 0604936211

CAPÍTULO I

INTRODUCCIÓN

El término “Deepfake” posee un acrónimo anglosajón, derivadas dos palabras “ Fake” (falso) y “Deep” (profundo), surge desde el año 2017 en Hollywood, ciudad de Los Ángeles California, los “deepfakes” se crean con la ayuda de la inteligencia artificial, y desarrolla algoritmos que permite a una computadora moldear abstracciones faciales con el objetivo de generar patrones audiovisuales, la técnica tiene un software que utiliza inteligencia artificial en el cual edita voz y video de manera hiperrealista a través del Deep Learning (Somers,2020). El fin de estos videos e imágenes, es realizar copias digitalizadas de cualquier persona ya sea públicas o privadas e implementarlos en videos de carácter sexual, o en cualquier otro video que al autor se le ocurra, perjudicando así la vida privada de la víctima y su derecho a la intimidad.

El derecho a la intimidad es un derecho fundamental establecido en la Constitución ecuatoriana que protege la esfera más privada de cada persona y de su familia, lo cual conlleva el respeto a: la personalidad humana, el aislamiento del hombre, lo íntimo de cada uno, es innata e inherente desde el momento de su nacimiento, por lo que significativamente se determina que las nuevas tecnologías (Inteligencias Artificial) pueda vulnerar el derecho de la intimidad.

El presente proyecto de investigación realiza un análisis legal, doctrinal y de derecho comparado, en relación a los riesgos que ocasiona las nuevas tecnologías como son los llamados “Deepfake” y establecer su incidencia en el derecho de la intimidad, caso contrario, de no regularse a tiempo y de amanera oportuna, generaría complicaciones a la vida privada de la víctima, así como la salud, entorno laboral y social.

Es esencial abordar estos desafíos desde un enfoque legal, así como las dificultades probatorias para encontrar al autor del hecho, y su relación con la vulneración al derecho constitucional de la intimidad. Es preocupante la capacidad de los “deepfakes” para invadir la privacidad personal, ya que las imágenes y videos son obtenidas mediante las redes sociales o inclusive de cualquier otro sitio web. A través del derecho comparado se realiza un análisis normativo de legislaciones como Estados Unidos, México, España, para poder determinar los desafíos que enfrenta actualmente la comunidad legal, y así poder proporcionar perspectivas para solucionar este problema de una manera efectiva.

El método que se aplicará es de un enfoque cualitativo, de tipo documental, bibliográfico, dogmática, descriptiva, que contiene un diseño no experimental. Finalmente, la estructura planteada en el presente proyecto de investigación respeta los criterios establecidos en el Reglamento de Titulación de la Universidad Nacional de Chimborazo vigente y que se transcribe en: portada; introducción; planteamiento de problema; objetivos: general y específicos; estado del arte; marco teórico; metodología; referencias bibliográficas; anexos.

1.1. PLANTEAMIENTO DEL PROBLEMA

No se requiere ser un experto informático para encontrar y manejar sitios web, aplicaciones, para crear "deepfakes" pornográficos, solo se necesita una foto o un video que fácilmente puede ser obtenida de cualquier red social o sito web. Para hacer un video de contenido sexual de 60 segundos se necesita solo 25 minutos para el procesamiento total, además existe webs y aplicaciones gratuitas lo que los hace más accesibles, salvo otras aplicaciones que son pagadas, de acuerdo a los datos del informe "State of "deepfakes" (Home Security Heroes, 2023, p.56). Este fenómeno social subraya la facilidad en la que se crean los "deepfake" pornográficos con la ayuda de la IA, así como la disponibilidad de acceder a herramientas gratuitas y de paga, lo que amplía la preocupación en su utilización indebida y su difusión.

Los rostros de actrices son recortados e incrustados en escenas de contenido pornográfico y luego cargadas en páginas para adultos, los "deepfakes" crean audio y video falsificados extremadamente convincente, lo cual, da como resultado una serie de incidentes que han socavado la privacidad de las personas. Estas manipulaciones digitales han cobrado relevancia en el contexto global y genera una preocupación creciente, y un impacto en la sociedad, específicamente relacionado al derecho a la intimidad de las mujeres.

En la actualidad existe un aumento en la creación y distribución de los "deepfakes" que inclusive ya ha llegado al Ecuador, en la ciudad de Quito. Esto incide en el derecho de intimidad de las personas, que se violenta por la falta de normativa vigente, la dificultad probatoria, respecto a la autenticidad y búsqueda del autor de los contenidos alterados. Las creaciones de imágenes o videos pornográficos creadas con la ayuda de la inteligencia artificial, no se encuentran contemplados en el Código Integral Penal del Ecuador, cómo ya lo han hecho en otros países como: España, Estados Unidos y México. Con el avance de la tecnología, se prevé que los "deepfakes" pornográficos se vuelvan más sofisticados y accesibles.

El problema jurídico a investigar se refiere a la falta de tipificación en Ecuador sobre los "deepfakes" así como su relación con las dificultades probatorias que esto conlleva. Además, es necesarios destacar que la falta de regulación de este acto afecta el derecho de intimidad de las personas y resalta la necesidad de implementar medidas normativas para prevenir y sancionar estas manipulaciones digitales maliciosa en el futuro.

1.2.JUSTIFICACIÓN

Esta investigación es relevante por la razón de que en Ecuador no está tipificado el acto de los "deepfake" que son totalmente nuevo a nivel global, lo cual con esta investigación puede servir a establecer una perspectiva de reforma al artículo 178 del Código Orgánico Integral Penal en adelante (COIP), ya que es totalmente emergente, debido a que utiliza inteligencia artificial para crear contenido audiovisual falso hiperrealista, pues la misma está en constante evolución. Es importante analizar cómo diferentes jurisdicciones ya han trabajado en la regulación del "deepfake".

De acuerdo con estudios realizados en España entre el año 2022 y 2023, la cantidad de pornografía "deepfake" se ha creado un aumento, pasando de 3725 videos en 2022 a 21.019 en 2023, un patrón alarmante según el informe "State of deepfakes" (Home Security Heroes, 2023). En este caso videos e imágenes que se combina en una aplicación web o una aplicación móvil, en la que la aportación de entrada es una imagen o video y de salida otra imagen o video pero transformada, que en éste caso es un desnudo. La creación de este acto, es una nueva forma de violencia en contra de la mujer, ya que tiene la finalidad de intimidar, acosar, manipular y destruir la reputación de la víctima, así como difamar, invadir la privacidad, fraude y vulneración del derecho a la intimidad, honor y el buen nombre como lo hace el "revenger porn" en español porno venganza o sexting.

En la actualidad, la problemática de los "deepfakes" en Ecuador es reciente, en el que ya se dio un caso, en octubre de éste 2023, por parte de un estudiante de un Colegio Católico de Quito en la cual utilizó fotografías de sus compañeras para crear contenido de carácter sexual con la inteligencia artificial, se cree que son 700 contenidos en total de esta falsificación, creados y difundidos por diferentes medios de comunicación y redes sociales, se realizó la respectiva denuncia en fiscalía, así como en el Ministerio de Educación (Vistazo, 2023). Por tanto es cuestión de tiempo para que ésta práctica maliciosa se popularice en nuestro país a tal punto que surja alguien que utilice esta herramienta con mala fe, en las cuales las mujeres son susceptible a ser víctima de los "deepfake".

El "deepfake" son sumamente realista, con pocos porcentajes de errores, se constituye por un intercambio de caras, a menudo son utilizados para insertar a actores famosas en acciones que nunca hicieron, en su mayoría las víctimas son mujeres para crear contenidos pornográficos manteniendo una sincronización casi perfecta de todas las características faciales, movimiento musculares de la boca con el audio original del contenido sexual. Por lo tanto el uso malicioso de los "deepfakes" supone una amenaza para figuras públicas como no públicas, así como las vulneraciones de derechos personales como son: el derecho a la intimidad personal como la intimidad familiar, el honor, la reputación, la imagen y voz.

Por ésta razón, resulta absolutamente necesario cuestionar el alcance de la normativa ecuatoriana para hacer frente a estas situaciones, debido a que hasta el momento no existe legislación específica, por lo que podría recaer en un grave vacío normativo que traería serias consecuencias al futuro y en las víctimas del "deepfake" en la que este acto puede quedar en la impunidad.

Ésta investigación sirve para identificar y comprender los riegos legales relacionados con la creación y difusión de "deepfake", y así poder establecer un precedente para poder desarrollar políticas públicas y regular esta problemática actual, desde el enfoque del desafío legal, como es la necesidad de establecer leyes específicas para el manejo malicioso de contenidos audiovisuales creados con la inteligencia artificial, he imponer la respectiva sanción al infractor como pena privativa de libertad proporcional al acto cometido y su respectiva reparación integral a la víctima.

Los beneficiarios directos de ésta investigación, son mujeres quienes son la más afectadas en este tipo problemas del "deepfake" pornográfico, por otra parte los beneficiarios indirectos son los abogados y estudiantes de carrera de derecho y personas interesadas en el tema, para que puedan tener conocimientos tanto a nivel académico como en el ámbito profesional, ya que es un tema emergente, relevante y sobre todo actual.

1.3. OBJETIVOS

Objetivo General

Analizar el impacto del "deepfake" en el derecho a la intimidad y sus dificultades probatorias en el Ecuador, a través de un estudio documental y de derecho comparado, para establecer la pertinencia de una reforma al COIP, que tipifique esta infracción penal.

Objetivo Específicos

1. Estudiar la definición doctrinal y dogmática del "deepfake".
2. Determinar cuáles son las dificultades probatorias del "deepfake".
3. Establecer a través del derecho comparado el "deepfake" y su aplicabilidad en el Ecuador.

CAPÌTULO ll MARCO TEÓRICO

ESTADO DEL ARTE

Acerca del tema: "Deepfakes", las dificultades probatorias, y su incidencia en la vulneración al derecho de intimidad, no existen trabajos de investigación similares, pero si hay investigaciones de enfoque general, de la siguiente manera:

Lavanda (2022), en los artículos publicados en Lawgic Tec - Revista de Derecho y Tecnología, realizó un trabajo de investigación titulado: "Deepfake": Cuando la inteligencia artificial amenaza el Derecho y la Democracia" y concluye:

El mal uso del "deepfakes", genera una amenaza para figuras políticas como no políticas. Generalmente estos videos, están creados con fines delictivos, específicamente en la generación de pornografía no consentida. Los "deepfakes" pornográficos actualmente posee un tema bastante complejo, en razón de la persona afectada quién sufre múltiples vulneraciones de sus derechos personales, como son; el derecho a la intimidad de forma personal así como de su familia, el derecho al honor y el buen nombre, derecho a la imagen y el uso de la voz no consentido así como expresiones faciales y voz, entre otros (p. 87).

Cerdan et al. (2019), perteneciente a la Universidad Complutense de España, realizó un trabajo de investigación titulado: "Historia "deepfake" audiovisual: "deepfake" y la mujer en un escenario imaginario, falsificado y perverso," y concluye que:

El "deepfake" tiene una perspectiva del presente y futuro en relación a la desinformación y la falsedad. El común de la sociedad, no puede determinar la veracidad o falsedad del video o imagen, pues solo se pude detectar con programas, el "deepfake" crea una máscara de una persona y sobreponer en el cuerpo de otra persona en un vídeo, en movimiento. Se ha confirmado que es una herramienta muy peligrosa que atenta contra la imagen de las mujeres. La investigación sobre esta problemática, se ha determinado ya existieron varios casos de personas públicas entre ellas: Scarlett Johansson, Gal Gadot y Emma Watson supuestamente actuando en vídeos pornográficos (p. 89).

Dvořáková, (2020), estudiante de doctorado en el Departamento de Derecho Constitucional y Ciencias Políticas Facultad de Derecho de la Universidad de Masaryk y asistente de un juez del Tribunal Supremo Administrativo en la República Checa, realizó un trabajo de investigación titulado: "Porno de venganza y "deepfakes": protección privacidad en la era de las tecnologías modernas" y concluye lo siguiente:

La pornografía "deepfake" apareció en 2017 y cada vez se ha ido extendiendo rápidamente. Generalmente son utilizados para realizar vídeos pornográficos falsos, que parecen muy reales, en estos videos aparecen mujeres en el cual el autor de dicha creación, quiere dañar la reputación personal de la víctima. Por tal motivo, personas famosas han sido el centro de atención que los internautas desean ver desnudas, e inclusive personajes políticos con la finalidad de desacreditarlos y poner en tela de duda el buen nombre, con vídeos de este tipo (p. 51).

Celebi et al. (2022), perteneciente al departamento de Informática en la Universidad Estatal Sam Houston, Huntsville, TX, EE.UU, realizaron un trabajo de investigación titulado: "Un estudio sobre la detección de falsificaciones en profundidad para los tribunales de primera instancia" y concluye lo siguiente:

La existencia de desafíos en el ámbito de la dificultad probatoria, se relaciona con el avance de la tecnología y su impacto en la autenticación de pruebas en el contexto judicial. La presencia de Redes Generativas complica aún más este panorama, ya que estas redes están diseñadas para mejorar continuamente y pueden producir videos pornográficos "deepfakes" cada vez más convincentes. Esto refiere a que en el futuro próximo, la dificultad probatoria aumentará significativamente, ya que incluso los expertos pueden no ser capaces de discernir la autenticidad de las pruebas digitales. En consecuencia, es fundamental que el sistema legal desarrolle estrategias y estándares robustos para abordar estos desafíos y garantizar la integridad del proceso judicial (p. 320).

Soler (2023) es Doctora de Derecho Procesal, profesora en la Universidad de Valencia, Abogada y politóloga, realizó un trabajo de investigación acerca de la inteligencia artificial y defensa planetaria titulado: "Retos jurídicos derivados de la Inteligencia Artificial Generativa" y concluye lo siguiente:

Existe la necesidad de contar con una competencia judicial avanzada, refinada y altamente especializada, que puede incluso requerir la participación de la propia inteligencia artificial, para identificar los vídeos falsificados. Es de suma urgencia garantizar la disponibilidad de personas dentro del poder judicial que posean experiencia en el ámbito de la investigación digital, particularmente con respecto a las redes generativas de confrontación, a fin de proporcionar información lúcida que pueda moldear los criterios empleados por quienes tienen autoridad judicial para aceptar o rechazar las pruebas o, alternativamente, asignarles el valor probatorio adecuado.

Estas investigaciones indican que los vídeos pornográficos de "deepfake", que constituyen la mayoría disponible en Internet, son particularmente perjudiciales. La aparición de la tecnología "deepfake" también pone de relieve la difícil situación que se está desarrollando en el ámbito legal y de la privacidad de la víctima, en este contexto, está estrechamente vinculada a las nociones de dignidad, autonomía y manifestación de la propia identidad.

ASPECTO TEÓRICO

UNIDAD 1. DERECHO A LA INTIMIDAD Y SU AMBITO NORMATIVO

1.1.1 ANTECEDENTES DEL DERECHO A LA INTIMIDAD Y SU PROTECCIÓN LEGAL

Los derechos humanos en el siglo XIX y a inicios del siglo XX, no eran considerados a nivel social, las normas para su protección eran limitadas. Luego de la Segunda Guerra Mundial, adquirieren la importancia verdadera, es menester mencionar el significado de derechos humanos, pues se define como aquellos derechos indispensables para el desarrollo de una vida digna y plena, entre ellos destacan el derecho a la intimidad. Aquí algunos antecedentes históricos normativos del derecho a la intimidad:

***Common Law* y la protección de la propiedad privada (siglos XVIII-XIX):** esta ley jugó un papel crucial en el desarrollo de la privacidad. Las primeras formas de protección se centraban en la inviolabilidad del hogar y la correspondencia. Es así que desde este enfoque se revela la conexión intrínseca entre la preservación de los derechos de propiedad y el desarrollo de su vida privada, por primera vez.

(Janariz, 1996) menciona que en el año de 1890 Samuel D. Warren y Louis D, escribieron un artículo jurídico respecto a la discusión sobre el derecho a la intimidad bajo el título " El derecho a la privacidad" en la revista de leyes de Harvard, el cual ha sido uno de los artículos más citados por la doctrina y jurisprudencia norteamericana, además en EEUU, define la privacidad como un derecho a no ser molestado y respetar su soledad si así lo desea.

El artículo 12 de la Declaración Universal de Derechos Humanos [DUDH]: establece el derecho a la privacidad y a la protección contra injerencias arbitrarias en la vida privada, la familia, el hogar y la correspondencia (ONU, 2015, art.12). El texto destaca la importancia de salvaguardar el derecho a la intimidad personal y familiar, resguarda la esfera privada de las personas, frente a intervenciones indebidas.

Pacto Internacional de Derechos Civiles y Políticos (PIDCP): El artículo 17 menciona sobre el derecho a la privacidad en el cual nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, ni en su domicilio, ni de su familia, no puede haber ataques ilegales a reputación y su honra, toda persona tiene derecho a la protección ante la ley (Barrera, 2012). Éste artículo refleja la preocupación de la comunidad internacional por preservar la esfera personal y familiar de las personas contra intervenciones arbitrarias por parte de los gobiernos u otras entidades.

Convención Europea de Derechos Humanos [ECHR]: En su artículo 8 menciona que toda persona tiene derecho al respeto de su vida privada y de su familia, de su domicilio y correspondencia. No podrá haber injerencia de la autoridad pública, sino solo cuando esta injerencia esté prevista por la ley, necesarias bajo ciertas condiciones" ([ECHR], 1950, art.8). Este artículo establece ciertos límites a este derecho, permitiendo la intervención de

la autoridad pública en situaciones específicas siempre que se cumplan ciertos criterios legales.

En la Jurisdicción Ecuatoriana, el término privacidad se introdujo por primera vez en la Constitución de 1978. Posteriormente la Carta Magna de 1998 incluyó el derecho a la inviolabilidad del domicilio y la correspondencia, esta legislación garantizaba que las personas tuvieran el derecho civil a mantener la confidencialidad en relación sus creencias políticas y religiosas, por lo que es prohibido divulgar información de una persona ni compartirla con terceros, como por ejemplo los datos de salud o la vida sexual, si no es con fines médicos. Y es así que la Constitución de la Republica de Ecuador [CRE] de 2008 reconoce y garantiza los derechos de libertad y entre ellos se encuentra el derecho a la privacidad personal y familiar en el literal 20 del artículo 66.

1.1.2 Definición del derecho a la intimidad

El derecho a la intimidad es un derecho fundamental que protege la esfera más privada del individuo, etimológicamente el término intimidad deriva del latín *"intimus*" que significa, lo que está más adentro, lo más profundo, lo interior de una persona. El derecho a la intimidad es el respeto a la personalidad humana, al aislamiento del hombre, lo íntimo de cada persona, la vida privada innata, inherente y necesaria para el desarrollo de una vida plena, sin perturbaciones y publicidades indeseada(Quiroga, 1995).

Martínez (2000), define al derecho de la intimidad, de la siguiente manera: "El derecho a la intimidad es aquel derecho humano que toda persona física tiene la facultad y el poder de excluir a las demás personas, sobre el conocimiento de la vida personal" (p.3). En esta definición refiere a la vida reservada de las personas, pues constituye un secreto para los demás, se aparta del conocimiento público, es un aspecto que cada individuo desea mantener oculto a los demás.

Según Mejan (1996) menciona que "El derecho a la intimidad se encuentra protegido constitucionalmente, este derecho es irrenunciable, inalienable e imprescriptible por su naturaleza jurídica" (p.3). Este derecho garantiza a los individuos el control sobre ellos desde el momento de su nacimiento al que no pueden renunciar, y no acaba conforme pasa el tiempo, además este derecho no se puede enajenar, no se lo puede vender.

El derecho a la intimidad, se presenta como un derecho a la libertad, ya que el individuo puede hacer lo que le parece, específicamente a estar solo, a no ser incomodado, y tomar decisiones en su esfera privada sin la intervención del estado, entre estas decisiones están las siguientes: la libertad sexual, libertad de revelar o no conductas íntimas, la libertad de actuar libremente en su domicilio, la libertad a la identidad, particulares que se encuentran establecidas en al art 66 del CRE.

En tal sentido derecho a la protección de datos garantiza al ciudadano el poder de uso y disposición sobre los mismos. Además podemos mencionar que la sentencia 001-14-PJOCC de la Corte Constitucional del Ecuador, refieren al derecho a la protección de datos, denominado "autodeterminación informativa", lo cual refiere a la protección de otros

derechos constitucionales, que pueden verse afectados derechos como: la intimidad, la honra, buen nombre (Corte Constitucional, 2014, p. 6).

1.1.3 Características del derecho a la intimidad

Algunas de las características claves del derecho a la intimidad son las siguientes:

1. Es un Derecho Fundamental: El derecho a la intimidad es considerado como un derecho fundamental, inherente a la dignidad humana, los derechos fundamentales se destacan por ser la base de una sociedad justa y democrática, garantiza la protección de todos los individuos frente a posibles violaciones de sus derechos. Está reconocido en varios instrumentos internacionales, es originario porque nace con el sujeto activo, es personalísimo debido a que solo puede ejercitarlo el titular, es irrenunciable no se puede renunciar, es imprescriptible no prescribe con el pasar del tiempo

2. Protege la vida privada: El núcleo del derecho a la intimidad incluye la protección de la vida privada de las personas, lo cual implica la esfera doméstica, las relaciones familiares, la correspondencia y otros aspectos de la vida personal que no deberían ser objeto de injerencias arbitrarias. La legislación y regulación adecuadas son fundamentales para que se respete y proteja este derecho en todos los ámbitos de la vida.

3. Inviolabilidad del Hogar y la Correspondencia: Muchas legislaciones reconocen la inviolabilidad del hogar y la correspondencia, en la cual las autoridades no pueden ingresar a la vivienda o la correspondencia sin orden judicial debidamente motivada. Estos derechos están en la esfera privada de las personas debe ser respetada y protegida.

4. Protección contra Injerencias Arbitrarias: Refiere a que las personas están protegidas contra injerencias arbitrarias o ilegales en su vida privada. La intromisión del Estado u otras autoridades debe cumplir los fundamentos legales y estar motivada jurídicamente. La protección contra injerencias arbitrarias es esencial para garantizar la preservación de los derechos individuales

5. Derecho a Controlar la Propia Información: Toda personas tienen el derecho de controlar la información que comparten sobre sí mismas, en el ámbito físico o digital. De la misma forma las personas tienen el derecho de solicitar que se elimine, rectifique o se limite el acceso a información, irrelevante o inexacta de las mismas, un claro ejemplo es una base de búsqueda en línea.

6. Protección contra Difamación y Calumnia: Implica la protección contra ataques ilegítimos a la reputación y el buen nombre de una persona, debido a que se considera una violación al derecho de intimidad. Por otra parte la difamación refiere a la publicación de falsas afirmaciones que perjudican la reputación de una persona y pueden perjudicar a su buena imagen ante sociedad.

8. Derecho a la Protección Legal: Las personas tienen el derecho a buscar protección legal y reparación vulneración de su derecho a la intimidad. Este derecho implica que todos los individuos tienen el derecho a acceder a la justicia, a recibir un trato justo. Así lo menciona el art 75 de la [CRE], respecto a que toda persona tiene el derecho a acceder de

manera gratuita a la justicia y a la tutela judicial efectiva, expedita e imparcial, sujetos al principio de inmediación y celeridad ([CRE], 2008, artículo. 75).

1.2. Derecho a la intimidad en los instrumentos internacionales

El derecho a la intimidad ha sido motivo de creciente preocupación para los organismos internacionales, dada la gravedad de las implicaciones que conlleva su violación. Entre los principales documentos que abordan el derecho a la intimidad, se destacan los siguientes:

Tabla 1 *Instrumentos Internacionales*

Instrumento internacional	Artículo	
[DUDH]	Art. 12	Ninguna persona será víctima de injerencias en su vida privada, ni en contra de su familia, correspondencia y domicilio, tampoco contra su honra y reputación. Todas personas tiene el derecho a la protección ante la ley por dichas injerencias ([DUDH], 1948, art. 12). Éste artículo subraya la prohibición de injerencias en la vida privada, de la familia, domicilio o correspondencia de cualquier individuo, además, garantiza el derecho a la protección legal.
[PIDCP],	Artículo 17. Núm. 1	El [PIDCP], determina en su Artículo 17. Núm. 1. Ninguna persona será objeto de injerencias ilegales, arbitrarias en su vida privada, ni la de su familia, domicilio y correspondencia, tampoco a su honra o reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias ([PIDCP], 1996, art. 17). Establece claramente que toda persona tiene derecho a la protección legal contra esta violación del derecho a la intimidad, subrayando la importancia de resguardar la integridad personal y social mediante la aplicación de la ley.
Convención Americana sobre Derechos Humanos o Pacto de San José (OEA	Artículo 11	1. Toda persona tiene derecho al respeto de su honra y dignidad. 2. Ninguna persona será víctima de injerencias, en su vida privada, ni la de su familia, domicilio, correspondencia. 3. Toda persona tiene derecho a la protección de la ley contra dichas injerencias ([OEA], 1978, art. 11). Este artículo resalta los derechos fundamentales relacionados con la dignidad y el respeto a la honra de toda persona.
Convención Europea para la protección de los Derechos Humanos y Libertades Fundamentales	Artículo 8	8 numeral 1. Todas las personas tienen derecho al respeto de vida privada y la de su familiar, su casa y su correspondencia. 2. No debe existir intromisiones de una autoridad pública, excepto aquella establecidas por ley, con la finalidad de obtener una sociedad democrática, la prevención del desorden y el crimen, seguridad pública, la protección de la salud (Convención Europea para la protección de los Derechos Humanos y Libertades Fundamentales, 1950, art. 11).

Autor: Franklin Sinaluisa

1.3 Derecho a la intimidad en la legislación Ecuatoriana

Con respecto al análisis jurídico en la legislación ecuatoriana, la violación del derecho a la intimidad, se determina por la ausencia de consentimiento para acceder a la información y utilizarla de manera maliciosa, por tal motivo, hay que tomar en cuenta el art 11 númeral 19 de la Constitución, la cual garantiza el derecho a la protección de datos de carácter personal, así como el acceso, decisión sobre su información y sus datos, la distribución y difusión de estos datos o información requerirán 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 que resguarde la intimidad frente a posibles intromisiones, asegurando así la dignidad y autonomía de las personas, fortaleciendo una sociedad democrática y respetuosa de los derechos individuales.

El derecho al acceso universal a las tecnologías de información y comunicación, el núm. 2 del art. 16 de la Constitución ecuatoriana, garantiza la libertad informática. El derecho de libertad tecnologías de información y comunicación ([CRE], 2008, art. 16, núm.2). Este derecho es de carácter inherente al desarrollo de la personalidad humana, entonces con el apoyo de los derechos reconocidos en la Constitución y los tratados internacionales, se da la necesidad de extender la tutela de derechos de forma indispensable, como es a la intimidad, ante el usos malicioso de otras personas .

El Código Orgánico Integral Penal, tipifica a los delitos contra el derecho a la intimidad personal y familiar, haciendo énfasis en vulneración del derecho a la intimidad determina lo siguiente:

Art. 178. Será sancionada con una pena privativa de libertad de uno a tres años, la persona que sin contar con el consentimiento, la autorización legal, intercepte, acceda, retenga, examine, reproduzca, grabe, publique datos personales, difunda, información contenida en un soporte informático, comunicaciones privadas de otras personas (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 físicos o digitales. La sanción establecida refleja la importancia de preservar la privacidad de las personas en el entorno digital.

En Ecuador tenemos 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 sin costo al archivo, para su ratificación, actualización de datos, anulación o eliminación de datos, que será autorizado por la ley o por el titular de derecho, además se adoptará medidas necesarias, si no se tiene su petición, podrá demandar por los perjuicios ocasionados ([CRE], 2008, art. 92, inc. 3ero). El derecho a la intimidad, es un bien jurídico protegido, merece determinadas protecciones, frente al desarrollo de las nuevas tecnologías a nivel nacional e internacional, este derecho individual es indispensable en sociedad contemporánea.

La Ley Orgánica de Protección de Datos Personales: El objetivo de esta norma es garantizar el derecho a proteger la información personal, tiene la capacidad de acceder y determinar el manejo de sus datos, además de proporcionar las garantías adecuadas. Con el fin de establecer, anticipar y desarrollar derechos, deberes y medidas de protección (LOPD] 2021, art.1). Este derecho incluye la capacidad de acceder y controlar el manejo de dichos datos, además de ofrecer garantías adecuadas. La legislación anticipa y desarrolla conceptos, derechos, deberes y medidas de protección esenciales, destacando su enfoque preventivo y proactivo para salvaguardar la privacidad de los individuos.

1.4 "Deepfake" y la vulneración al derecho a la intimidad

El derecho de intimidad, relacionándola con las nuevas tecnologías y la IA, como los "Deepfakes", este derecho tiene muchas posibilidades de ser vulnerado a través de internet con autores anónimos, pero hay que destacar que con la información digitalizada corre el riesgo que pueda ser ilegalmente difundidos, ya que los datos de una persona quedan públicamente expuestos en el ciberespacio.

Con la creación de las nuevas tecnologías, el bien jurídico más susceptible de ser lesionado es el derecho a la intimidad, algunos usuarios de internet disfrazan su identidad por medio del anonimato y utilizan como complemento la dificultad de rastreo (Castells, 2001, p.193). El texto destaca una preocupación relevante en la era de las nuevas tecnologías, haciendo hincapié en que el derecho a la intimidad se ha vuelto especialmente susceptible a lesiones. Esta reflexión resalta la dualidad de la tecnología, ya que, si bien ofrece numerosos beneficios y oportunidades, también plantea desafíos en términos de seguridad y privacidad.

Desde este enfoque, debemos mencionar que la Constitución toma en cuenta que el individuo desea excluir información que una persona determina como suya, del conocimiento público y de las intromisiones de terceros, por lo tanto el derecho a la protección de datos que "tiene como objeto garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso he impedir su difusión ilícita y lesiva" (Téllez, 2001, p. 73).

Existe 4 tipos de manipulación facial para generar "deepfakes", los cuales son los siguientes: Síntesis facial completa: Aquí se crea rostros a partir de redes generativas antagónica (GANs). Manipulación de características tales como color de ojos, pelo, edad o agrega accesorios como gafas o sombreros entre otras, mediante redes. Intercambio de expresiones trata de cambiar las expresiones de una persona por la de otra. Intercambio de identidad, este como el nombre indica, intercambia el rostro de una persona por otro proveniente de algún video, por técnicas basadas en gráficos por computadora o por aprendizaje profundo (Tolosana et al, 2022).

Los "deepfakes" representan una seria amenaza para el derecho a la intimidad de las personas en la era digital. Estas tecnologías permiten la creación de contenido audiovisual falso y convincente, donde se pueden superponer los rostros de personas reales en videos o imágenes de manera realista. Esto plantea riesgos significativos de difamación, acoso, extorsión y otros delitos que vulneran el derecho a la intimidad de los individuos.

En términos legales, la creación y difusión de “deepfakes” sin consentimiento pueden constituir diversos delitos, dependiendo de la naturaleza y el propósito del contenido manipulado. Sin embargo, la naturaleza novedosa y compleja de los “deepfakes” presenta desafíos adicionales para la aplicación efectiva de la ley, como la dificultad para identificar a los responsables y establecer la autenticidad del contenido manipulado.

Para abordar esta problemática, es crucial que los sistemas legales adapten sus marcos normativos y procedimientos para prevenir y castigar la creación y difusión de “deepfakes” sin consentimiento. Esto podría implicar la implementación de leyes específicas que prohíban la creación y difusión de “deepfakes” con intención maliciosa. De ahí la importancia de concientizar a la sociedad sobre los riesgos de los “deepfakes” y la promoción de la educación digital para ayudar a las personas a proteger su privacidad.

Los “deepfakes” de sexo es un medio que utiliza inteligencia artificial para insertar digitalmente la imagen de una persona en videos y fotos sexuales sin su consentimiento. La creación no consensuada requiere que una persona tenga acceso a las fotos y videos de otra persona que se pueden encontrar a través de videos públicos subidas en diferentes plataformas de redes sociales.

Es importante mencionar que el internet es un espacio abierto, en la cual se puede encontrar información de todos, siempre que el dueño por voluntad subió algún tipo de dato o información, es así que hay la necesidad de establecer relaciones jurídicas y elementos vinculantes de carácter normativo y de control para el uso de la tecnología de manera maliciosa.

La amenaza es considerable debido a su creciente capacidad para imitar la realidad de manera notable, con el avance de la IA, se vuelen más complejo y potente, esto gracias a la abundancia de imágenes disponibles en internet, y en las redes sociales, en la que facilita a personas inescrupulosas la creación de “deepfakes” pornográficos. Su aplicación no es ética ya que se utilizan principalmente con propósitos mal intencionados y perjudiciales a la intimidad de la víctima.

UNIDAD 2 DEEPFAKE COMO DELITO SEXUAL INFORMÁTICO

2.1 Historia, evolución y Conceptualización

2.1.1. Historia del “deepfake”

El video inicial de “deepfake” fue producido por un usuario de Reddit, que optó por utilizar los rostros de personas conocidas como Gal Gadot, Maisie Williams y Taylor Swift, y superponerlos a los cuerpos de actrices de películas pornográficas (Cole, 2017). Esto ilustra claramente la capacidad de generar vídeos que dan la impresión de que están siendo interpretados por celebridades. Este tema es preocupante y controvertido, debido a que los “deepfake” generan vídeos falsos, con los rostros de personas famosas superpuestos en escenas explícitas.

El usuario, empleó su computadora personal un algoritmo de aprendizaje automático al que se puede acceder fácilmente para su descarga desde Internet. Estos vídeos se publicaron posteriormente al sitio web Reddit, creada en 2005 por Steven Huffman y Alexis Ohanian, en Massachusetts. Reddit sirve como un sitio web social donde los usuarios pueden subir texto, imágenes, vídeos o enlaces (Cole, 2017). Esta práctica plantea serias inquietudes éticas y de privacidad, ya que puede dar lugar a la difamación, la manipulación y el acoso. El hecho de que un usuario de Reddit haya sido capaz de producir este tipo de contenido resalta el mal uso de la tecnología, lo que podría tener consecuencias negativas en la integridad de la información.

Fue dentro de este sitio web, donde los vídeos de "deepfake" inicialmente ganaron popularidad y comenzaron a difundirse. Es así que según Beamonte (2018), manifiesta que, "la tendencia resultante acumuló un número significativo de seguidores, lo que llevó a los "Deepfakes" a crear un subreddit dedicado exclusivamente a este género de vídeo. Sorprendentemente, en tan solo dos meses, esta comunidad atrajo a 15 000 suscriptores" (p.129). La tendencia en la creación de contenido "deepfake" que ha ganado popularidad rápidamente. La acumulación de un número significativo de seguidores para este género de vídeos indica un interés creciente en esta tecnología.

El desarrollo no concluyó ahí. Para simplificar el proceso, otro usuario de Reddit llamado Deepfakeapp presentó una aplicación conocida como Fakeapp. Este software permite a las personas, independientemente de su nivel de dominio de la informática, crear sus propios videos utilizando inteligencia artificial (Cole, 2017). Aunque la aplicación puede emplearse para fabricar vídeos de cualquier naturaleza, parece que existe un interés predominante en generar pornografía falsificada.

2.1.2. Evolución del "deepfake"

Los "deepfakes" fue creado por académicos e investigadores, ésta tecnología está al alcance de cualquier persona que tenga conocimientos básicos de informática, se origina como una herramienta para crear pornografía falsa, con las caras de celebridades femeninas, interpuestas en los cuerpos de estrellas porno, realizando actos sexuales que jamás hicieron, este problema fue realizado en el mes de diciembre del año 2017, cuando un usuario de Reddit, popularizó esta actividad, el nombre con el que se denominó a al video "deepfake" el cual se compone de dos términos " deep learnig" y "fake", tiene como objeto de crear contenido multimedia hiperrealista.

La evolución de los "deepfakes" presenta una expansión y dispersión, en los que se produce contenidos tanto benéficos como delictivos, las formas de expresión benéfica de los "deepfakes" aportan nuevas expresiones audiovisuales que a coadyuvaban al desarrollo educativo en diferentes ámbitos como es la medicina, ciencia, la moda, el comercio electrónico, la política, etc. Ésta evolución se nutre gracias a los constantes cambios tecnológicos de producción imágenes y sonidos mediante la IA, sobre todo de los contenidos encontrados en las redes sociales, plataformas digitales, las bases digitales (big data).

El uso negativo de estas tecnologías ha tenido un impacto considerable, afectando a las víctimas poniendo en riesgo a la sociedad en general por el mal manejo de los "deepfake". La ciberdelincuencia ha ido en aumento del 26% anual, con gastos económicos considerables (Symatec, 2018). Según la base de datos Scopus, se registran 603 artículos sobre los "deepfakes" entre 2017 y 2021, estos artículos tratan de diversos temas de discriminación a la mujer, pornografía, desinformación, política, racismo, seguridad, ocasionando pornografía no consensuada, porno extorsión.

"Las herramientas que producen estos vídeos, es de acceso gratuito, que contienen técnicas de IA y el aprendizaje automático, incorpora numerosos videos y fotografías en un algoritmo capaz de generar máscaras humanas realistas" (Beamonte, 2018). Además, el software posee la capacidad de mejorar su rendimiento con el tiempo. Se enfoca en la accesibilidad de las herramientas necesarias para crear vídeos "deepfake", subrayando que están disponibles libremente. Esto plantea inquietudes sobre la facilidad con la que cualquier persona puede acceder a tecnologías avanzadas.

En estos vídeos ficticios, el rostro de una celebridad se sustituye por el de una actriz pornográfica, mientras que el cuerpo de esta última permanece inalterado. "Deepfakes" en Reddit perfeccionó aún más el software hasta el punto de que los usuarios puedan seleccionar fácilmente un vídeo en su ordenador, descargar una red neuronal asociada a un rostro específico de una base de datos de acceso público y transformar el vídeo de forma instantánea con solo pulsar un botón. Fue en esta misma plataforma donde los primeros vídeos de "deepfake" ganaron popularidad y comenzaron a circular.

Según Beamonte (2018), "esta nueva tendencia acumuló un gran número de seguidores, lo que llevó a "Deepfakes" a crear un subreddit dedicado exclusivamente a contenido de esta naturaleza, lo que ganó rápidamente popularidad en los principales portales de contenido para adultos, como Pornhub" (p.56). En consecuencia, la popularidad de los deepfake generó una creciente base de seguidores, estos videos llegaron a ser populares en sitios web pornográficos.

El efecto del uso de los "deepfake" en su versión negativa, es que marca un nuevo panorama oscuro que "marca un punto de inflexión en la guerra de la información", esto se debe a que, por un lado, permite que las noticias falsas aumenten debido a la velocidad del internet y sus mecanismo de funcionamiento sociales y por otro lado se reduce la credibilidad de los medios de información, sin haberlos comprobado previamente.

La popularización entre 2018 y 2019 se lanzaron herramientas para la generación de

"deepfake", entre una de ellas está Fakeapp, aplicación que se lanzó en 2018, consistía en crear videos falsos, y estaba al alcance del público en general, sin conocimiento técnico de manipulación de videos. Los 2 "deepfakes" comenzaron a mejorar significativamente en términos de realismo, mejoraron la sincronización de labios, y expresiones faciales gracias a los avances tecnológicos, redes neurales más sofisticadas.

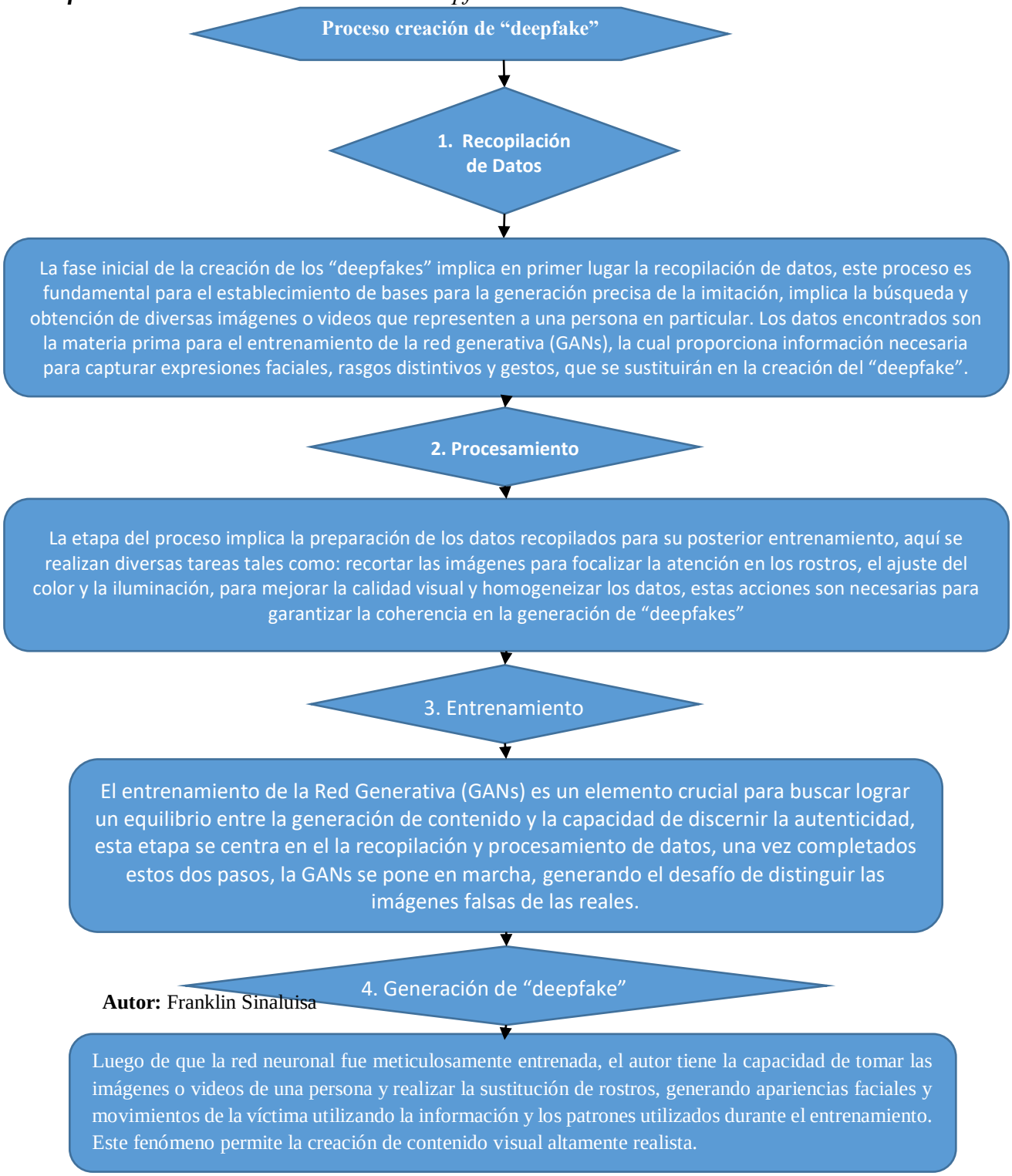
Las amenazas y los usos mal intencionados, con el aumento de la calidad de los deepfake, surgieron preocupaciones, sobre su uso para la desinformación, fraude y acoso.

Los gobiernos y plataformas, tecnológicas empezaron a regularse y a crear herramientas de detección de "deepfake". En 2020, por ejemplo Facebook implementó políticas para eliminar contenido manipulado que podría causar daños significativos.

Los avances recientes y Futuro, actualmente al año 2024, los "deepfake" han seguido evolucionando, con técnicas cada vez más sofisticadas, que permite no solo manipular rostros, sino también a modificaciones de voces y movimientos corporales completos, además de los usos maliciosos, existen aplicaciones positivas, que ayudan a la educación, entre otras cosas, por ejemplo, se ha utilizado para crear efectos visuales en películas o para preservar y recrear voces de personas fallecida.

2.1.3. Proceso de creación de un "Deepfake"

***Gráfico** 1 Proceso de creación de un "Deepfake"*



Autor: Franklin Sinaluisa

2.1.4. Aplicaciones y Usos

Muchas veces los creadores de estos videos pertenece a un ambiente más cercano de las víctimas estos pueden ser; amigos compañeros o ex parejas, para la creación se facilitan de aplicaciones muy accesibles en al cual recopilan fotos del perfil de una persona encontrada en su redes sociales, de forma pública. Es así que a continuación se establece los usos de le "deepfake", los cuales son los siguiente.

Suplantación de identidad: los "deepfakes" se pueden emplear para fabricar vídeos o imágenes que muestren a una persona realizando acciones o expresando puntos de vista en los que, en realidad, nunca participó. Este fenómeno puede generar suplantación de identidad y afectar a la reputación y la privacidad de la persona en cuestión. Además puede dañar potencialmente la imagen pública con esta difusión de información falsa y comprometedora lo que conlleva a tener consecuencias legales y sociales adversas

Contenido sexual falso: Una de las aplicaciones más desconcertantes de los "deepfakes" se refiere a la fabricación de contenido sexual. Tienen la capacidad de generar vídeos o imágenes que aparentemente muestran a una persona participando en actividades íntimas, que pueden difundirse sin el consentimiento de la persona y generar daños emocionales y sociales. Las víctimas de este tipo de manipulación enfrentan no solo traumas de ser objeto de una invasión a su privacidad y difamación pública, también amenaza y perjudica a sus relaciones personales, reputación e incluso oportunidades laborales

Amenazas y extorsión: la utilización de "deepfakes" en el ámbito de la privacidad puede generar amenazas y extorsión. Los creadores de "deepfakes" pueden aprovechar la amenaza de difundir material falso a menos que la persona afectada cumpla con exigencias específicas. Esta forma de explotación no solo puede causar daño emocional sino también psicológico a la víctima, sino que puede pude tener consecuencias devastadoras en su vida privada y profesional.

Daño psicológico: La revelación de los "deepfakes" puede provocar daños psicológicos a las personas afectadas. La conciencia de que es posible crear contenido falsificado que sea difícil de distinguir de la realidad puede fomentar un ambiente de desconfianza y ansiedad, esta sensación de incertidumbre y vulnerabilidad puede dar lugar a un aumento de niveles de estrés afectando negativamente a la salud mental de quienes se ven afectados por estas manipulaciones falsas.

Los daños que causan los "deepfakes" pornográficos, la víctima al ser reconocida por cualquier persona le pueden propinar improperios, y aún más atentar contra su integridad física y sexual, pero también existe una segunda víctima, que es la persona que apareció en el video original, la cual no dio el consentimiento de mostrar su cuerpo desnudo con la cara de otra persona.

2.2 Características del "deepfake"

Generación mediante Redes Neuronales: Los "deepfakes" se crean utilizando redes neuronales, en particular, modelos generativos como las Redes Generativas

Adversarias (GAN). Estos modelos son entrenados para aprender patrones y características de un conjunto de datos específico y luego generar contenido nuevo basado en ese aprendizaje. **Redes Generativas Adversarias (GAN):** Las GAN consisten en dos redes neurales, un generador y un discriminador, que operan de manera adversaria. El generador crea muestras sintéticas tratando de imitar un conjunto de datos específico, mientras que el discriminador evalúa si una muestra auténtica o generada. Estas redes, en general, se centran en aprender las distribuciones de probabilidad de los datos de entrenamiento y generar nuevos ejemplos que se ajusten a esas distribuciones.

Realismo: La principal característica distintiva de los "deepfakes" es su capacidad para crear contenido multimedia extremadamente realista y convincente. Esto incluye la capacidad de superponer el rostro de una persona en un video existente, cambiar expresiones faciales y sincronizar labios de manera precisa. Esta capacidad para crear contenido extremadamente realista puede ser utilizada para manipular información, difamar a individuos.

Manipulación Facial y de Voz: Los "deepfakes" pueden manipular no solo las imágenes visuales sino también las características faciales y la voz de una persona. A través de técnicas de síntesis de voz, los modelos pueden imitar con precisión el tono, la entonación y otros aspectos de la voz de una persona específica. Esto permite la creación de grabaciones de audio que suenan auténticas pero contienen palabras o frases que la persona nunca pronunció.

Uso de Grandes Conjuntos de Datos: La calidad de un "deepfake" a menudo depende de la cantidad y la calidad del conjunto de datos utilizado para entrenar el modelo. Estos datos son encontrados en el internet o redes sociales, en la que el autor puede acceder libremente, cuanto más grande y diverso sea el conjunto de datos, mejor será el modelo para capturar las sutilezas y detalles necesarios para crear "deepfakes" realistas.

Ética y Posibles Usos Malintencionados: Aunque los "deepfakes" tienen aplicaciones potenciales en la industria del entretenimiento y la creación de contenido digital, también plantean preocupaciones éticas significativas. Pueden ser utilizados para la difamación, el fraude, la desinformación y otros propósitos malintencionados. Representa una herramienta poderosa en manos equivocadas, cuya capacidad es generar contenido visual y auditivo realmente falso, con una sorprendente precisión que puede encadenar a en actividades fraudulentas, como la suplantación de identidad o creación de contenido falso con el fin de difamar a la víctima.

Generación de video: Crea videos completamente sintéticos de personas que no existen. En este caso, los modelos de deep learning se entrenan para generar videos de personas que son completamente ficticias y no tienen una contraparte en la realidad. La generación de videos porno tiene aplicaciones en la industria del entretenimiento, la creación de contenido digital y la animación, donde se pueden crear personajes completamente nuevos sin depender de actores reales.

2.3 Tipos de “deepfakes”

Algunos tipos comunes de “deepfakes” son:

1. “Deepfake” facial en videos: Reemplaza el rostro de una persona en un video con el rostro de otra. Esto puede utilizarse para cambiar expresiones faciales, gestos y hasta para hacer que una persona parezca decir cosas que en realidad no ha dicho. Este proceso no solo implica una simple superposición sino también puede ajustarse las expresiones faciales y gestuales de manera realista para coincidir con el contenido del video. Esta tecnología plantea preocupaciones éticas y de seguridad de manera significativa.

2. “Deepfake” de voz: En lugar de manipular un video, utiliza inteligencia artificial para imitar la voz de una persona. A menudo, se entrena con grabaciones existentes de la voz de la persona para crear un modelo que pueda generar audio que suena auténtico, ajustando el audio con los movimientos de la boca para que suene como si la persona estuviera verdaderamente hablando.

3. Imagen a imagen “deepfakes”: Los “deepfake” de imagen a imagen representa una preocupante tecnología en constante evolución. Este tipo de “deepfake” tiene la capacidad de modificar características específicas dentro de una imagen, lo que permite una amplia posibilidades creativas por parte del autor como es, el cambio de estilo de pintura de una obra de arte, hasta alterar el género de una persona , edad incluso el fondo de una fotografía, la versatilidad de esta herramienta es impresionante.

4. Generación de texto: Aunque son no tan común como los “deepfakes” visuales y de audio, existen tecnologías que pueden generar texto de manera realista, lo que podría tener aplicaciones en la creación de noticias falsas o mensajes fraudulentos. Utiliza un lenguaje avanzado para generar un escrito de una persona en particular, haciendo parecer real. Esta tecnología tiene la capacidad de producir textos que se asemejan notablemente al estilo y tono de escritura de una persona específica, imita la escritura de individuos particulares para generar fraude

5. “Deepfake” en tiempo real: Los “deepfake” en tiempo real representa un hito significativo en la evolución de esta tecnología, ya que implica el uso de algoritmos avanzados para realizar manipulaciones instantáneas durante transmisiones de video en vivo. Esta capacidad para alterar contenido visual en tiempo real plantea un riesgo inminente de desinformación, ya que las imágenes y los mensajes pueden ser distorsionados o falsificados en el momento mismo en que se transmiten. Esta técnica no solo aumenta la amenaza de desinformación, sino que también presenta desafíos adicionales en la detección y mitigación de contenido manipulado, dado el carácter instantáneo y dinámico de las transmisiones en vivo

Es importante señalar que, si bien estas tecnologías pueden tener aplicaciones creativas y útiles, también presentan riesgos significativos en términos de manipulación y desinformación. La lucha contra los “deepfakes” implica el desarrollo de herramientas para detectarlos y la promulgación de políticas y leyes que regulen su uso de manera ética y responsable.

2.4 El “deepfakes” en relación el Derecho comparado

Legislación española

El Parlamento Europeo presentó una propuesta de enmienda al Reglamento Europeo. Dentro de esta enmienda, el artículo 3144 incluye una definición de los “deepfakes”, que se refiere a una ultrafalcificación. Los “deepfake” abarca el contenido manipulado, en forma de audio, imágenes o vídeos, que posee la capacidad de fabricar una sensación ilusoria de autenticidad y veracidad, mediante la utilización de metodologías con la inteligencia artificial y el aprendizaje profundo. Para abordar los “deepfakes” el Parlamento Europeo (2021), realizó una proposición de Ley, “Ley de Inteligencia Artificial” que identifica los riesgos que derivan del uso malicioso de las tecnologías. Entre ellos abarcan los actos de difamación, coerción, engaño, manipulación de los medios de comunicación y las elecciones, el robo de identidad personal y el daño a la reputación, que también pueden implicar casos de acoso.

Las “Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial” (2019) del Consejo Europeo, destaca la importancia de garantizar los derechos de la ciudadanía europea, la adaptación y retos de las nuevas tecnologías. La Carta de los Derechos Fundamentales, en el contexto de la inteligencia artificial y el cambio digital abogaba por afrontar la complejidad, imprevisibilidad y sesgos derivados de ciertos sistemas tecnológicos.

La propuesta presentada en el Libro Blanco de la Unión Europea de 2020, sobre la inteligencia artificial, tiene como objetivo establecer una estructura legal, que armonice los principios fundamentales de la Unión Europea, que abarcan sus valores y derechos, ante el avance de la innovación científica. La legislación abarca varias modificaciones y prioriza las que se consideran más urgentes

Su artículo 1 propone modificar la Ley 13/2022 General de Comunicación Audiovisual. La difusión de “deepfakes” sin la autorización, o con el consentimiento expreso de la persona, ya que se considera un delito grave. Se determina una excepción a esta infracción, cuando el uso de estas tecnologías estén legalmente autorizado para detectar, prevenir, investigar y procesar actos delictivos, o cuando el contenido está claramente identificado ficticio.

El artículo 4 propone una enmienda a la Ley de Procedimiento Civil, introduciendo una medida cautelar específica que consista en eliminar las imágenes, vídeos o voces inventadas de personas generadas mediante sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial, a solicitud de las personas afectadas o sus representantes(Comisión Europea, 2020).

El artículo 7 sugiere una modificación de la Ley Orgánica, se refiere al Régimen Electoral General. La enmienda introduce un nuevo conjunto de normas relativas a la difusión maliciosa de imágenes y voces generadas por inteligencia artificial. La primera disposición adicional propone el establecimiento de un Consejo de Participación Ciudadana, que se encargaría de supervisar y evaluar la implementación de la inteligencia artificial .

El 13 de octubre de 2023, el Congreso de los Diputados publicó una propuesta de Ley Orgánica, la cual tiene como objetivo establecer normas para la simulación de videos, imágenes y voces de personas generadas con la utilización de inteligencia artificial, la propuesta fue presentada por el Grupo Parlamentario Plurinacional de SUMAR. El proyecto de ley, delimita un marco de regulación con el fin de salvaguardar los derechos fundamentales, en particular la preservación de los derechos a la dignidad, la intimidad (Congreso de Diputados, 2023).

Legislación de Estados Unidos/

En el estado de Virginia en 2019, el acto de distribuir vídeos pornográficos como represalia ya se ha considerado ilegal; sin embargo, la legislación ahora se ha revisado para incluir imágenes fijas o vídeos que muestran escenarios inventados. Las consecuencias de tales acciones incluyen penas de prisión de hasta 12 meses y multas a partir de 2.500 dólares. Esta enmienda responde a la constatación de que, hoy en día, las personas equipadas con software, herramientas e inteligencia artificial son capaces de generar vídeos falsificados en cuestión de horas.

A nivel federal, en los Estados Unidos, el Congreso aprobó en diciembre de 2018 la Ley de Prohibición de las "deepfake" con fines malintencionados, lo que la convirtió en la primera ley en definir formalmente este concepto. Posteriormente, en 2019, se introdujo la Ley de Responsabilidad de las "deepfakes". Sin embargo, recibió críticas considerables debido a sus definiciones vagas y a la posible amenaza que representaba para la Primera Enmienda de la Constitución de los Estados Unidos, que salvaguarda la libertad de prensa.

Ese mismo año, se aprobó la Ley de Denuncias "Deepfake", que obligaba al Departamento de Seguridad Nacional de los Estados Unidos a publicar periódicamente informes de evaluación sobre las tecnologías de las "deepfake". A nivel estatal, varios estados, como Virginia, Texas, California, Washington, Nueva York y Massachusetts, han promulgado leyes que especifican el uso permitido de las copias falsas en el contexto de las elecciones políticas y su explotación pornográfica.

Si bien el uso de los "deepfakes" no está regulado explícitamente a nivel federal en los Estados Unidos, cada estado tiene su propio conjunto de regulaciones que permiten a las víctimas emprender acciones legales en caso de que se violen sus derechos. Además, algunos estados han propuesto proyectos de ley destinados a proteger a las víctimas de los "deepfakes".

Uttamchandani (2022), abogado especializado en tecnología y privacidad, aclara además que estas regulaciones dependen de las leyes de cada estado individual (p.78). Texas es una de las jurisdicciones que proporcionan un marco legal sólido para emprender acciones legales en el contexto de la tecnología "deepfake", prohíbe expresamente la creación y difusión de vídeos engañosos destinados a dañar a los candidatos políticos.

En California, el proyecto de ley núm. 602 denominada "Derecho de Acción Privada" (2019) de la Asamblea tiene como objetivo introducir un mecanismo para que las personas representadas en pornografía falsa puedan emprender acciones legales a fin de

agilizar el proceso de denuncia de este tipo de incidentes. Otros estados, como Virginia y Nueva York, también han promulgado reglamentos sobre este asunto, aunque con algunas variaciones.

Legislación de México

Un proyecto de ley propuesto en México busca imponer sentencias de hasta 12 años de prisión a las personas que emplean inteligencia artificial para fabricar contenido íntimo engañoso. Propuesta para enmendar el código penal de la Ciudad de México aboga por la inclusión de la pornografía en el ámbito de los delitos contra la privacidad sexual. Un miembro de un partido político menciona que los "deepfakes" que incorporan representaciones sexuales pueden generar un daño irreparable de las personas.

Código Penal Federal, Libro Segundo, Título Séptimo Bis. Delitos contra la indemnidad de la privacidad de la información sexual. Capítulo II. Violación de la intimidad sexual. Se propone una reforma de la siguiente manear: Artículo 199 octies. La persona que comete el delito de violación a la intimidad sexual, comparta, divulgue publique, distribuya imágenes, videos o audios de contenido íntimo sexual, de una persona, sin su consentimiento, aprobación o su autorización. De igual manera quién videograbe, fotografíe, audiograbe, imprima, fotografíe o elabore, imágenes, audios o videos reales o simulados con inteligencia artificial con contenido íntimo sexual de una persona sin consentimiento, aprobación o autorización. Se sancionará con una pena 'privativa de libertad de tres a seis años y una multa de quinientas a mil Unidades de Medida y Actualización (Cámara de Diputados, 2023).

Iniciativa con proyecto de decreto por el que se adiciona el artículo 205 bis al Código Penal para el distrito federal, para la tipificación del contenido audiovisual modificado conocido como "deepfake" utilizado con fines degradantes e indebidos

Ley Olimpia (Ley de acceso de las mujeres a una vida libre de violencia de la ciudad de México)

Tras una larga lucha, en 2018 logró la aprobación de la ley "Ley Olimpia", la cual castiga el acoso digital y tipifica como delito contra la intimidad sexual grabar, tomar fotos o difundir imágenes o mensajes de contenido sexual sin consentimiento. La joven logró que se reconociera la violencia digital y se sancionara hasta con seis años de prisión a quienes comparten materiales íntimos sin

Artículo 7.- Modalidades de violencia contra las mujeres: Violencia digital es todo acto realizado por medio del uso de correo electrónico, , redes sociales, mensajes telefónicos, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se exponga, difunda, distribuya, reproduzca, exhiba, comercialice, transmita, intercambie, oferte, comparta imágenes, audios o videos reales o simulados de contenido sexual íntimo de una persona, sin consentimiento, que atente la intimidad, la dignidad, la libertad, la integridad, y la vida privada de las mujeres, causando daño, psicológico, económico, en el ámbito privado como en el público, así como daño moral, tanto a ellas como a sus familias.(Ley Olimpia, 2018).

Art 63. Las medidas u órdenes de protección en materia penal son consideradas personalísimas e intransferibles. Estas pueden incluir la interrupción, destrucción o eliminación de imágenes, audios y videos de contenido sexual íntimo de una persona sin su consentimiento, por cualquier medio digital como redes sociales o cualquier otro dispositivo móvil. (Ley Olimpia, 2018).

Art 72 TER.- En casos de violencia digital, la o el Ministerio Público o el Juez de la causa procederá el siguiente protocolo: I. La querella podrá presentarse vía electrónica o mediante escrito de manera presencial. El Ministerio Público tomara las medidas de protección necesarias de manera inmediata, solicitando electrónica o por escrito a las empresas de plataformas digitales, redes sociales o páginas web, y se realizará la respectiva eliminación de imágenes, audios y videos relacionados con la denuncia. (Ley Olimpia, 2018).

Artículo 20 Quáter.-Violencia digital refiere a cualquier acción intencional utilizando tecnologías de la información y la comunicación, incluyendo la distribución, difusión, transmisión, comercialización, oferta, intercambie imágenes de audios o videos reales o simulados de contenido íntimo sexual, sin consentimiento, aprobación o autorización, causando daño psicológico o emocional, en cualquier ámbito dela vida privada de la víctima. (Ley Olimpia, 2018).

Artículo 181 Quintus. Delito contra la intimidad sexual: I. La persona que mediante engaño audiograbe, videograbe, fotografíe o elabore, imágenes, audios o videos reales o simulados de contenido sexual íntimo. II. Quien con conocimiento exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos de contenido sexual íntimo de una persona mediante cualquier medio tecnológico, será sancionado con cuatro a seis años de pena privativa de libertad así como una multa de quinientas a mil unidades de medida y actualización. (Ley Olimpia, 2018).

UNIDAD 3 DIFICULTADES PROBATORIAS DEL “DEEPFAKE” EN EL CONTEXTO LEGAL

3.1 Rastreo del Origen

Los “deepfakes” representan un desafío judicial respecto al rastreo de su origen, así como las técnicas de generación de contenido falso dificulta una identificación precisa del origen, esto resulta una dificultad y obstaculiza la atribución de responsabilidad y la determinación de las pruebas presentadas. 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.

El origen de la grabación desempeña un papel fundamental en la identificación de un “Deepfake”. Se debe analizar a la persona que difundió por primera vez el archivo a través

de varias redes sociales o sitios web, así como las circunstancias que rodearon su publicación y los atributos específicos del archivo inicial que podrían ayudar a identificarlo.

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, tenemos un mensaje que se puede ver se puede revisar, si están encriptados, se puede desencriptar mediante pericia. Un claro ejemplo es un caso mediático que paso en la ciudad de Riobamba que paso con caso de Dana, la se obtiene los datos relevantes para la búsqueda de los posibles responsables del hecho a través de Whatsapp, Facebook. Por la altera Emilia que es un sistema de búsqueda rápida, en el que incluye apoyo internacional, para dar prioridad a un caso específico.

Rastreo de dirección IP

La dirección IP está definida como la identificación numérica que está 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.

Internet Protocol, es el término bajo las siglas IP, un concepto que cumple la función como un documento de identidad de una persona, este código es la forma más eficiente de saber quién es quién. Es por ello, que en varias ocasiones surge la idea de rastrear la dirección IP, en la que podemos conocer quienes han visitado un página web, a quién llegó un mensaje, de dónde salió le mensaje, quién fue el emisor, o conocer la dirección física con ayuda de la geolocalización.

La principal dificultad en la imputación de este acto ilícito a través de la dirección IP, es la identificación de actor, cuando de imputar este delito la dirección IP no proporciona la información suficiente para identificar al responsable, comúnmente esta dirección es propiedad de un proveedor de servicio de internet, y es utilizado para identificar al dispositivo que fue conectado al internet, pero no específicamente a la persona que utilizó el dispositivo.

Posee una numeración única para el dispositivo del emisor y también para el destinatario, independientemente del canal y el contenido o mensaje que se transfiera, al encontrar el dominio asignado en cada ordenador, 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.

Proveedores de Internet y los administradores redes sociales, 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.

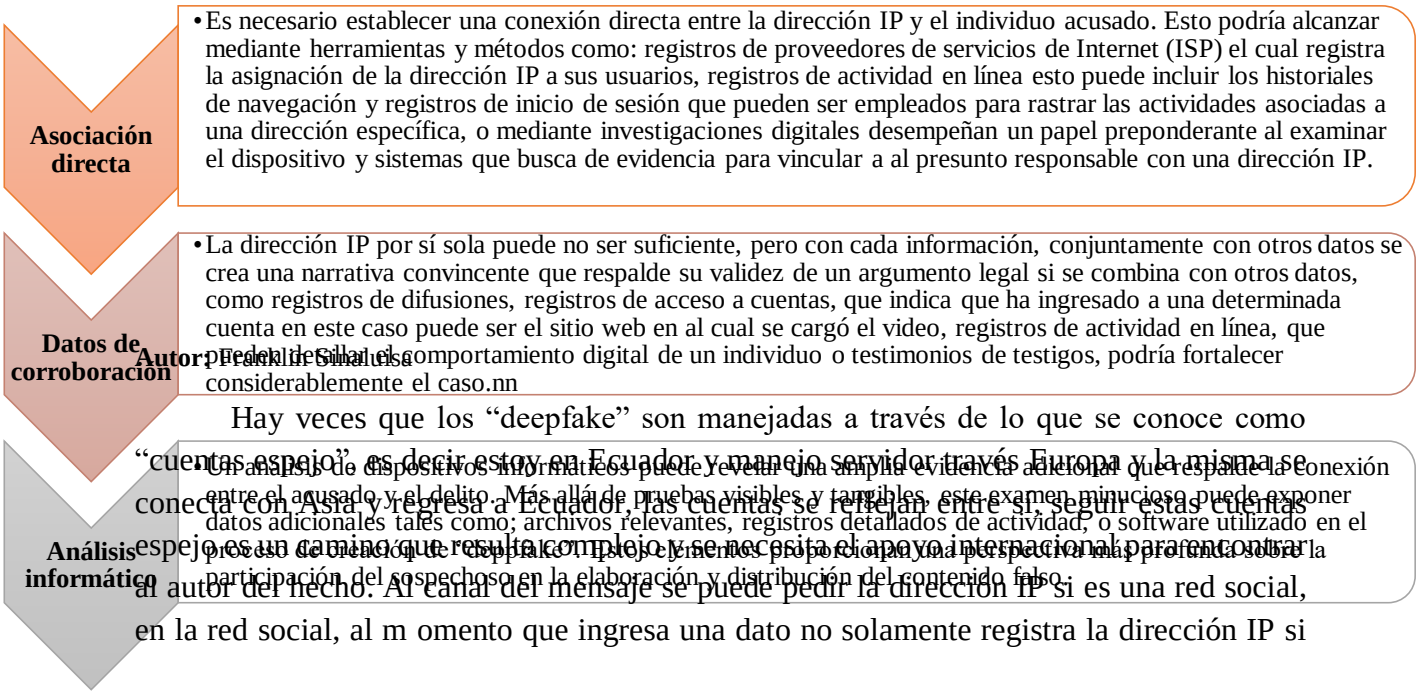
Las direcciones IP fijas son asignadas permanentemente a un dispositivo y no cambia con el tiempo, y pueden ser más fáciles de rastrear al usuario, mientras que la dirección dinámica están en constante frecuencia por tanto resulta más difícil rastrear la actividad informática. Las direcciones IP pueden ser compartidas con varias personas en por lo que dificulta la identificación del autor.

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 evidencia digital como lo es la dirección IP, registro de navegación, registro de trasferencia en line de contenido puede ser utilizado para establecer el nexo causal de esta actividad ilegal.

La evidencia digital debe ser obtenida conforme a lo establecido en la ley y así poder materializar al proceso judicial, para eso es imperante la participación de un perito informático especializado, con conocimientos en Inteligencia Artificial, de la misma manera abogados especializados en derecho digital para garantizar que la evidencia sea presentada bajo las condiciones de un debido proceso. En Ecuador tenemos un serio problema con los Cyber ya que no existe un control de registro con datos de cada persona al utilizar una computadora en la cual se puede estar cometiendo un delito como es la generación del "deepfake".

La dirección IP es considerado como un elemento probatorio, no puede ser tenido en cuenta como único elemento de convicción que pueda condenar a un acusado, pero se requerirá más elementos de convicción, pues la autoría del delito no queda suficientemente probada. Las garantías de identificación del acusado pueden depender de varios factores:

Gráfico 2 *Identificación del acusado*



Autor: Franklin Sinaluisa

Hay veces que los "deepfake" 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 reflejan entre sí, seguir estas cuentas espejo es un camino que resulta complejo y se necesita el apoyo internacional para encontrar al autor del hecho. Al canal del mensaje se puede pedir la dirección IP si es una red social, en la red social, al m omento que ingresa una dato no solamente registra la dirección IP si

no también lo que se conoce como la máscara que significa los código de cada equipo y sus características.

3.2 Pericias informáticas

Las pericias informáticas son fundamentales para determinar la veracidad de los contenidos digitales, incluidos los “deepfakes”. Expertos en informática (inteligencia artificial) deben aplicar técnicas especializadas para analizar la estructura del archivo, identificar anomalías y detectar manipulaciones. Sin embargo, la evolución constante de las herramientas de generación de “deepfakes” plantea un desafío en la capacidad de los peritos para mantenerse al día con las técnicas más recientes. La correcta aplicación de la pericia informática es esencial para garantizar la integridad de las pruebas digitales en los procedimientos legales.

Cuando encontramos el equipo con que se realizó el hecho, se inicia con un proceso que implica la recolección y preservación de evidencia digital asociada, lo cual es un proceso complejo que requieren de conocimientos especializados, comprensión profunda de tecnología y sistemas informáticos para garantizar que la evidencia digital sea recolectada de manera precisa y exhaustiva. Esto implica el uso de herramientas especializadas para extraer datos de dispositivos electrónicos así como también la compresión de comprensión de protocolos y procedimientos necesarios para preservar la integridad de la evidencia durante el proceso de recolección. Es un trabajo meticuloso que exige atención a los detalles y un compromiso absoluto con la respectiva objetividad y la imparcialidad que asegure a la evidencia para ser utilizada en la investigación legal.

3.2.1. Recopilación y preservación de la evidencia digital

Identificación y aseguramiento de evidencia: Destaca la necesidad de contar con un equipo digital para la recolección y aseguramiento de dispositivos pertinentes, como computadoras, dispositivos móviles, de servidores. Se realiza mediantes técnicas informáticas una copia para garantizar la cadena de custodia así como la integridad de los datos, incluso aquellos que fueron eliminados y que esta encriptados hay que destacar la importancia de contar con una cuidadosa cadena de custodia de la evidencia para preservar la autenticidad en todo el proceso de investigación en el proceso judicial.

Adquisición de la evidencia y explotación del Equipo.

Es de vital importancia el proceso para asegurar la recopilación y preservación adecuada de la información, para su posterior análisis, se detallan técnicas específicas para la adquisición de la evidencia digital, en computadoras como en teléfonos móviles, haciendo hincapié en la utilización de herramientas especializadas que garanticen la integridad de los datos y su autenticidad. Aquí también se incluyen la descripción de las características del equipo, como el color, color, marca, titular del esquipo. Por otra parte se puede solicitar a la empresa del canal ayude a encontrar la dirección IP o a su vez recuperar mensaje borrados.

Análisis de la evidencia.

El proceso de análisis de la evidencia digital implica examinar la información recopilada con la finalidad de buscar patrones, pistas relevantes para la investigación. Durante el análisis de la evidencia le perito informático utiliza un variedad de herramientas y técnicas para examinar datos, que son la siguientes.

Análisis de metadatos: examinar los metadatos incluye información de la fecha, hora, ubicación y los tamaños de los archivos, proporcionan pistas cruciales sobre las actividades de sospechoso. El análisis exhaustivo de metadatos abarca una variedad de aspectos cruciales que pueden ofrecer valiosas pistas sobre las actividades de una persona bajo sospecha. Más allá de simplemente examinar la fecha y hora de creación o modificación de un archivo, el análisis de metadatos profundiza en detalles como la ubicación geográfica asociada con la creación del archivo en la que revela si un archivo fue creado en un lugar específico, así como también los tamaños de los archivos pueden indicar la cantidad y el tipo de información que se estaba manipulando, lo que podría ser relevante para determinar la naturaleza de las actividades del sospechoso. Estos datos pueden proporcionar un panorama más completo de las acciones y movimientos del responsable.

Análisis de archivos: El análisis de archivos constituye un procedimiento integral en el ámbito de la investigación, que abarca tanto examinar de manera exhaustiva los archivos presentes como la recuperación de aquellos que pudieran estar ocultos o encriptados de difícil acceso. Este proceso no solo se limita a la mera identificación de los archivos, sino que también comprende la evaluación de su relevancia dentro del contexto de la investigación en curso. Dicha identificación se realiza con el propósito de discernir aquellos archivos que puedan proporcionar información significativa o esclarecedora para el caso en cuestión, permitiendo así avanzar de manera más efectiva en el análisis y la resolución del mismo.

Análisis de comunicaciones: El análisis de comunicaciones es esencial que se enfoca en examinar detalladamente los intercambios de información a través de diversos canales virtuales de comunicación, como correos electrónicos, mensajes de texto y llamadas telefónicas. Estos análisis tienen como objetivo principal identificar patrones de comportamiento que puedan proporcionar pistas clave para determinar la responsabilidad de individuos o grupos asociados a esta actividad. Al estudiar estas comunicaciones, los investigadores pueden obtener una comprensión más profunda de las interacciones entre las partes involucradas, detectar posibles conspiraciones o coordinaciones, y reconstruir la secuencia de eventos relevantes. Este enfoque analítico es fundamental en la investigación criminal, la inteligencia de seguridad y otros campos donde la identificación precisa de los responsables sirve para la resolución de casos

Análisis de redes sociales: analizar las redes sociales proporciona información realmente sobre actividades en línea de los actores y sus conexiones con otras víctimas. El análisis de redes sociales emerge como una herramienta invaluable en la comprensión de las interacciones y dinámicas en línea de los individuos. Al profundizar en estas plataformas, se obtiene un panorama de las actividades de los actores, así como también de sus relaciones y conexiones con otras personas implicadas. Este proceso revela no solo las acciones individuales, sino también los patrones emergentes y las estructuras subyacentes que pueden

estar presentes en la red. A través del estudio meticuloso de estas interconexiones, se puede identificar tanto a víctimas potenciales como a posibles perpetradores, lo que permite una intervención más efectiva y dirigida en la prevención de diversas formas de abuso, engaño o manipulación en el ámbito digital.

Análisis de la 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. El análisis de memoria del dispositivo representa una etapa crucial en las investigaciones digitales, ya que permite extraer información valiosa sobre las actividades llevadas a cabo en un dispositivo en el momento en que se cometió un delito. La memoria RAM, almacén volátil de datos temporales, puede contener una amplia información relevante, desde procesos en ejecución hasta fragmentos de datos manipulados. Al examinar esta memoria, los expertos pueden identificar patrones de comportamiento, actividades sospechosas o incluso evidencia directa relacionada con el delito en cuestión. Este proceso de análisis puede implicar la recuperación de datos eliminados, la identificación de aplicaciones en uso, la reconstrucción secuencial de conversaciones o actividades en línea, entre otros aspectos.

Se desarrollan modelo para la detección de videos modificados por la técnica de intercambio facial o "Deepfake". Con el objetivo de analizar la sucesión de frame en los videos, es decir determina una imagen concreta dentro de una sesión de imágenes en movimiento**,** y así poder detectar discrepancias en la transmisión del flujo óptico, mediante redes convolucionables (CNN) (Güera et al. 2018). Desde este enfoque hay una importancia en el ámbito de la jurisprudencia. La capacidad de identificar vídeos alterados es fundamental para combatir la difusión de información falsa, el engaño y la difamación, en los que se puede emplear "Deepfakes" para generar material engañoso o perjudicial.

Documentación y presentación de la evidencia.

La correcta documentación y presentación de las evidencias digitales son importantes para la investigación, permite los hallazgos del análisis de trasmitan de manera clara al juzgador, y hacia la otra parte. Esto implica registrar y etiquetar todos los detalles de la investigación, en la que debe especificar fecha y hora en la que se recopilo, técnicas y procedimiento utilizado, herramientas de análisis, esta documentación debe ser precisa con información relevante del hecho, y debe tener fotografías, videos o de ser el caso declaraciones de testigos.

Un ejemplo de documentación y presentación de la evidencia digital sería en el caso de una investigación de un "deepfake" en la que se creó un video sexual utilizando el intercambio de rostros. En este caso, la documentación abarca información sobre la descripción detallada de los imperfectos visuales del video para establecer su falsedad. Asimismo, se incluyen los procedimientos empleados para su análisis y de manera detallada las herramientas utilizadas para recabar pruebas adicionales.

En cuanto a la presentación de la evidencia, esta comprendería un resumen conciso de los hallazgos clave, como la identificación de la dirección IP del equipo del autor de delito

o cualquier correspondencia incriminatoria descubierta. Además se brindará, y la explicación pormenorizada del proceso seguidor para llegar a estas conclusiones. Destocando los métodos de investigación empleados, como gráficos o diagramas, con el fin de facilitar una mejor compresión efectiva de los descubrimientos realizados, además el recurso visual sirve de complemento al informe pericial.

Se llega a la exactitud más alta, con el extractor de rostros más desarrollado en el momento, Face2Face del año 2016 y la red XceptionNet, pre entrenados con ImageNet y mediante reglas de inferencia para determinar si el video fue modificado o no (Rossler 2019). El uso de tecnologías avanzadas como las aplicaciones ya mencionadas, esta evolución está impulsada por la necesidad de combatir eficazmente las amenazas emergentes y hacer frente a los desafíos que plantea la creciente prevalencia de los "Deepfakes" y otros métodos de manipulación de los medios digitales.

XceptionNet: realiza una inmersión profunda en la red neuronal convolucional, se encarga de recopilar datos, es un modelo de red neuronal avanzado de aprendizaje profundo para captar la diferencia e imperfecciones entre el vídeo original y el manipulado. Las redes convolucionales (CNN) son utilizadas comunalmente para el procesamiento de imágenes, estas redes se han ido desarrollando de acuerdo a diferentes fines. Todas estas redes buscan tener mayor precisión en la detección de objetos, y a continuación se menciona algunos ejemplos de las herramientas que puede ayudar a detectar un "deepfake":

Deepware Scanner: utiliza inteligencia artificial para realizar un análisis de vídeos con el fin de identificar posibles deepfakes mediante la detección de irregularidades y patrones de generación, al igual que los hacen otras aplicaciones como Microsoft Video Authenticator, Deepware Scanner, Sensity AI, DeepGuard analizan los movimientos faciales y reconocen anomalías y manipulaciones. Es importante tener en cuenta que estas herramientas pueden tener ciertas limitaciones lo que indica que no garantizan una detección total. Además, el avance de la tecnología en la creación de contenido falso representa un desafío continuo para la detección, por lo que es necesario que las herramientas y procedimientos para detección se actualizan con frecuencia.

3.2.2. Pericia de análisis de video y fotografía

Es de suma importancia reconocer el aumento de los vídeos "deepfake", lo cual resalta la necesidad de contar con herramientas que puedan autenticar la veracidad del contenido, ya que los avances tecnológicos permiten manipular vídeos y audios de forma muy convincente (Anderson, 2018, p. 123). Lo que el autor manifiesta es la facilidad con la que se puede crear contenido manipulado y difundirlo a través de las plataformas de redes sociales o sitios web, crea un desafío cada vez mayor a la hora de establecer su veracidad, así también surge la demanda de expertos en delitos informáticos con conocimientos de la IA, así como un perito experto en comparación de rasgos faciales.

En la detección de rostros existen diversas líneas de investigación, por lo que es importante delimitar ciertas regiones como los ojos, nariz y boca: estimar hacia donde apunta

la mirada, la pose del rostro, si la persona se encuentra sonriendo. Estas líneas se pueden agrupar de la siguiente manera:

Encontrar fallos: es pertinente que algunos "Deepfakes" presentan imperfecciones que los manipuladores no han podido corregir. Estas imperfecciones pueden manifestarse como sutiles disparidades en las expresiones faciales, la posición precisa de la cabeza o la iluminación, así también contornos borrosos, piel artificialmente lisa o movimientos espasmódicos y antinaturales. Si bien las personas suelen esforzarse por diferenciar entre una imagen auténtica y una "Deepfake", se puede entrenar un algoritmo para identificar estas aberraciones.

Parpadeo: otra técnica para detectar potencialmente un "Deepfake" consiste en examinar la frecuencia con la que parpadea la persona que aparece en la imagen. En un "Deepfake", la tasa de parpadeo es inferior a la observada en los vídeos genuinos. Esta discrepancia se debe a que el algoritmo es incapaz de reproducir el parpadeo de manera convincente, al menos no tan rápida como un humano. El parpadeo de los ojos de los "deepfake" pornográficos son diferentes l de una persona de la vida real, debido que el ser humano normalmente parpadea una vez cada s a 10 segundos, por lo que esto no sucede en el video manipulado (Ehrenkranz, 2018, p.175).

El cuello y la cara: Vale la pena señalar que los "Deepfakes" manipulan principalmente los rasgos faciales en lugar de todo el cuerpo, ya que este último sería significativamente más complejo. En consecuencia, es importante examinar minuciosamente el cuerpo de la persona cuyo rostro ha sido sustituido. Si las características del cuerpo no se alinean con las del individuo genuino, sirve como un indicio adicional de falsedad. De hecho, los "Deepfakes" suelen centrarse en los primeros planos del rostro, ya que incluir toma más ancha requeriría editar una mayor cantidad de contenido de vídeo, lo que aumentaría la probabilidad de que se detectaran errores.

Poca duración: La mayoría de los Deepfakes tienen una duración breve, normalmente de unos pocos segundos, debido al considerable esfuerzo que supone el proceso de aprendizaje del algoritmo. Un vídeo excesivamente corto y con contenido inverosímil también puede proporcionar pistas que indiquen su naturaleza de "Deepfake". Por ejemplo un clip demasiado breve refleja sospechas sobre su autenticidad es por ello la necesidad de poner atención a detalles sutiles al evaluar la veracidad de los medio digitales.

El sonido: En muchos "Deepfakes", es habitual observar una falta de sincronización entre los componentes auditivos y visuales, ya que el algoritmo responsable de alterar el archivo de vídeo a menudo no consigue alinear correctamente el sonido con los movimientos de los labios. "Es lógico destacar la importancia de múltiples voces y contribuir a la detección de una sola voz" (Vives, 2019, p.78). Esta falta de sincronización no solo afecta la credibilidad del contenido generado, sino que también puede ser un indicador clave para detectar la manipulación digital.

Velocidad: Además, prestar atención a los detalles más sutiles de la grabación puede resultar informativo. En este sentido, reproducir el vídeo a una velocidad reducida puede

ayudar a identificar alteraciones repentinas en la imagen o cambios bruscos en el fondo del vídeo, los cuales pueden indicar la presencia de un “Deepfake”.

El interior de la boca: Los algoritmos de inteligencia artificial muestran una incapacidad para replicar fielmente las intrincadas características de la lengua, los dientes y la cavidad interna de la cavidad oral durante el habla. Tras un examen meticuloso de estos intrincados aspectos, incluso una pequeña imperfección en la cavidad oral puede ser un indicio inequívoco de la existencia de un “Deepfake”.

3.3 Materialización de prueba pericial

La carga de la prueba es obligación de las partes a probar los supuestos de hecho cuya finalidad tener un consecuencia jurídica y favorecer a de las partes en el proceso, esta debe ser desarrollado con los principio del debido proceso y buena fe, pues para una de las parte es más fácil acreditar un hecho y que pueda probarlo, en el caso del “deepfake” la carga de la prueba corresponde al fiscal de delitos informáticos, conforme a los plazos procesales oportunos. Cundo sea necesaria los conocimientos científicos, técnicos y práctico en el ámbito de la informática se debe realizar el proceso correspondiente para la designación del perito de conformidad a los lineamientos establecidos por ley.

3.3.1. Informe pericial

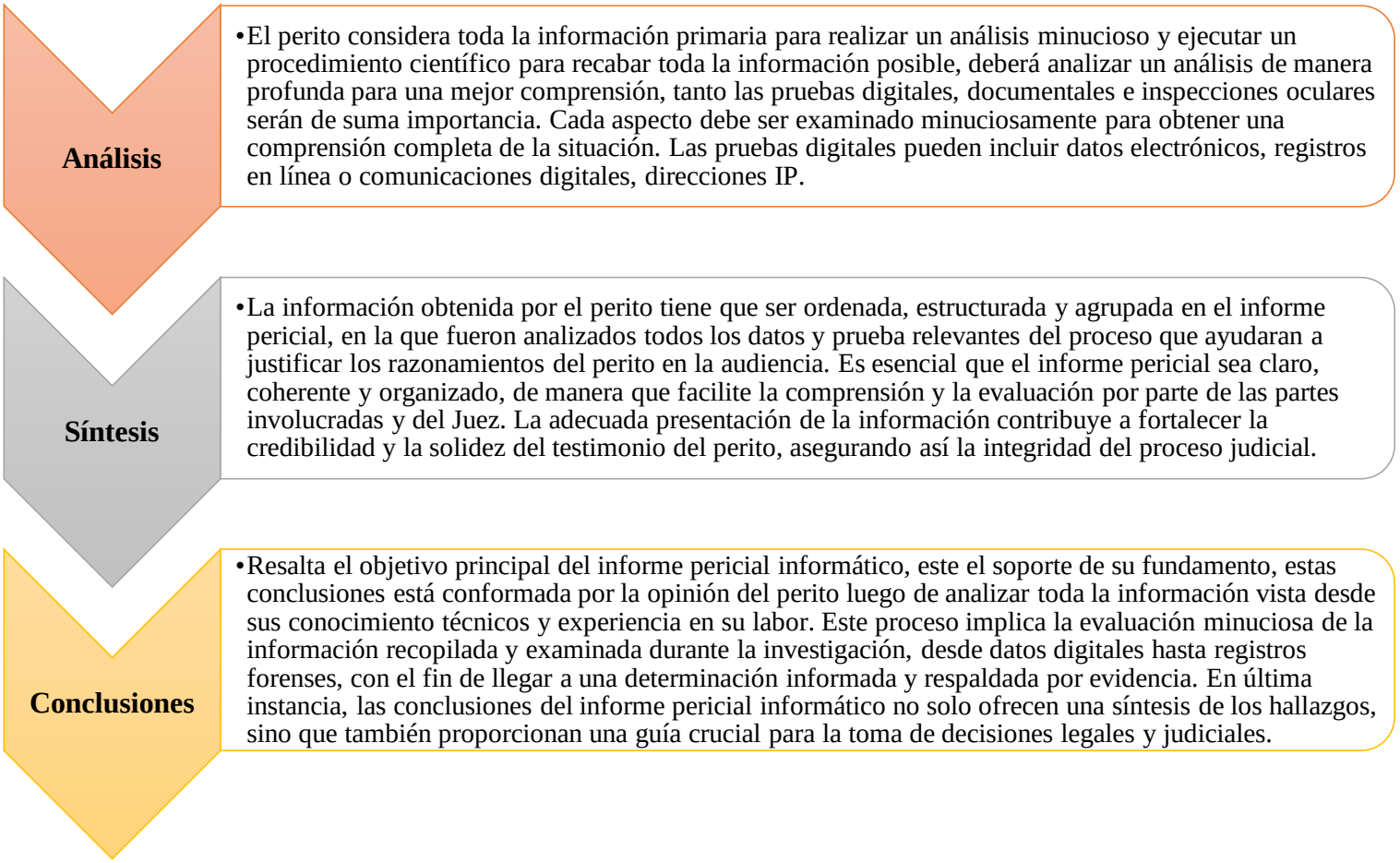
El informe pericial informático que se realiza para encontrar y detectar a los responsables así como los contenidos falsificado del “deepfake” es considerado como un medio de prueba documental, dentro de un proceso judicial, el cual sirve como un vehículo para introducir la prueba digital en el proceso, ha esto se une el testimonio del perito en audiencia donde sustenta su informe, documentos públicos o privados que se considere, pruebas y registros que aporten. El informe es realizado mediante un análisis técnico, que determina hechos complejos. La importancia del informe del perito es de vital importancia debido a que le perito es el auxiliar del juez, le ayuda a tomar una decisión acorde a su sana crítica y lo plasma en sentencia.

El informe pericial informático tiene carácter de prueba en el procesos, este informe analiza cono se ha producido este hecho y determina sus causa y consecuencias desde una perspectiva técnica, este procedimiento puede destacarse hacia uno u otro lado, esto permitirá un debate racional en juicios complejos, ayudando a un juez a tomar una decisión basada en razonamientos lógicos y científicos.

Con la sofisticación de la tecnología resulta una problemática en la identificación al ojo desnudo, como establece Gómez et al. (2021) “Los índices de verosimilitud de los “deepfake” son tan elevados que no solo son indistinguibles las recreaciones de las figuras reales, sino que las imágenes creadas con IA tienden a generar falsificaciones hiperrealistas” (p.67). Es por ello que la estas técnicas son complejas para localizar los videos falsos, para luego introducirnos en el ámbitos judicial. Dedicada en la etapa procesal oportuna para su acervo probatorio.

3.3.2. Fase de la elaboración del perito informática

Gráfico 3 Fase de la elaboración del perito informática



Autor: Franklin Sinaluisa

3.3.3. Características del informe parcial informático

Peritaje experto: Se puede requerir el testimonio de expertos en tecnología informática y peritos que realicen análisis de características faciales, para determinar si un video o inteligencia artificial es auténtico y la confiabilidad del contenido. Estos expertos pueden proporcionar opiniones especializadas sobre la manipulación digital y sus efectos en la integridad de la prueba.

1. Didáctico: utiliza un vocabulario en la que explica con palabras conocidas, a diferencia de las palabras técnicas del especialista. Se destaca por su capacidad para emplear un lenguaje comprensible y familiar, que facilita la comprensión del lector, en contraste con la terminología técnica específica utilizada por los especialistas en un campo particular. Este enfoque busca transmitir información de manera accesible y clara, evitando la jerga técnica que puede resultar confusa para quienes no están familiarizados con el tema.

2. objetiva e independiente: su argumento debe basarse en el conocimiento y la experticia ajustada a la verdad. Esto implica que cualquier afirmación o conclusión presentada debe ser respaldada por evidencia confiable y verificable, sin sesgos ni

influencias externas que puedan distorsionar la interpretación de los hechos. Un enfoque objetivo busca entender los diferentes puntos de vista y considerar todas las perspectivas relevantes antes de llegar a una conclusión. Asimismo, la independencia garantiza que el análisis y la evaluación se realicen sin influencias externas que puedan comprometer la imparcialidad del proceso.

3. Contundente: se relaciona los argumentos y evaluaciones, mismo que debe mantener en el testimonio. Esta característica implica mantener una estructura lógica y sólida en la presentación del testimonio, de modo que cada argumento respalde y refuerce los demás, contribuyendo así a la fuerza general de la posición defendida. La contundencia no solo implica la claridad y cohesión en la expresión de los puntos de vista, sino también la capacidad de sostenerlos con evidencia sólida y razonamiento sólido. Un testimonio contundente no solo presenta argumentos convincentes, sino que también es capaz de mantener su fuerza y coherencia incluso frente a posibles objeciones o críticas.

4. Admisibilidad de la prueba: La evidencia obtenida a través de técnicas de detección de "Deepfakes" debe cumplir con los estándares de admisibilidad de la prueba los cuales son la utilidad, pertinencia y conducencia. Esto implica que los métodos utilizados sean reconocidos como confiables y científicamente válidos por la comunidad jurídica. Asimismo, la conducencia, es decir, la capacidad de la evidencia para demostrar o refutar un hecho relevante en el caso, también es fundamental para su admisibilidad. Por lo tanto, es esencial que los métodos de detección de "Deepfakes" sean rigurosamente evaluados y validados para garantizar su aceptación en los procedimientos legales

5. Verídico: El principio de veracidad es fundamental en el trabajo del perito informático, ya que implica la obligación ética de expresarse con la verdad en todas las evaluaciones y conclusiones que realice. Este compromiso con la veracidad no solo es un requisito ético, sino también un deber profesional que garantiza la integridad y la credibilidad de su labor. En el contexto de la pericia informática, la veracidad se traduce en proporcionar informes precisos y objetivos, basados en evidencias sólidas y metodologías rigurosas. Además, este principio implica la transparencia en la comunicación de hallazgos.

6. Autenticidad y origen: implica investigar la fuente del material, su cadena de custodia y cualquier manipulación o edición que pueda haber ocurrido. Este proceso implica no solo rastrear la fuente del material, sino también examinar detenidamente su cadena de custodia, es decir, el registro de los pasos que ha seguido desde su creación hasta su presente estado. Además, es esencial analizar cualquier indicio de manipulación o edición que pueda haber ocurrido en el material, ya que estas alteraciones podrían afectar significativamente a su autenticidad y precisión.

7. Análisis técnico: Implica una evaluación meticulosa de diversas señales que podrían revelar la presencia de una falsificación. Entre estas señales se encuentran los artefactos digitales, que son anomalías visuales que pueden surgir durante el proceso de manipulación y que pueden ser detectados mediante un escrutinio detallado de la imagen o el vídeo. Además, las inconsistencias en la iluminación o la perspectiva pueden proporcionar

indicios reveladores, ya que una integración deficiente de elementos en el entorno visual puede resultar en discrepancias visuales notorias.

8. Comparación con fuentes originales: Si es posible, se debe comparar el contenido sospechoso con fuentes originales o versiones auténticas para detectar discrepancias. Esto puede implicar el uso de metadatos, análisis de calidad de imagen. Examinar el contenido en sí mismo, sino también hacer uso de diversos métodos de análisis, como la revisión de metadatos y la evaluación de la calidad de la imagen. Al contrastar el material sospechoso con fuentes conocidas y verificadas, es posible identificar discrepancias significativas que podrían indicar la manipulación digital. Este enfoque permite a los investigadores y expertos en medios discernir entre contenido auténtico y falsificado, proporcionando así una herramienta crucial en la lucha contra la desinformación y la manipulación mediática.

La validación de las pruebas relacionadas con los "deepfakes" requiere un enfoque multifacético que combine análisis técnico, peritaje experto y evidencia complementaria para establecer la autenticidad del contenido y su idoneidad como prueba en un proceso legal. Es importante abordar estas cuestiones con precaución y diligencia para garantizar la integridad del proceso judicial y proteger los derechos de las partes involucradas.

Tal y como define "que los cambios son necesarios medios probatorios tradicionales del derecho penal que lesionan bienes jurídicos nuevos en un sentido de los derechos tradicionalmente tutelados con una mayor intensidad" (Lloria, 2013) .La autora interpreta el bien jurídico de intimidad a la luz de los avances que han procurado la transformación de un escenario tradicional a uno absolutamente tecnológico, puede generar lesión más graves en el entorno virtual.

Si bien el sistema judicial ecuatoriano puede estar avanzando en la adopción de medios tecnológicos, normativos y peritos especializados para abordar delitos de "deepfake", es probable que aún existan desafíos en términos de recursos, capacitación y coordinación interinstitucional. Es importante que se continúe fortaleciendo el marco legal, la infraestructura tecnológica y la capacitación del personal judicial para hacer frente eficazmente a estos delitos en el contexto digital en constante evolución.

3.4 Repercusiones en la confianza judicial

Los "deepfakes" representan una grave amenaza para la integridad del sistema judicial al socavar la confianza en las pruebas presentadas. Hay varias formas en las que los "deepfakes" pueden impactar negativamente la confiabilidad de las pruebas judiciales, por ejemplo, la capacidad de generar vídeos y audios falsos convincentes puede llevar a la presentación de evidencia adulterada o manipulada que podría influir en el resultado de un juicio. Además, la proliferación de "deepfakes" podría sembrar dudas sobre la autenticidad de las pruebas presentadas, lo que socavaría la confianza en el sistema judicial en su conjunto. Asimismo, la rápida evolución de esta tecnología plantea el desafío adicional de mantenerse al día con los métodos de detección y autenticación de pruebas digitales, lo que

podría exacerbar aún más el problema de la confiabilidad de las pruebas judiciales en el futuro. Estos problemas son los siguientes:

Manipulación de evidencia: Los "deepfakes" pueden generar contenido audiovisual falso que es extremadamente convincente y difícil de distinguir de la realidad. La posibilidad de crear evidencia aparentemente auténtica pero completamente fabricada presenta un riesgo considerable para la integridad de los procesos legales y la confianza pública en la información presentada. Además, esta tecnología también podría ser explotada para difundir desinformación o realizar ataques dirigidos a individuos, instituciones o comunidades. En consecuencia, la detección y mitigación efectivas de los "deepfakes" se han convertido en un desafío crucial para preservar la veracidad y la fiabilidad en el mundo digital contemporáneo.

Falsificación de testimonios: Los "deepfakes" pueden ser utilizados para crear videos falsos de personas dando testimonio de eventos que nunca ocurrieron. Estos testimonios falsos pueden ser presentados como prueba en un Juicio, lo que puede llevar a decisiones judiciales erróneas y a la condena injusta. La capacidad de crear testimonios falsos con un grado sorprendente de realismo plantea desafíos significativos para la integridad del sistema judicial y para la búsqueda de la verdad.

Desafíos para la autenticidad: La creciente sofisticación de los "deepfakes" dificulta la verificación de la autenticidad de la evidencia presentada. Los jueces tiene dificultades para determinar si un video o audio es genuino o si ha sido manipulado digitalmente, lo que puede generar dudas sobre la credibilidad de la evidencia presentada. Es crucial que el sistema judicial desarrolle estrategias efectivas para abordar este problema y proteger la integridad de las pruebas presentadas en el sistema judicial.

Impacto en la percepción pública: La aparición de "deepfakes" puede repercutir la confianza del público en el sistema judicial ecuatoriano. La difusión de evidencia falsa o manipulada puede socavar la percepción de imparcialidad y justicia del sistema, lo que puede tener consecuencias negativas para la legitimidad de las decisiones judiciales. Este fenómeno plantea una amenaza seria a la legitimidad de las decisiones judiciales, ya que el público podría cuestionar la autenticidad de las pruebas presentadas en los tribunales. Además, la propagación de "deepfakes" podría sembrar la duda sobre la validez de las sentencias y generar un clima de escepticismo generalizado hacia el funcionamiento del sistema legal.

Sin embargo, los "deepfakes" presentan un desafío difícil y novedoso para los jueces y los legisladores. Plantean cuestiones fundamentales sobre la ilicitud moral de actos tecnológicos nuevos e inusuales que pueden dañar a otros. La falta de legislación clara en ciberseguridad es un problema mundial. Según un informe de la Unesco y la Unión Internacional de Telecomunicaciones, es crucial modernizar las leyes, ya que solamente el 72% de los países tienen legislación funcional en ciberdelincuencia. La falta de definiciones normativas claras permite que los criminales operen impunemente a nivel global (UNDOC, 2019).

UNIDAD 4 PROBLEMÁTICA DE APLICACIÓN DEL "DEEPFAKE" EN ECUADOR

La aplicación del "deepfakes" pornográfico en Ecuador presenta diversas problemáticas, entre las cuales destaca el riesgo de impunidad, difamación, chantaje, extorción, ya que la tecnología puede ser utilizada para difundir videos falsos. La dificultad probatoria en la detección de "deepfakes", así como la falta de peritos especializados en esta materia complica la identificación de contenido falso.

4.1 Influencia de medios tecnológicos en la práctica del "deepfakes"

En Ecuador, el acceso a la Internet ha aumentado considerablemente, alcanzando el 60,4% de los hogares en el país (INEC, 2021). De este porcentaje, el 73,3% lo utiliza principalmente para actividades comunicacionales y redes sociales. Esta realidad plantea la posibilidad de enfrentar riesgos y situaciones de violencia digital (ChildFund, 2023). Destaca la creciente intromisión de Internet en los hogares ecuatorianos. Sin embargo, también señala la necesidad de abordar los riesgos y desafíos asociados con esta conectividad, como la violencia digital.

La influencia de los medios tecnológicos en la práctica del "deepfakes" pornográfico en Ecuador se presenta como una expresión particular y preocupante en la manipulación de contenidos digitales, el avance de las herramientas informáticas permite la creación de vídeos pornográficos falsificados con una precisión cada vez mayor. Esta tendencia no solo plantea serias preocupaciones en términos de privacidad y consentimiento, sino que también resalta los desafíos legales y éticos que enfrenta la sociedad ecuatoriana en la era digital. Los aspectos más relevantes son:

Acceso a tecnologías de generación de contenidos falsos: La disponibilidad generalizada de tecnologías avanzadas, como algoritmos de aprendizaje profundo y software de edición de imágenes y videos, facilita la creación de "deepfakes" pornográficos. Esto amplía la posibilidad de que individuos con intenciones maliciosas o inescrupulosas utilicen estas herramientas para crear contenido engañoso. La disponibilidad generalizada de tecnologías avanzadas para la creación de deepfakes pornográficos plantea serios desafíos que deben ser abordados desde una perspectiva jurídica integral. En Ecuador surge la necesidad de actualizar y fortalecer un marco normativo para proteger efectivamente los derechos fundamentales de sus ciudadanos frente amenazas, esto incluye la tipificación de una normativa penal específica, conjuntamente con la cooperación internacional, con el fin de garantizar una protección efectiva contra el uso malicioso de la IA.

Difusión a través de plataformas digitales y redes sociales: La facilidad de compartir contenido en plataformas digitales y redes sociales contribuye a la rápida propagación de "deepfakes" pornográficos, aumentando el impacto y la visibilidad de estos materiales manipulados. Esta situación de violencia ocurre al compartir, reenviar o publicar en entornos digitales con contenido sexual de personas sin su consentimiento. Estas imágenes son obtenidas sin permiso para compartirlas o robadas de dispositivos. Las principales víctimas son mujeres (Ministerio de Educación Argentina, 2021). En el contexto Ecuatoriano, la constitución y la normativa legal deben proteger el derecho a la intimidad,

la dignidad y la integridad de la persona de todos los ciudadanos. Por ende la necesidad de fortalecer el marco normativo para abordar esta problemática. La Constitución del Ecuador en su artículo 66, garantiza el derecho a la intimidad y la integridad personal. La creación y difusión de "deepfakes" pornográficos infringe estos derechos.

Afectación a la Privacidad y Reputación: La creación y difusión de "deepfakes" pornográficos pueden tener consecuencias devastadoras para la privacidad y la reputación de las personas afectadas, ya que estas imágenes manipuladas pueden ser utilizadas para difamar, acosar o extorsionar. Estos contenidos alterados pueden circular rápidamente en línea, propagando información engañosa que puede dañar irreparablemente la imagen y la integridad de quienes son objeto de estos ataques. La posibilidad de que las personas sean identificadas erróneamente en situaciones comprometedoras y falsas puede socavar la confianza pública y generar un clima de temor en el ciberespacio. Es crucial abordar estos riesgos con medidas efectivas de protección de la privacidad y de regulación de la difusión de contenido digital manipulado, para salvaguardar la dignidad y el bienestar de las personas en la era digital.

Desafíos para la Identificación y Eliminación: La naturaleza realista de los "deepfakes" pornográficos dificulta su detección y eliminación. Esto plantea desafíos adicionales para las plataformas en línea y las autoridades encargadas de abordar la difusión de contenido no consensuado. Esta dificultad se magnifica por la sofisticación constante de las técnicas de generación de "deepfakes" y su capacidad para imitar fielmente características faciales y corporales de las personas. Además, la rápida propagación de este tipo de contenido en plataformas en línea plantea un reto adicional, pues su eliminación oportuna y efectiva es crucial para evitar daños graves a la reputación y bienestar de las personas involucradas. En este sentido, las plataformas en línea y las autoridades pertinentes se enfrentan a una tarea monumental en la lucha contra la difusión de este contenido no consensuado, que requiere la implementación de estrategias innovadoras y colaborativas para proteger a los usuarios y preservar la integridad de sus plataformas.

Necesidad de Medidas Legales y Educación Digital: La proliferación de "deepfakes" pornográficos destaca la importancia de establecer medidas legales específicas para abordar este tipo de contenido. Además, la educación digital y la conciencia pública son esenciales para prevenir la propagación y minimizar el impacto de estos ataques. Fomentar la conciencia pública sobre los riesgos asociados con estos ataques digitales puede ayudar a prevenir su propagación y mitigar su impacto en la sociedad. En última instancia, abordar el fenómeno de los "deepfakes" requiere un enfoque integral que combine medidas legales sólidas con programas educativos y campañas de sensibilización para proteger la integridad de la información y la privacidad de las personas.

4.2 Análisis de la tipicidad de los Art. 178

Artículo 178. Violación del derecho a la intimidad manifiesta lo siguiente: La persona que, sin contar con el consentimiento o la autorización legal, acceda, retenga, grabe, reproduzca, intercepte, examine, difunda o publique datos personales, mensajes de voz, audio y vídeo, objetos postales, información contenida en soportes informáticos,

comunicaciones privadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años ([COIP], 2014, art. 178).

Análisis

Alcance de la norma: El artículo abarca una amplia gama de acciones que pueden comprometer la privacidad de una persona. Estas acciones van más allá del mero acceso no autorizado a información confidencial e incluyen aspectos como la divulgación o la publicación indebida de una variedad de datos personales y comunicaciones privadas. Desde la intrusión en sistemas informáticos hasta la difusión maliciosa de información sensible, el artículo examina exhaustivamente las diversas formas en que la privacidad puede ser violada en el contexto actual de la era digital.

Consentimiento o autorización legal: Es fundamental destacar la importancia de obtener el consentimiento explícito de las personas involucradas antes de crear o distribuir cualquier contenido generado mediante esta tecnología. De igual manera, la existencia de una base legal sólida es esencial para respaldar estas acciones y garantizar su legitimidad. La ausencia de consentimiento o de un respaldo legal adecuado para llevar a cabo tales acciones constituye un factor determinante que puede considerarse como indicativo de su carácter ilegal.

Medios de comisión: El artículo no limita las formas en que se pueden cometer estas violaciones a la intimidad. Incluye acciones tanto analógicas como digitales, abarcando desde la interceptación de comunicaciones hasta la reproducción de datos almacenados en soportes informáticos. Esto refleja la complejidad y la versatilidad de las amenazas a la privacidad en la era digital, donde los infractores pueden emplear una variedad de herramientas y técnicas para acceder, utilizar o comprometer información personal.

Tipos de información protegida: Entre los elementos explícitamente mencionados se incluyen datos personales, que abarcan información sensible sobre individuos, así como mensajes de datos, que pueden comprender cualquier forma de comunicación escrita o electrónica. Además, se extiende la protección a la voz, el audio y el vídeo, lo que implica una salvaguarda de la integridad y privacidad de las grabaciones de sonido y video. También se incluyen objetos postales, lo que refleja la importancia de proteger los envíos físicos y su contenido de cualquier forma de intrusión o manipulación no autorizada. Además, la normativa abarca información almacenada en soportes informáticos, reconociendo la importancia de salvaguardar la confidencialidad y seguridad de los datos digitales.

Sanciones: El artículo establece la pena privativa de libertad como consecuencia para aquellos que violen la intimidad de otra persona. La duración de la pena se establece en un rango de uno a tres años, lo que sugiere la gravedad que se asigna a este tipo de infracciones.

El Artículo 178 del [COIP] busca proteger la privacidad de las personas al establecer sanciones para aquellos que accedan, intercepten, reproduzcan o divulguen información sin el consentimiento adecuado o la autorización legal. Está diseñado para abordar tanto las violaciones analógicas, pero no se encuentra establecidas específicamente acerca de

imágenes y videos con contenido sexual, que son realizados con ayuda de la inteligencia artificial.

Tabla 2. *Elementos objetivo del tipo penal del Art 178*

Elementos	Descripción
Sujeto activo	Cualquier persona (sujeto calificado)
Sujeto pasivo	Cualquier persona (sujeto calificado)
Tipo	Dolo
Verbo rector	Acceder, interpretar, examinar, retener, grabar, reproducir, difundir o publicar
Objeto jurídico	La intimidad
Elementos normativos	Comunicación privada o reservada
Elementos valorativo	No existe
Otras circunstancias	Dentro de la tipicidad se establece que se excluye de sanción cuando la información que se divulga que pública y cuando la persona que divulgue intervenga en el audio o el video.

Fuente: Código Orgánico Integral Penal
Autor: Franklin Geovanny Sainaluisa Sagñay

4.3 Legislación Vigente y Desafíos Jurídicos

Legislación vigente

El artículo 178 tipifica el delito de violación a la intimidad: La persona que, sin contar con consentimiento o autorización legal acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, 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 ([COIP], 2014, art. 178).

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, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Además, en su artículo 8.- Consentimiento, señala que: Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá

mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas (Ecuador A. N., Ley Orgánica de Protección de Datos Personales, 2021).

El acto de "Deepfake" no se encuentra tipificado de manera específica en nuestro Código Penal, la ausencia de esta podría tener repercusiones en el marco legal, particularmente en los casos relacionados con este comportamiento ilícito, la ausencia de este repercute en el principio de legalidad, en la cual la acción u omisión debe estar prescita con antelación al hecho cometido. En consecuencia, a pesar de la posibilidad de que las autoridades traten los casos de "deepfake", sin embargo, por sus fines, se podría sancionar como un delito contra el derecho a la imagen, injuria, delito de odio.

Sobre este tema Castillo (2022) señala que: La falta de tipificación de los "Deepfake" conlleva un vacío legal dentro del ordenamiento jurídico que ataca directamente a las personas que han sufrido este tipo de violación a su intimidad. No existe normativa que abarque esta figura, debido que es completamente nueva (…) (p. 12).

En igual sentido, Leonardo Amores (2022) al referirse sobre esta conducta delictiva describe lo siguiente: Es por ello que al no encontrarse tipificado este delito de forma oportuna dentro de nuestro [COIP] y al encontrarnos dentro de en un estado de derechos constitucionales y justicia no se garantizan los derechos, especialmente a los más débiles y menos protegidos (p.3). Cabe señalar que el Ecuador tiene una obligación internacional con respecto a los documentos internacionales ratificados. Por ello, en este caso se deben adoptar una serie de medidas legislativas, judiciales y administrativas enfocadas a la protección de las mujeres y los ciudadanos en general.

4.4 Análisis de caso de "deepfake" en el Ecuador

La Fiscalía General del Estado, inició una investigación de un presunto delito de pornografía en un colegio privado de Quito. Esta investigación fue impulsada por las acciones denunciadas a dos estudiantes que supuestamente utilizaron inteligencia artificial para crear montajes de contenido sexual. Estas personas, ambas de primero de bachillerato, asistían a una institución educativa ubicada en el valle de Los Chillos. Al parecer, fotografiaron a alumnas de varios niveles educativos (del primero al tercer año de) y, posteriormente, utilizaron estas imágenes para producir vídeos y fotografías con contenido sexual explícito.

Las víctimas se enteraron de este material cuando empezó a circular en Unidad Educativa. Se estima que aproximadamente de 20 a 24 estudiantes mujeres fueron afectadas por este acto de violencia digital. Aunque el número exacto de vídeos y fotos generados sigue sin confirmarse, pero se cree que ronda los 700.

Los autores de esta agresión se retiraron voluntariamente de la Unidad Educativa, según lo afirmó Sybel Martínez, de la Fundación Grupo Rescate Escolar, durante una entrevista con canal televisivo Ecuavisa. Esta organización, en colaboración con padres preocupados y de las víctimas, presentaron una queja formal, pero existió una demora en la respuesta de la Unidad Educativa. Martínez explicó: Según los padres, el director de la escuela mencionó el que estaban preparando un informe para presentarlo al distrito. En vista de esto, la queja menciona que dicho informe debería haberse presentado de inmediato.

En respuesta al incidente, la escuela envió un correo electrónico a Ecuavisa en el que expresaba su convicción de que la resolución de los asuntos legales y la salvaguardia del bienestar de los menores deberían tener prioridad sobre las discusiones públicas sobre el tema. La Fiscalía anunció su investigación sobre el presunto delito de pornografía infantil y adolescente, centrándose específicamente en la difusión de imágenes y videos modificados de estudiantes que emplean tecnología de inteligencia artificial.

Además, el Ministerio de Educación destacó que desde el 28 de septiembre está en vigor un "Protocolo para abordar los casos de violencia digital dentro del Sistema Educativo Nacional" (Ministerio de Educación, 2023). En consecuencia, cualquier caso de violencia digital debe cumplir con las pautas descritas en este documento obligatorio, aplicable a todos los niveles educativos.

El caso mencionado, destaca el mal uso de la inteligencia artificial para crear contenido pornográfico a partir de imágenes de estudiantes en una institución educativa de Ecuador, se plasman diversos problemas legales, así como consideraciones jurídicas que deben ser evaluados bajo el marco legal ecuatoriano. Según el Código Orgánico Integral Penal del Ecuador, en su artículo 103 y 104 tipifica la pornografía infantil como un delito, en cual define y penaliza a la producción, distribución, difusión, venta, acceso a material pornográfico que involucre a menores de edad(Asamblea Nacional, 2014). En el caso descrito, el estudiante que utilizo las imágenes de sus compañeras y las modificó con la ayuda de la inteligencia artificial para crear contenido pornográfico podría estar incurriendo en este delito, debido a la producción y difusión de este material dentro y posiblemente fuera del colegio, lo cual agravarías la situación.

La constitución de la República del Ecuador conjuntamente con el Código Orgánico Integral Penal, protegen el derecho al a intimidad y la imagen personal, la manipulación de fotografías sin consentimiento, y su posterior manipulación y difusión, esto conlleva a la clara violación al derecho fundamental ya mencionado. Las víctimas tienen derecho a la protección de su imagen y privacidad, y la divulgación de materiales que atente contra sus derechos personales.

Las víctimas y sus familiares tienen el derecho a una reparación integral que contemple medidas de restitución, indemnización, rehabilitación y satisfacción acorde a lo dispuesto por la Ley de Protección Integral de Niños y Adolescentes. Además de las acciones penales se puede proceder con las acciones civiles, que consisten en reclamar los daños y perjuicios derivados de la vulneración de derechos, y la afectación psicológica y emocional causada por estos actos. La actuación diligente y coordinada de la Fiscalía, el Ministerio de

Educación y la Unidad Educativa es esencial para asegurar que se haga justicia, se protejan los derechos de las víctimas y se prevengan futuros casos de violencia digital, además es fundamental que se apliquen las sanciones correspondientes para que garanticen una reparación integral.

HIPÓTESIS

La pornografía falsa "Deepfakes" inexistencia de normativa y sus dificultades probatorias, violentan el derecho de intimidad en el Ecuador.

CAPÍTULO lll

3. METODOLOGÍA

3.1 Unidad de análisis

Ésta investigación se centra en el Estado ecuatoriano, con el fin de determinar la inexistencia de normativa y su dificultad probatoria, aplicable a casos futuros de los "deepfake", su impacto en la sociedad, analizando una perspectiva de reforma al Código Orgánico Integral.

3.2 Métodos

- **Método inductivo:** "En las ciencias jurídicas, donde la investigación cualitativa presencia la inducción, como una forma de razonamiento posibilita a construir teoremas desde situaciones concretas y particulares, estableciendo regularidades, generalizando y pautando conclusiones" (Villabella, 2020). El método inductivo recorre el camino de desde lo particular a lo general, en donde se parte de las situaciones específicas induciendo regularidades aplicables a casos semejantes, siendo la manera de establecer conclusiones de estudio de casos y la forma de razonar en una investigación cualitativa.

- **Método jurídico-analítico**: "es aquel método que descompone, un objeto o problema en una de sus partes o elementos para poder estudiar cada una de ellas, desmiembra un todo y l descomponen elementos para observar las causas, la naturaleza y los efectos" (Maldonado et al, 2019). Este método jurídico analítico, pretende el estudio mediante un análisis los instrumentos técnicos necesarios para conocer, elaborar, aplicar y enseñar el objeto del conocimiento del derecho, analiza el lenguaje del discurso jurídico, realiza la descripción del Derecho positivo, un análisis lingüístico cuyo objetivo de estudio son las proposiciones normativas.

- **Método dogmático:** "tiene por objeto de estudio el derecho positivo, describe, a través de la interpretación y sistematización las normas, para construir conceptualizaciones que agrupan normas" (Atianza, 2017). Es decir tiene por objeto, el orden sistemático de los conceptos jurídicos, agregando, por tanto el método dogmático o se especializa en distintas áreas del conocimiento científico, por tanto hablar de dogmática jurídica penal, procesal, administrativo, Bancaria, etc.

- **Método jurídico descriptivo:** permite "(…) descomponer un problema jurídico en sus diversos aspectos, estableciendo relaciones y niveles que ofrecen una imagen de funcionamiento de una norma o institución jurídica" (Antar, 2016). Además, posibilita a la investigadora decidir el camino que debe seguir para entender las características y cualidades del objeto de estudio de manera lógica, ayudando a describir las particularidades del problema de investigación, con base a la observación, recopilación de la información, análisis y comparación de la información de datos y conclusiones.

3.3 Enfoque de la investigación

Debido a las características de la presente investigación re realizó con un enfoque mixto.

3.4 Tipo de Investigación

- **Investigación dogmática,** "Es el estudio de la estructura del derecho objetivo, es decir la norma jurídica, así como el ordenamiento jurídico, ya que se basa en la fuentes formales del derecho objetivo, se investiga, lo que los humanos dicen que hacen con el derecho " (Tantaleán Odar, 2016). Se encarga de estudiar la estructura del Derecho positivo (jurisprudencia, normas jurídicas, doctrinas, etc.), y tener una primera aproximación hacia el estudio del ordenamiento jurídico es o no válido, sin adentrase en detalles sobre su legitimidad y eficiencia.

- **Investigación jurídica descriptiva,** "Consiste en aplicar de manera pura, el método analítico a un tema jurídica, se trata de descomponerlo en tantas partes como sea posible. Lo cual implica que el tema salvo que persiga un fin determinado" (RIVERA, 2007). Busca especificar la propiedades de personas o cualquier otro fenómeno a analizar, midiendo diversos aspectos de la investigación, además de medir conceptos o variables del tema, se centra en dar las características del fenómeno en evaluación, también a través del análisis de puede descomponer un problema jurídico en sus componentes, demostrando su funcionamiento de una institución jurídica.

- **Investigación documental,** "El método documental bibliográfico, consiste en la captación para la investigación, con el fin de que a través de un análisis críticos se pueda construir procesos coherentes para comprender el fenómeno y de abstracción discursiva del mismo, para apreciar nuevas circunstancias" (Botero , 2006).Entonces la investigación documental es cuando se realiza un contacto directo con los documentos y en el lugar que estos se encuentran, en consecuencia nos sirve como principal fuente de información, como libros y documentos ya que son medios, muy importantes para la transmisión de conocimientos, sobre el problema jurídico planteado.

- **Investigación comparación jurídica,** al derecho comparado o también llamado comparación jurídica es el método de investigación teórica propia. Permite describir mediante la comparación de leyes, derechos reconocidos por otros países, en tanto compara los fenómenos jurídicos constituye el medio para poner en orden las imágenes, destacar su cualidad y clasificarlas, ya que las primera etapa de la investigación es la observación y la segunda es la comparación (Villabela, 2012). En definitiva el derecho comparado permite cotejar dos ordenamientos jurídicos pertenecientes a un mismo dominio, estos son; conceptos, instituciones, normas, procedimientos, etc., lo cual permite destacar sus semejanzas y diferencias.

3.5 Diseño de la Investigación

El diseño de la presente investigación, se debe tener en cuenta, que acorde a la materia, objetivos, métodos y tipos de investigan, se realizó a través de un enfoque no experimental cualitativo, en que se obtiene resultados favorables, por la naturaleza de investigación Jurídica, ya que es el diseño netamente esencial para la carrera de Derecho, en la que únicamente se describe las variables de estudio, tanto un contexto, sin manipular las misma de manera deliberada.

3.6 Población

La población en este trabajo es:

Fiscales 5

Jueces de la Unidad Judicial Penal 3

Defensores Privados especializados en víctimas 7

3.7 Muestra

A criterio del investigador, se utilizó un muestreo no probabilístico de conveniencia, en vista de que se encuesta a personas conocedores de la materia con un total de 10 involucrados, de ahí que no sea necesario aplicar fórmulas que permitan obtener muestra.

3.8 Técnicas e instrumentos de investigación

Las técnicas que se realizó en la presente investigación es la guía de encuesta, por lo cual se obtuvo datos relevantes de las variables establecidas, por consíguete se hizo necesario la elaboración de un cuestionario con preguntas centradas en la investigación, adecuado al instrumento de investigación, que fue el mecanismo utilizado por el investigador para recabar los datos e información del problema jurídico que se investigó.

3.9 Pregunta científica orientadora

¿El “Deepfake” como conducta informática no tipificada, incide en la vulneración del derecho a la intimidad en Ecuador?

3.10 Procesamientos de Datos

Dentro de la presente investigación se utilizó las siguientes técnicas:

Elaboración del instrumento de investigación

Aplicación del instrumento de investigación

Tabulación de datos

Procesamiento de los datos e información

Interpretación o análisis de resultados

CAPÍTULO lV.

4. RESULTADOS Y DISCUSIÓN

4.1. Resultados

ENCUESTA DIRIGIDA A: Fiscales Especializados de Violencia de Género de la ciudad de Riobamba, Jueces de la Unidad Judicial Penal y Defensores Privados especializados en víctimas.

PREGUNTA NO. 1. ¿Está familiarizado con el concepto de "Deepfakes" y su uso en contextos legales?

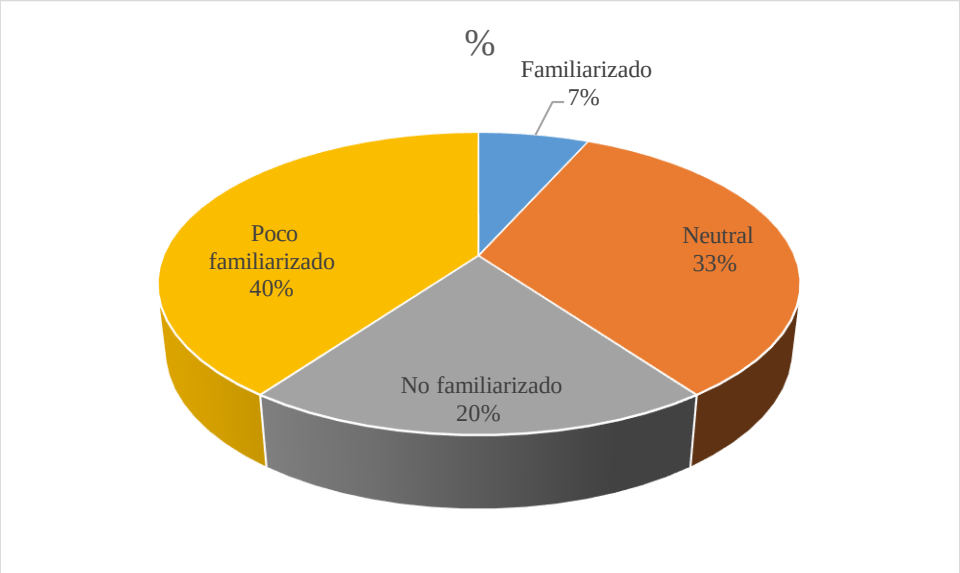
Tabla 3.*Está familiarizado con el concepto de "Deepfakes" y su uso en contextos legales*

Opciones	F	%
Familiarizado	1	6,67%
Neutral	5	33,33%
No familiarizado	3	20,00%
Poco familiarizado	6	40,00%
TOTAL	15	100%

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 Sinaluisa

Gráfico 4.*Está familiarizado con el concepto de "Deepfakes" y su uso en contextos legales*



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 Sinaluisa

Interpretación de los resultados: La tabla muestra la distribución de respuestas sobre la familiaridad con el concepto de "Deepfake" entre los encuestados. 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. Estos resultados sugieren una tendencia hacia una falta de conocimiento o comprensión limitada sobre el fenómeno de "Deepfake" entre la muestra encuestada.

PREGUNTA NO. 2. ¿Considera que el uso de "Deepfakes" está en aumento en los casos que involucran vulneración del derecho de intimidad?

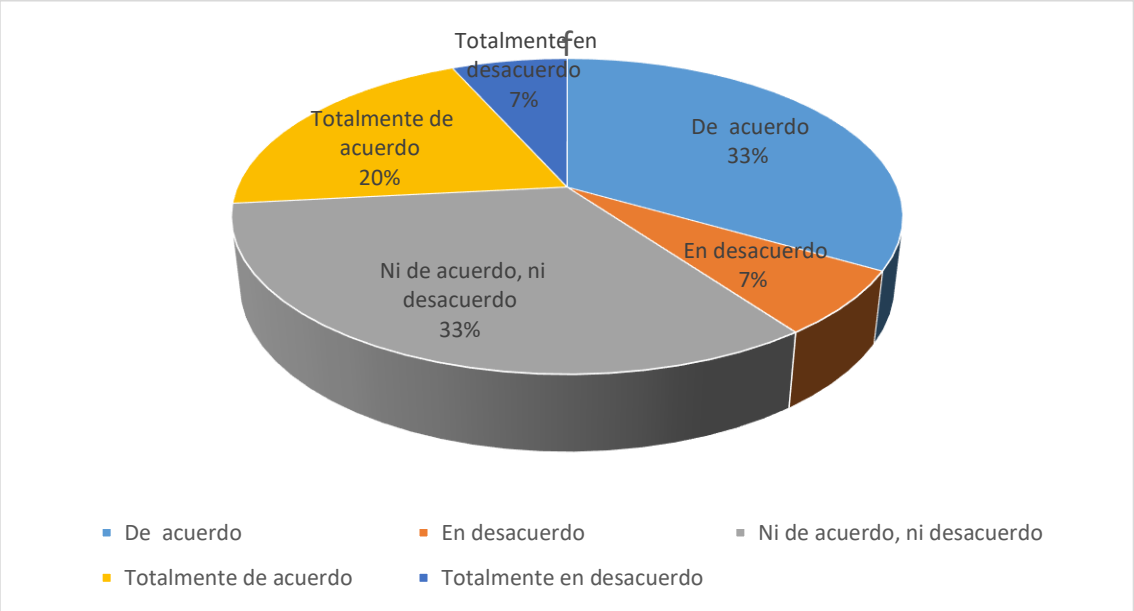
Tabla 4.*Considera que el uso de "Deepfakes" está en aumento en los casos que involucran vulneración del derecho de intimidad*

Opciones	f	%
De acuerdo	5	0,33333333
En desacuerdo	1	0,06666667
Ni de acuerdo, ni desacuerdo	5	0,33333333
Totalmente de acuerdo	3	0,2
Totalmente en desacuerdo	1	0,06666667
TOTAL	15	100%

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 Sinaluisa

Gráfico 5.*Considera que el uso de "Deepfakes" está en aumento en los casos que involucran vulneración del derecho de intimidad*



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 Sinaluisa

Interpretación de resultados: La tabla proporciona datos 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, con una parte significativa que no percibe un aumento sustancial. Sin embargo, es importante tener en cuenta que una minoría considerable sí reconoce este incremento, lo que podría reflejar una mayor conciencia sobre el fenómeno y sus implicaciones legales en la sociedad.

PREGUNTA NO.3. ¿Usted cree urgente la necesidad de incorporar regulaciones legales que aborden la problemática de los "deepfake" en el Ecuador?

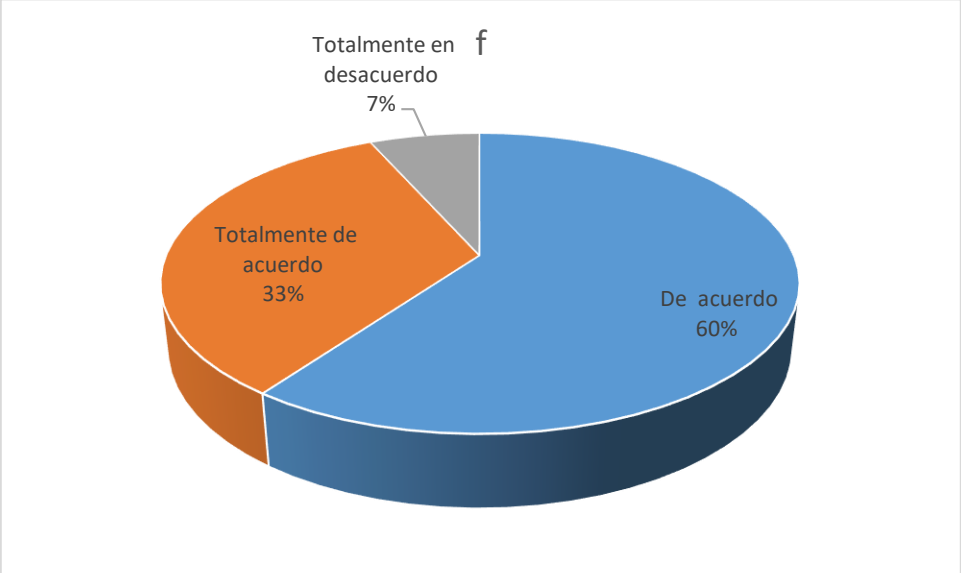
Tabla 5.*Usted cree urgente la necesidad de incorporar regulaciones legales que aborden la problemática de los Deepfakes en el Ecuador*

Opciones	f	%
De acuerdo	9	60,00%
Totalmente de acuerdo	5	33,33%
Totalmente en desacuerdo	1	6,67%
TOATAL	15	100%

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 Sinaluisa

Gráfico 6.*Usted cree urgente la necesidad de incorporar regulaciones legales que aborden la problemática de los "Deepfakes" en el Ecuador*



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.

Interpretación de resultados: La tabla muestra una clara tendencia hacia 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. Este alto porcentaje de acuerdo sugiere un consenso generalizado dentro de la comunidad jurídica sobre la importancia de establecer marcos normativos para abordar cuestiones específicas o emergentes, como podría ser el caso de las regulaciones relacionadas con el ámbito de los "deepfakes". Esta tendencia refleja una comprensión compartida de la necesidad de adaptar el marco legal a los cambios tecnológicos y sociales para garantizar la protección de los derechos y la seguridad de las personas.

Basándome en la tabla proporcionada, parece que 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 repetición de términos como "tipificar", "reforma al COIP" y "ley" sugiere un movimiento hacia la creación de legislación específica para abordar los "deepfake". Esto indica una creciente conciencia sobre la amenaza que representan los "deepfake" y la necesidad de medidas legales para prevenir su abuso y proteger la integridad del sistema judicial. En resumen, la tendencia en relación con el concepto de "deepfake" en esta tabla es hacia la implementación de reformas legales que tipifiquen y sancionen esta práctica.

PREGUNTA NO.4. ¿Considera que la tecnología actual proporciona herramientas suficientes para detectar y autenticar "deepfake"?

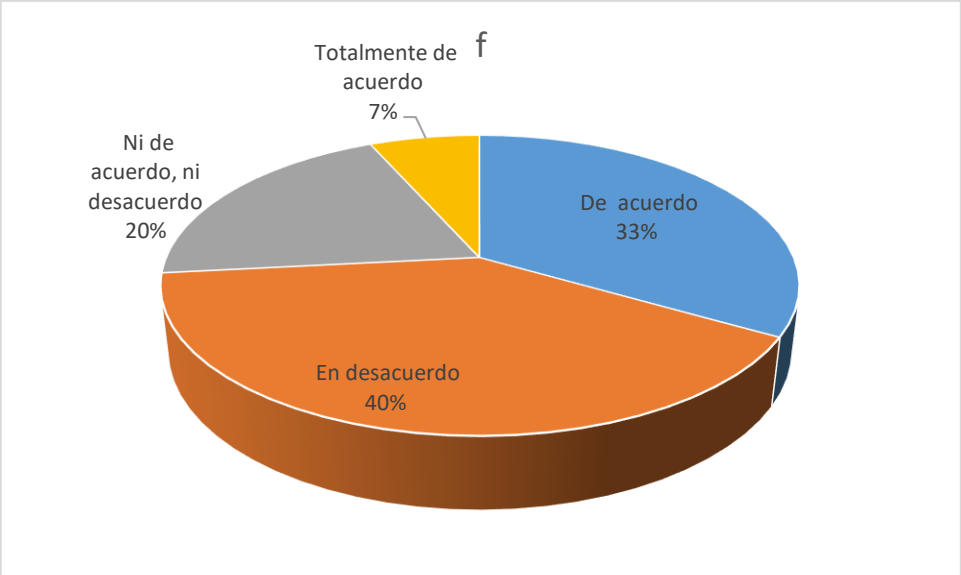
Tabla 6.*Considera que la tecnología actual proporciona herramientas suficientes para detectar y autenticar "Deepfake"*

OPCIONES	f	%
De acuerdo	5	33,33%
En desacuerdo	6	40,00%
Ni de acuerdo, ni desacuerdo	3	20,00%
Totalmente de acuerdo	1	6,67%
TOTAL	15	100%

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 Sinaluisa

Gráfico 7.*Considera que la tecnología actual proporciona herramientas suficientes para detectar y autenticar "Deepfakes"*



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 Sinaluisa

Interpretación de resultados: La tabla proporciona datos relevantes sobre 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 para identificar y abordar el fenómeno de los "deepfake". Esta percepción positiva puede reflejar la necesidad de adoptar medidas proactivas para proteger la integridad de la información y la veracidad de las pruebas presentadas en los procedimientos legales, lo que indica una posible tendencia hacia una mayor adopción y desarrollo de tecnologías de detección de "deepfakes" en el ámbito legal.

Basándome en la tabla proporcionada, parece que hay una tendencia hacia la presencia y utilización de herramientas tecnológicas relacionadas con el concepto de "deepfakes". Específicamente, se mencionan aplicaciones de edición de audio y video, así como aplicaciones de edición Photoshop. Estas herramientas son ampliamente conocidas por su capacidad para manipular imágenes y medios digitales, lo que sugiere un entorno propicio para la creación y propagación de "deepfakes". La presencia de peritos informáticos podría indicar una creciente conciencia sobre la importancia de contar con expertos en tecnología para abordar cuestiones relacionadas con los "deepfakes". En resumen, la tendencia en relación con el concepto de "deepfakes" en esta tabla es hacia la presencia y utilización de herramientas tecnológicas que pueden ser utilizadas para crear o detectar "deepfakes".

PREGUNTA NO.5. ¿Considera que el sistema judicial mantiene desafíos importantes en la autenticidad de un contenido de "Deepfake"?

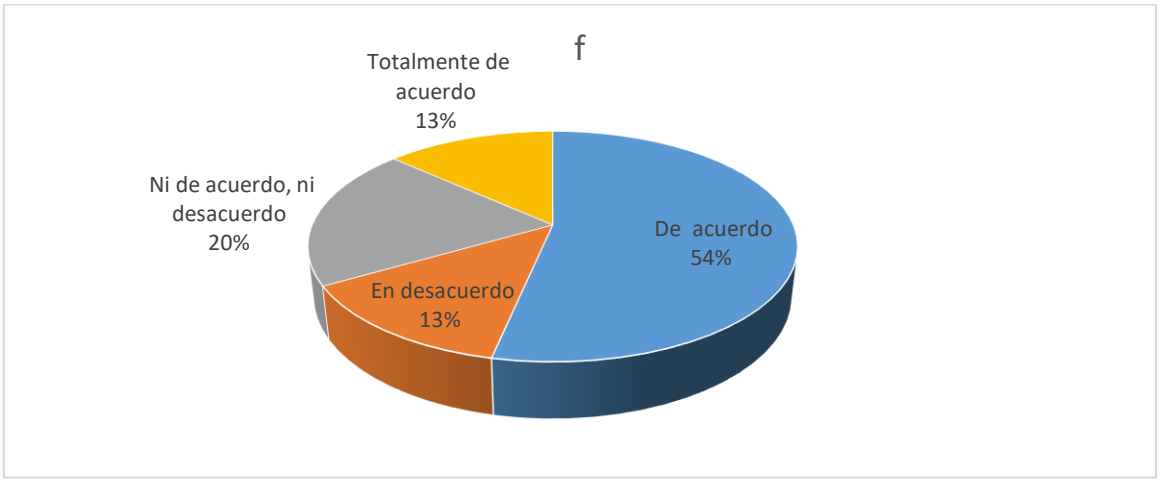
Tabla 7.*Considera que el sistema judicial mantiene desafíos importantes en la autenticidad de un contenido de "Deepfake"*

OPCIONES	f	%
De acuerdo	8	53,33%
En desacuerdo	2	13,33%
Ni de acuerdo, ni desacuerdo	3	20,00%
Totalmente de acuerdo	2	13,33%
TOTAL	15	100%

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 Sinaluisa

Gráfico 8.*Considera que el sistema judicial mantiene desafíos importantes en la autenticidad de un contenido de "Deepfake"*



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 Sinaluisa

Interpretación de resultados: La tabla refleja una división en la percepción de los encuestados sobre el desafío que representa la autenticidad del contenido de los "deepfakes" en el ámbito del derecho. Aunque una parte significativa, 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 sobre la magnitud del problema y la urgencia de abordarlo. Sin embargo, la mayoría de los encuestados reconoce al menos en cierta medida el desafío que representa la autenticidad del contenido de los "deepfakes", lo que puede indicar una conciencia creciente sobre la importancia de desarrollar estrategias y herramientas para verificar la veracidad de la información en el contexto legal.

En relación a la pregunta sobre los desafío y limitaciones en relación con la autenticidad del contenido de los "deepfakes" y la falta de herramientas tecnológicas especializadas para abordar este problema en el ámbito legal. Se señala la ausencia de peritos expertos en temas informáticos y la falta de peritos especializados como dificultades para enfrentar el problema de los "deepfakes". Además, se menciona la dificultad probatoria y el desafío de incorporar la normativa como otros obstáculos significativos. Estos datos sugieren una tendencia hacia la necesidad de desarrollar y adoptar herramientas tecnológicas más avanzadas y especializadas para abordar la autenticidad del contenido de los "deepfakes" en el contexto legal. Además, destacan la importancia de la formación y la investigación en este campo para mejorar la capacidad de respuesta ante los desafíos planteados por los "deepfakes" y su impacto en el sistema judicial.

PREGUNTA NO.6. ¿En su opinión, cree que los "Deepfakes" representan una amenaza significativa para el derecho de intimidad de las personas?

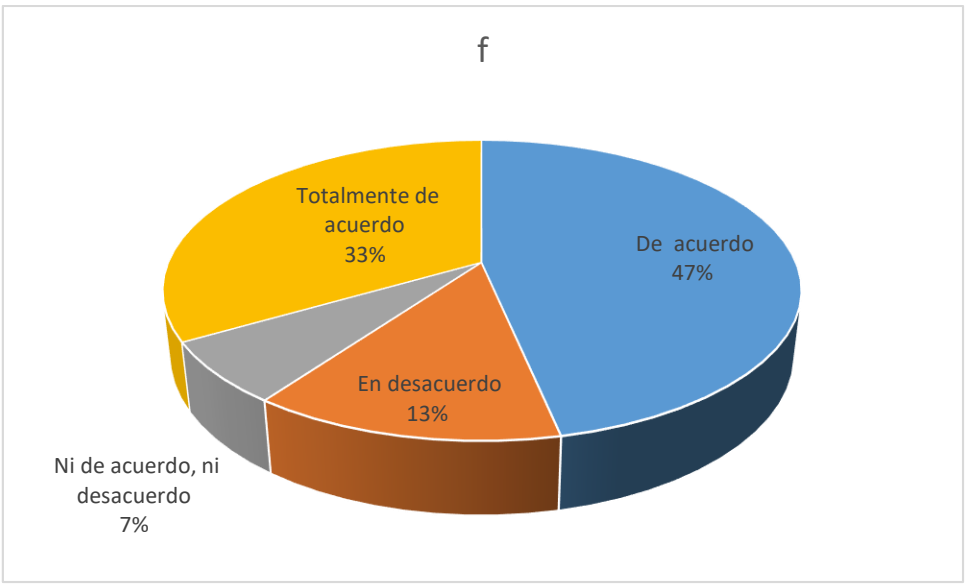
Tabla 8.*En su opinión, cree que los "Deepfakes" representan una amenaza significativa para el derecho de intimidad de las personas*

OPCIONES	f	%
De acuerdo	7	46,67%
En desacuerdo	2	13,33%
Ni de acuerdo, ni desacuerdo	1	6,67%
Totalmente de acuerdo	5	33,33%
TOTAL	15	100%

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 Sinaluisa

Gráfico 9.*En su opinión, cree que los "Deepfakes" representan una amenaza significativa para el derecho de intimidad de las personas*



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 Sinaluisa

Interpretación de resultados: La tabla presenta datos relevantes sobre la percepción de los encuestados acerca de si 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" representan para el derecho a la intimidad. Este hallazgo refleja una creciente conciencia sobre los riesgos que la manipulación digital de contenido puede suponer para la privacidad y la reputación de las personas, lo que puede llevar a un impulso en la implementación de medidas legales y tecnológicas para abordar esta preocupación y proteger el derecho a la intimidad en el contexto digital.

PREGUNTA NO.7. Usted cree que las víctimas han sufrido consecuencias emocionales o psicológicas debido a la difusión de "Deepfakes"

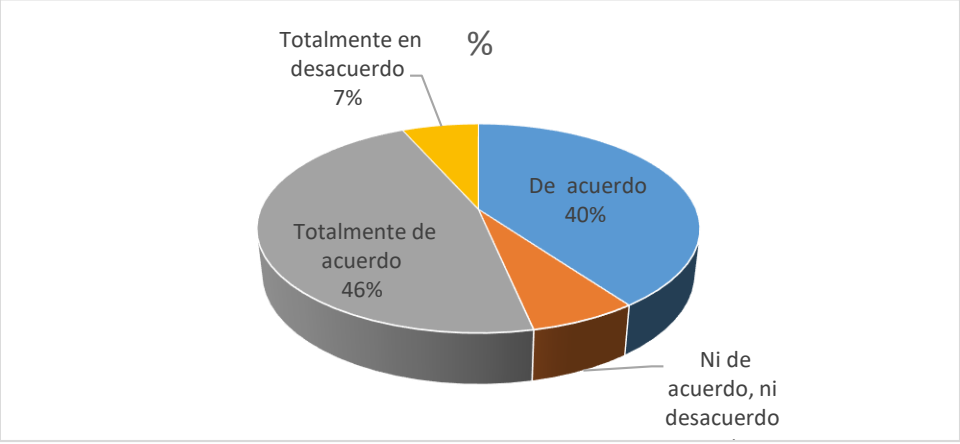
Tabla 9.*Usted cree que las víctimas han sufrido consecuencias emocionales o psicológicas debido a la difusión de "Deepfakes"*

OPCIONES	%	Cuenta de porcentaje
De acuerdo	6	40,00%
Ni de acuerdo, ni desacuerdo	1	6,67%
Totalmente de acuerdo	7	46,67%
Totalmente en desacuerdo	1	6,67%
TOTAL	15	100%

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 Sinaluisa

Gráfico 10.*Usted cree que las víctimas han sufrido consecuencias emocionales o psicológicas debido a la difusión de "Deepfakes"*



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 Sinaluisa

Interpretación de resultados: La tabla muestra una clara tendencia hacia el 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. Esta alta proporción sugiere una percepción generalizada dentro de la comunidad jurídica sobre el impacto negativo que los "deepfakes" pueden tener en el bienestar emocional y psicológico de las personas afectadas. Esta tendencia resalta la importancia de abordar estas consecuencias al desarrollar estrategias legales y políticas para prevenir y mitigar los efectos perjudiciales de los "deepfakes" en las víctimas.

PREGUNTA NO.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?

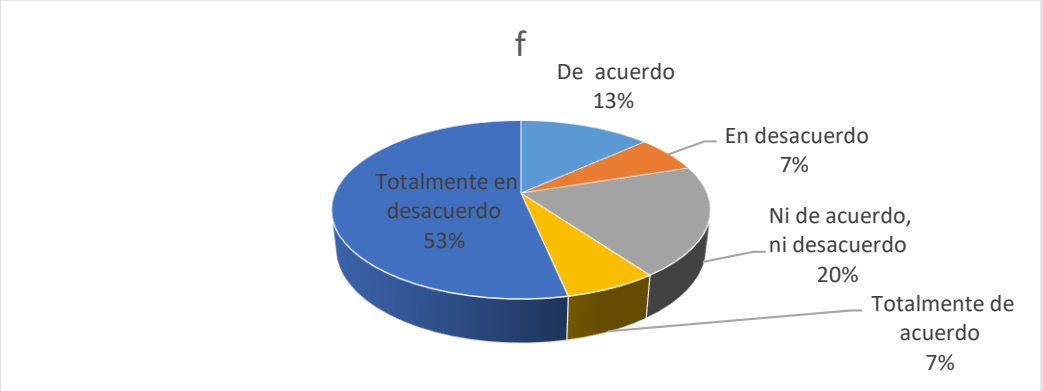
Tabla 10. *Considera que la legislación actual en el Ecuador aborda adecuadamente los casos de "Deepfakes" y su relación con la vulneración del derecho de intimidad*

OPCIONES	f	%
De acuerdo	2	13,33%
En desacuerdo	1	6,67%
Ni de acuerdo, ni desacuerdo	3	20,00%
Totalmente de acuerdo	1	6,67%
Totalmente en desacuerdo	8	53,33%
TOTAL	15	100%

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 Sinaluisa

Gráfico 11.*Considera que la legislación actual en el Ecuador aborda adecuadamente los casos de "Deepfakes" y su relación con la vulneración del derecho de intimidad*



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 Sinaluisa

Interpretación de resultados: La tabla revela una tendencia significativa hacia la percepción negativa sobre la manera en que Ecuador aborda los casos de "deepfakes". 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. Esta tendencia resalta la necesidad de revisar y fortalecer las políticas y regulaciones actuales para abordar de manera más efectiva el desafío emergente que representan los "deepfakes" en el país.

PREGUNTA NO.9. ¿Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos?

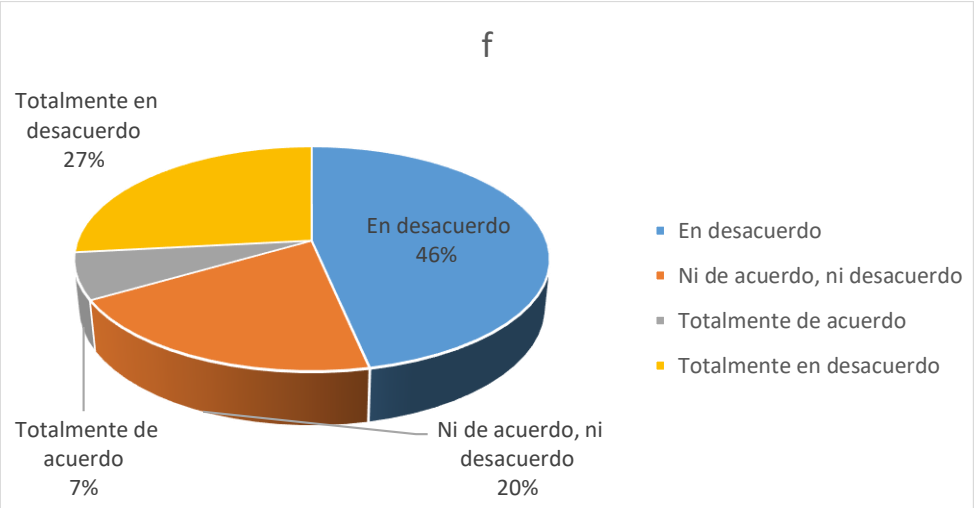
Tabla 11.*Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos*

OPCIONES	f	%
En desacuerdo	7	46,67%
Ni de acuerdo, ni desacuerdo	3	20,00%
Totalmente de acuerdo	1	6,67%
Totalmente en desacuerdo	4	26,67%
TOTAL	15	100%

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 Sinaluisa

Gráfico 12.*Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos*



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 Sinaluisa

Interpretación de resultados: La tabla sugiere una 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 generalizada dentro de la comunidad jurídica respecto a la capacidad del sistema judicial ecuatoriano para abordar efectivamente los delitos informáticos. Estos resultados resaltan la necesidad de implementar medidas adicionales, como la capacitación especializada y la actualización de la legislación, para mejorar la preparación de la justicia en este ámbito y garantizar una respuesta adecuada ante los desafíos que presentan los delitos informáticos en la era digital.

PREGUNTA NO.10 ¿Usted considera que se debe establecer como un tipo penal especifico al "Deepfakes", en nuestro Código Orgánico Integral Penal?

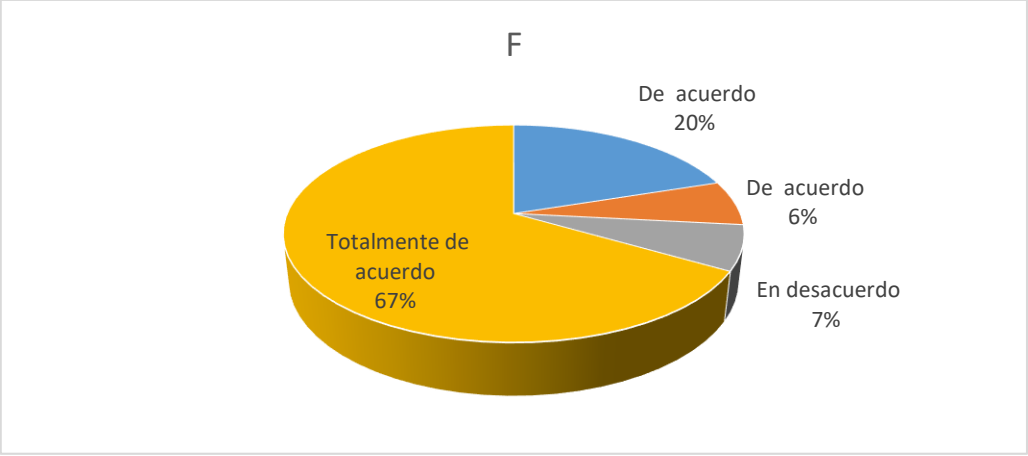
Tabla 12.*Usted considera que se debe establecer como un tipo penal especifico al "Deepfakes", en nuestro Código Orgánico Integral Penal*

OPCIONES	F	%
De acuerdo	3	20,00%
Ni De acuerdo, ni desacuerdo	1	6,67%
En desacuerdo	1	6,67%
Totalmente de acuerdo	10	66,67%
TOTAL	15	100%

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 Sinaluisa

Gráfico 13.*Usted considera que se debe establecer como un tipo penal especifico al "Deepfakes", en nuestro Código Orgánico Integral Penal*



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 Sinaluisa

Interpretación de resultados: La tabla revela una clara 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 una percepción generalizada dentro de la comunidad jurídica sobre la necesidad de establecer una legislación específica para abordar los delitos relacionados con los "deepfakes". Esta tendencia refleja una comprensión de la complejidad y gravedad de los impactos potenciales de los "deepfakes" en el ámbito legal y subraya la importancia de contar con un marco legal claro y adecuado para abordar este fenómeno emergente de manera efectiva.

En definitiva con los resultados de la encuesta realizada se destaca una falta de familiaridad generalizada con el concepto, lo que plantea dificultades para la identificación y el manejo adecuado de evidencia digital manipulada en el sistema judicial. Sin embargo, hay una creciente conciencia sobre la importancia de contar con herramientas especializadas para detectar y abordar los "deepfakes", así como una clara tendencia hacia la necesidad de regulaciones legales para abordar este fenómeno emergente. Además, se evidencia una preocupación extendida sobre los riesgos que los "deepfakes" representan para la privacidad y la reputación de las personas, lo que destaca la necesidad de adaptar el marco legal para proteger los derechos fundamentales en un entorno digital.

4.1.1. Análisis de la definición doctrinal y dogmática del "deepfake"

Los hallazgos de los datos recopilados con respecto a la definición doctrinal de varios autores manifiestan que el fenómeno "deepfake", se genera a través del aprendizaje profundo y la inteligencia artificial, tiene como objetivo principal la producción de contenido audiovisual fabricado con la intención de engañar mediante la manipulación de estímulos visuales y auditivos. Esta metodología permite crear vídeos altamente engañosos que son capaces de imitar las expresiones faciales, los gestos y las voces de personas reales de una manera extraordinariamente realista, basándose en el análisis de amplios conjuntos de datos. Además, cabe señalar que la existencia de "deepfakes" pornográficos es una manifestación específica de esta tecnología, en la que se emplea el aprendizaje profundo para fabricar y manipular contenido sexualmente explícito sin el consentimiento de las partes involucradas, lo que amplifica las preocupaciones éticas y legales asociadas con su uso.

4.1.2. Dificultades legales probatorias del "deepfake".

Con los resultados se ha llegado a determinar que el desafío jurídico que representan los "deepfakes", abordando diversos aspectos desde el rastreo de su origen hasta las repercusiones en la confianza judicial. En primer lugar, se destaca la dificultad para atribuir responsabilidad y determinar pruebas en casos relacionados con "deepfakes" debido a la complejidad para identificar su origen y la manipulación del contenido. Se resalta la necesidad de contar con expertos en investigaciones en línea y ciberinteligencia para abordar estos desafíos, señalando que en Ecuador existen escasos expertos en este ámbito.

El papel fundamental de la dirección IP en la identificación de "deepfakes", así como las dificultades asociadas con la imputación de responsabilidad a través de esta evidencia,

ya que la dirección IP puede no proporcionar información suficiente para identificar al responsable directo del delito. Se menciona la diferencia entre direcciones IP fijas y dinámicas, así como la necesidad de contar con peritos informáticos especializados para analizar la evidencia digital de manera adecuada.

Además, se hace hincapié en la importancia de las pericias informáticas para determinar la veracidad de los contenidos digitales, incluidos los "deepfakes", destacando que los peritos deben mantenerse actualizados con las técnicas más recientes debido a la evolución constante de las herramientas de generación de "deepfakes". Se aborda también la importancia de la documentación y presentación adecuada de la evidencia digital en los procedimientos judiciales, así como la necesidad de contar con herramientas especializadas para detectar "deepfakes", aunque se reconoce que estas herramientas pueden tener limitaciones.

Por otro lado, se discute la carga de la prueba en casos de "deepfakes", señalando que corresponde al fiscal de delitos informáticos probar los supuestos de hecho, y la importancia de contar con informes periciales informáticos como medio de prueba en los procesos judiciales.

Finalmente, se mencionan las repercusiones de los "deepfakes" en la confianza judicial, destacando cómo pueden afectar la manipulación de evidencia, la autenticidad de las pruebas presentadas y la percepción pública del sistema judicial. Se plantea la necesidad de desarrollar estrategias efectivas para abordar este problema y proteger la integridad de las pruebas presentadas en el sistema judicial.

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

Tabla 13.*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. leyes contra la "pornografía no consensual" (más conocida como "porno venganza") que buscan incluir dentro de dicha definición los "*deepfakes*" pornográficos, así como cualquier vídeo o imagen manipulados con herramientas digitales.	**Enmienda** el artículo 3144 incluye una definición de los "deepfakes" que se refiere a una ultra falsificación. Los "deepfakes" abarca el contenido manipulado	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 de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.	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 El Título III enuncia los derechos de las personas en relación la protección y tratamiento de sus datos personales	Ley Federal de Protección de Datos Personales ejerce sus derechos de acceso, rectificación, cancelación y oposición	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
Sanciones y penas	En Virginia hasta un año de cárcel y 2.500 dólares de multa	El artículo 189 del Código Penal y establece condenas de hasta 9 años de prisión	En el Código Penal Federal sería de entre tres y seis años de prisión y multas de entre 54,000 y 109,000 pesos.	No hay legislación específica sobre "deepfakes" , pero se podría aplicar leyes relacionadas con la vulneración del derecho a la intimidad
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 Sainaluisa Sagñay*

4.2. Discusión

Lavanda (2022) destaca la grave amenaza que representa el mal uso de los "deepfakes" tanto para figuras políticas como no políticas. Estos videos, creados con fines delictivos, especialmente en la generación de pornografía no consentida, en el cual las víctimas sufren múltiples vulneraciones de sus derechos, incluyendo el derecho a la intimidad personal y familiar, y por ello la necesidad de crear normativa legal ante esta problemática. De lo mencionado por el autor concuerdo totalmente , ya que de acuerdo a la investigación, ya tenemos un precedente, un caso en la ciudad de Quito, pues de los resultados de las encuestas existe una fuerte tendencia que sugiere una percepción generalizada dentro de la comunidad jurídica sobre la necesidad de establecer una legislación específica para abordar los delitos relacionados con los "deepfakes", es importante tener en cuenta que una minoría considerable sí reconoce este incremento, también se reflejar una mayor conciencia sobre el fenómeno y sus implicaciones legales, un alto porcentaje de encuestados sugiere un consenso generalizado dentro de la comunidad jurídica sobre la importancia de establecer marcos normativos para abordar cuestiones específicas o emergentes, de los "deepfakes". Por otra parte se destaca la sobre el desafío probatorio partiendo de la falta de herramientas tecnológicas y técnicas, así como peritos especializados en Inteligencias artificial y comparación facial, estos son los desafíos que presenta en el sistema judicial ecuatoriano, ante futuros delitos de los "deepfakes" pornográficos.

Celebi et al. (2022) manifiestan que la existencia de desafíos en el ámbito de la dificultad probatoria, se relación con el avance de la tecnología y su impacto en la

autenticación de pruebas en el contexto judicial. La presencia de Redes Generativas Adversarias complica aún más este panorama, ya que estas redes están diseñadas para mejorar continuamente y pueden producir videos pornográficos "deepfakes" cada vez más convincentes. Coincido totalmente con los autores en virtud de que la problemática de los "deepfakes" desde una perspectiva jurídica existen desafíos sustanciales en la atribución de responsabilidad y la determinación de pruebas en casos judiciales. La dificultad para rastrear el origen de estos contenidos falsos y la identificación precisa de los responsables. Se requiere profesionales expertos en ciberinteligencia y peritaje informático, habilidades escasas en el contexto ecuatoriano. La dirección IP emerge como un elemento clave para rastrear la actividad delictiva en línea, pero su imputación a individuos específicos presenta desafíos, ya que suele estar asociada a proveedores de servicios de Internet y no a usuarios individuales. La ausencia de peritos expertos en temas informáticos son obstáculos significativos para abordar el problema de los "deepfakes", lo que dificulta la identificación y la verificación de la autenticidad de estos contenido, tal como lo indica Celebi et al.

Soler (2023) destaca la necesidad apremiante a nivel internacional de contar con una competencia judicial avanzada y altamente especializada para abordar los desafíos planteados por la proliferación de vídeos falsificados generados por inteligencia artificial. Propone la participación de la propia inteligencia artificial en el proceso judicial para identificar dichos vídeos. Coincido con el autor debido que a medida que evoluciona la tecnología y su uso malicioso, las normas y procesos judiciales en varios países como EEUU, México, España ya han cambiado, para sancionar actos que vulneren derechos, sin embargo el Ecuador no cuenta con una normas y procesos para tratar ese tipo de actos, además, la dificultad probatoria y el desafío de incorporar normativa adecuada también representan obstáculos importantes, tal como lo menciona en su estudio Soler.

El texto normativo actual está establecido de la siguiente manera: art 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, 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, 2014). La perspectiva de propuesta de reforma: 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. Por esta razón concuerdo lo que menciona Vásconez (2020) respecto a un verdadero Estado, el cual deber ser garante de derechos y garantías para todos los ciudadanos, el Estados debe ser coherente en su política criminal, y la necesidad de un reforma al COIP, acorde va evolucionando al sociedad, por lo tanto el sistema legislativo debe establecer normativa coherente y garantista.

Los “deepfake” vulneran el derecho a la intimidad, debido a la falta de normativa y su dificultad probatoria para llegar a los responsables, la pornografía falsa, representa un problema emergente actualmente, su impacto significativo en relación a derecho a la intimidad, especialmente en Ecuador dónde la normativa es inexistente para este acto delictivo. Ecuador como otros países enfrentan desafíos significativos en la regulación y sanción de la creación y distribución de deepfake, pues la normativa existente no contempla específicamente el mal uso del IA para crear contenido falso, por otra parte las dificultad probatoria es otro aspecto relevante para demostrar que un video es un “ deepfake” por lo que se requiere de evidencia técnica sólida y pericias especializadas, que no siempre está disponible o es accesible en el sistema judicial ecuatoriano. Por ende la necesidad de una reforma a la normativa penal, y fortalecimiento de técnicas conjuntamente con la cooperación internacional. Con lo expresado concuerdo Valpato (2016) quien menciona que los perjuicios que causa la información falsa, afecta la esfera de la vida íntima, vinculadas con la tecnología, a través del internet, causan más daños que las noticias falsas que se daba por medios tradicionales.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Varios doctrinarios coinciden en significado del “deepfakes”, el cual es un método de inteligencia artificial en el cual desarrolla algoritmos que permiten moldear abstracciones faciales, y generar patrones audiovisuales, y como resultado se obtiene un video falso. Además varías legislaciones como México, Estados Unidos y España, ya han tipificado al “deepfakes” como un delito, con su respectiva sanción, es así que representan un riesgo significativo en términos del uso indebido de la tecnología para crear “deepfakes” pornográficos. Estos vídeos no solo afectan a la privacidad y la reputación de las personas involucradas, sino que también socavan la confianza pública y difundir información errónea y desacreditar a figuras políticas y públicas. Lo cual resalta la necesidad urgente de abordar esta cuestión desde una perspectiva legal y tecnológica integrada para salvaguardar los principios democráticos y los derechos fundamentales

Respecto a la Dificultad probatoria en el ámbito Judicial se concluye que los “deepfakes” plantean desafíos significativos para la identificación del origen y la atribución de responsabilidad. El rastreo de la dirección IP es una herramienta muy importante para establecer la veracidad, autenticidad, responsabilidad, ya que se determina el dispositivo que fue utilizado para generar y distribuir el contenido falso. Las pericias informáticas desempeñan un papel crucial para determinar la veracidad del contenido mediante técnicas especializadas en el cual se analiza la estructura del archivo, mediante anomalías y detectar manipulaciones. El análisis exhaustivo de la evidencia digital implica examinar metadatos, archivos, comunicaciones y redes sociales para buscar patrones y pistas relevantes para la investigación, estos datos son plasmados en el informe del perito informático especializado en la IA. Ante la complejidad y las implicaciones de los “deepfakes” en el sistema judicial ecuatoriano, se sugiere la necesidad de implementar normativas urgentes para fortalecer la capacidad del sistema legal en la identificación, manejo de pruebas de casos relacionados con esta tecnología. Esto incluye la formación y especialización de peritos informáticos en inteligencia artificial y análisis facial.

Respecto al derecho comparado, la legislación y medidas adoptadas en Estados Unidos, España, México en relación con el fenómeno del “deepfakes” revela similitudes y diferencias significativas en la forma en que estos países abordan el problema. Mientras que Estados Unidos, y España, han promulgado leyes específicas que incluyen la prohibición de “deepfakes” en contextos como la pornografía no consensuada, México y Ecuador carece de una legislación explícita sobre este tema. Sin embargo, tanto México como Ecuador han establecido disposiciones legales para proteger la privacidad y los datos personales, lo que podría proporcionar un marco para abordar los aspectos de privacidad relacionados con los “deepfakes”. En términos de sanciones, aunque varían en intensidad, todos los países consideran el delito de “deepfakes” como una violación grave, lo que subraya la importancia atribuida a la protección de la integridad y la privacidad de las personas en el entorno digital. Además, la cooperación internacional en la lucha contra la cibercriminalidad, incluidos los

"deepfakes", se ve reflejada en la adhesión a convenios internacionales como el Convenio de Budapest en todos los países analizados, lo que destaca la necesidad de una colaboración global para abordar eficazmente este fenómeno en constante evolución.

La pornografía falsa "Deepfakes" y sus dificultades probatorias, violentan el derecho de intimidad debido a que estas tecnologías, representan una seria amenaza para la integridad y privacidad de las personas, permitiendo la creación de contenido audiovisual falso y convincente que puede ser utilizado para difamar, acosar o extorsionar a individuos. En términos legales, la creación y difusión de "deepfakes" sin consentimiento pueden constituir diversos delitos, como difamación, violación de la privacidad, acoso o extorsión. Sin embargo, la complejidad de los "deepfakes" presenta desafíos para la aplicación efectiva de la ley, incluyendo la identificación de responsables y la autenticación del contenido manipulado.

5.2 RECOMENDACIONES

Se recomienda la implementación de estrategias integrales que combinen medidas legales y tecnológicas para hacer frente al problema del "deepfakes" y sus implicaciones, especialmente en lo que respecta a la creación de "deepfakes" pornográficos y su impacto en la privacidad, reputación y confianza pública. Es fundamental que los países que aún no han tipificado al "deepfakes" como un delito consideren hacerlo y establezcan sanciones proporcionales, al tiempo que fortalecen la cooperación internacional para abordar este desafío de manera efectiva. Además, se debe promover la educación y concienciación sobre los riesgos asociados con el uso indebido de la tecnología, tanto entre la población general como entre las figuras públicas y políticas, para mitigar la difusión de información errónea y la desinformación. En última instancia, es crucial desarrollar y aplicar herramientas y técnicas de detección y verificación de "deepfakes" para proteger los derechos fundamentales y preservar la integridad de la información en la era digital.

En relación con el fenómeno del "deepfakes", se recomienda que México y Ecuador consideren la promulgación de leyes específicas que aborden directamente los "deepfakes", especialmente en contextos como la pornografía no consensuada. Esta acción legislativa contribuiría a llenar el vacío legal existente en ambos países y proporcionaría un marco claro para abordar este problema emergente de manera más efectiva. Además, se sugiere que tanto México como Ecuador fortalezcan y amplíen sus disposiciones legales existentes relacionadas con la protección de la privacidad y los datos personales para abordar de manera más completa los aspectos de privacidad relacionados con los "deepfakes". Esto garantizaría una mayor protección de la integridad y la privacidad de las personas en el entorno digital.

En el Ecuador ante la complejidad de los " deepfakes" en el sistema judicial, se sugiere la implementación de medidas emergentes para fortalecer la capacidad del sistema legal respecto a la identificación, el manejo y búsqueda y recopilación de pruebas para identificar al responsable de este hecho delictivo, para ello se incluye la formación y especialización de peritos informáticos en la inteligencia artificial y el análisis de características faciales, con la finalidad de establecer protocolos y normativas para garantizar la admisibilidad, confidencialidad y autenticidad de las pruebas digitales en los procesos

judiciales. Es relevante configurar un marco legal sólido y eficaz que aborde los desafíos establecidos por los "deepfakes", asegurando así la justicia y la protección de los derechos de las partes involucradas en el procedimiento legal.

Es recomendable que nuestra sociedad se difunda información sobre la naturaleza del "deepfakes" y los posibles riesgos asociados a su utilización. Esta difusión debe realizarse a través de diversos medios de comunicación y redes sociales, y los datos deben ser proporcionados por profesionales del campo respectivo. El objetivo principal de este esfuerzo es educar a la sociedad sobre asuntos relacionados con sus derechos sexuales y su derecho a la intimidad. Es importante hacer hincapié en que nuestras acciones en las redes sociales tienen implicaciones duraderas, por lo que es necesario estar atentos a la hora de compartir información personal.

BIBLIOGRAFÍA

6. Referencias bibliográficas

6.1 Bibliografía

Antar, L. 2016. (2016) Tipología De Las Investigaciones Jurídicas https://dialnet.unirioja.es/descarga/articulo/5456267.pdf

Aguilera, A. T. (2001). Nuevas tecnologías, intimidad y protección de datos: Con Estudio Sistemático de la Ley Orgánica 15/1999. Edisofer S.L.

Anderson, K. E. (2018). Getting acquainted with social networks and apps: combating fake news on social media. Library Hi Tech News, 35(3), 1-6. https://doi.org/10.1108/lhtn-02-2018-0010

Asamblea Estadounidense. (2019). Proyecto De Ley "Derecho De Acción Privado" https://factchequeado.com/teexplicamos/20230922/nuestros-derechos-si-utilizan-nuestra-imagen-en-deepfake-sin-nuestro-consentimiento/

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

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

Asamblea Nacional. (2022). *Código Orgánico Integral Penal.* Lexis Finder.

Atienza, M. (2017). Filosofía del derecho y transformación social. 1(1) https://dialnet.unirioja.es/servlet/libro?codigo=699047

Atienza, M. (2017). Filosofía del derecho y transformación social. Dialnet. https://dialnet.unirioja.es/servlet/libro?codigo=699047

Barrera, G. (2012). *El Pacto Internacional de Derechos Civiles y Políticos.* Comisión

Beamonte, P. (2018). FakeApp, el programa de moda para crear vídeos porno falsos con IA. Hipertextual. https://hipertextual.com/2018/01/fakeapp-videos-porno-falsos-ia

Bernal, A. B. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. Opinión Jurídica, 2(4), 109-116. https://revistas.udem.edu.co/index.php/opinion/article/view/1350

Bezanson, R. P. (1992). The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990. California Law Review, 80(5), 1133-1175. https://doi.org/10.2307/3480738

Borges, L., Martins, B., & Calado, P. (2019). Combining Similarity Features and Deep Representation Learning for Stance Detection in the Context of Checking Fakehttp://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

News. Journal Of Data And Information Quality, 11(3), 1-26. https://doi.org/10.1145/3287763

Botero Bernal, A. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. Opinión Jurídica, 2(4), 109-116. Recuperado a partir de https://revistas.udem.edu.co/index.php/opinion/article/view/1350

Cámara de Diputados. (2020). Ley Olimpia. URI: http://bibliodigitalibd.senado.gob.mx/handle/123456789/5043.

Cámara de Diputados. (2023). Código Penal Federal. https://mexico.justia.com/federales/codigos/codigo-penal-federal/

Carrasco, O. D. (2022) Detección de videos modificados por la técnica de intercambio de identidad DeepFake. Retrieved from: https://hdl.handle.net/20.500.12371/18327.

Castells, M. (2001): Internet y la Sociedad Red.

Cebeli et al. (2022) Una encuesta sobre la detección profunda de falsificaciones para los tribunales de primera instancia, Departamento de Informática, Universidad Estatal Sam Houston, Huntsville, TX, EE.UU. https://arxiv.org/abs/2205.15792

Cerdán, M. & Castillo, G. (2019) *Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso*. Fundación Dialnet, Universidad de la Rioja https://revistas.ucm.es/index.php/HICS/article/view/66293/4564456552459

ChildFund. (2023). Campaña "Naveguemos Seguros". https:// www.eloriente.com/articulo/childfund-presento-en-ecuador-la-campana-naveguemos-seguros/38860

Cole, S. (2017). AI-Assisted Fake Porn Is Here and We're All Fucked. VICE MEDIA GROUP. https://www.vice.com/en/article/gydydm/gal-gadot-fake-ai-porn

Congreso de Diputados. (2023) Código Federal Penal. https://docs.mexico.justia.com/federales/testing/codigo-penal-federal.pdf

Comisión Europea. (2020)*libro blanco sobre la inteligencia artificial*. https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-

b9e44e79825b_es?filename=commission-white-paper-artificial-intelligence-feb2020_es.pdf

Comisión Europea. (2020)*LIBRO BLANCO sobre la inteligencia artificial*. https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_es?filename=commission-white-paper-artificial-intelligence-feb2020_es.pdf

Congreso Estadounidense. (2018) ley sobre la difusión de Deep fakes por medios de comunicación social.

Congreso de Diputados. (2023) Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial. https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF

Consejo Europeo & Parlamento Europeo. (2022) *Ley de Comunicación Audivisual*. file:///C:/Users/user/Downloads/2340-5155-2022-0010-0002-0195-0199.pdf

Consejo Europeo & Parlamento Europeo. (2022) *Ley de Comunicación Audivisual*. file:///C:/Users/user/Downloads/2340-5155-2022-0010-0002-0195-0199.pdf

Consejo Europeo. (2019) Plan Coordinado sobre la Inteligencia Artificial. https://www.lexis.com.ec/noticias/parlamento-europeo-ue-sobre-ley-inteligencia-artificial-union-europea

Consejo Europeo. (2019) Plan Coordinado sobre la Inteligencia Artificial. https://www.lexis.com.ec/noticias/parlamento-europeo-ue-sobre-ley-inteligencia-artificial-union-europea

Convención Europea de Derechos Humanos. (1950). Roma: European Court og HumanRights. https://prdechr.coe.int/documents/d/echr/Convention_Instrument_SPA#:~:text=El%20Convenio%20Europeo%20de%20Derechos%20Humanos%2C%20firmado%20en%20Roma%20el,Universal%20de%20los%20Derechos%20Humanos.

Corte Constitucional. (2012) Sentencia de Protección de Datos Personales De Persona Jurídica. https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=001-14-PJO-CC

Dvovarkova, M. (2020). Pornovenganza y Deepfake: Protección Privacidad En La Era De La Tecnologías Modernas. Revisión de derecho y tecnología, 11(22).https://doi.org/10.5817/RPT2020-2-2

Ehrenkranz, M. (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

El Oriente. (2023). ChildFund presentó en Ecuador la campaña «Naveguemos Seguros». https://www.eloriente.com/articulo/childfund-presento-en-ecuador-la-campana-naveguemos-seguros/38860

Fido, D., & Harper, C. A. (2020). An Introduction to Image-Based Sexual Abuse. En Springer eBooks (pp. 1-26). https://doi.org/10.1007/978-3-030-59284-4_1

Gomes, G. (2022) Los deepfakes como una nueva forma de desinformación corporativa – una revisión de la literatura .*IROCAMM*, 5(2). https://institucional.us.es/revistas/IROCAMM/5_2_2022/IROCAMM_V5-N2-2022_02_gomes-goncalves.pdf

Gonçalves, S. G. (2022). Los deepfakes como una nueva forma de desinformación corporativa – una revisión de la literatura. International Review Of Communication And Marketing Mix, 5(2), 22-38. https://doi.org/10.12795/irocamm.2022.v05.i02.02

Guera, D., & Delp, E.J. (2018). Deepfake Video Detection Using Recurrent Neural Networks. 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 1-6. https://doi.org/10.1109/avss.2018.8639163

Hamborg, F., Donnay, K., & Gipp, B. (2018). Automated identification of media bias in news articles: an interdisciplinary literature review. International Journal On Digital Libraries, 20(4), 391-415. https://doi.org/10.1007/s00799-018-0261-y

Hassemer, W., & Sanchez, A. C. (2003). El Derecho a la Autodeterminación Informática y los Retos del Procesamiento Automatizado de Datos Personales. Editorial Del Puerto. http://fcaenlinea.unam.mx/anexos/1141/1141_u5_act1.pdf

Home Security Heroes (2023) State of Deepfake. [Estados de los falsificaciones profundas]. Consultado el 1 de marzo de 2024. https://www.homesecurityheroes.com/state-of-deepfakes/

INEC. (2021). Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación. http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J2VzY3JpdG8nLCB1dWlkOidlMWE3ZDk0MC0wZDE3LTRkYWEtYjVkNi04YmMzN2Q2YjMyYjQucGRmJ30=#:~:text=En%20Ecuador%2C%20el%20acceso%20a,actividades%20comunicacionales%20y%20redes%20sociales.

Janariz, A. (1996) El Derecho A La Intimidad, De Samuel D. Warren Y Louis D. Brandéis.file:///C:/Users/user/Downloads/Dialnet-ElDerechoALaIntimidad-2005532.pdf

Karasavva, V., & Noorbhai, A. (2021). The Real Threat of Deepfake Pornography: A Review of Canadian Policy. Cyberpsychology, Behavior, And Social Networking, 24(3), 203-209. https://doi.org/10.1089/cyber.2020.0272

Kugler, M. B., & Pace, C. (2021). Deepfake Privacy: Attitudes and Regulation. Social Science Research Network. https://doi.org/10.2139/ssrn.3781968

Lavanda, M. (2022) Deepfake: Cuando la inteligencia artificial amenaza el Derecho y la Democracia. *Lawgic Tec - Revista de Derecho y Tecnología*, 1(2). https://lawgictec.org/wp-content/uploads/Lawgic-Tec-Revista-de-Derecho-y-Tecnologia-No_2-Julio-2022.pdf

Lavié, H. Q. (1993). Derecho a la intimidad y objeción de conciencia. Universidad Externado de Colombia, Instituto de Estudios Constitucionales Carlos Restrepo Piedrahita https://www.bcn.cl/delibera/show_iniciativa?id_colegio=3701&idnac=1&patro=0&nro_torneo=2023

Maddocks, S. (2020). 'A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deep fakes. Porn Studies, 7(4),. https://doi.org/10.1080/23268743.2020.1757499

Maldonado et al. (2019). Tópicos De Metodología De La Investigación Jurídica. Universidad Xalapa. https://www.uv.mx/mdhjc/files/2021/12/Topicos-de-Metodologia-de-la-Investigacion-Juridica.pdf

Mania, K. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. Trauma, Violence, & Abuse, 25(1), 117-129. https://doi.org/10.1177/15248380221143772

Martínez, A. (2000) El Derecho a la Intimidad Y Su Necesaria Inclusión Como Garantía Individual. *Revista ABZ.* 126(1). https://repositorioinstitucional.buap.mx/server/api/core/bitstreams/616d21c1-ea6a-4b19-8822-ad0f5f871839/content

MEA. (2023). Violencia en Entornos Digitales. https://defensadelpublico.gob.ar/wp-content/uploads/2023/03/violencia-en-entornos-digitales-v3.pdf

Méjan, L. (1996) El Derecho a la Intimidad y la Informática. *Editorial Porrúa*. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Méjan, L. M. C. (1994). El derecho a la intimidad y la informática. Editorial Porrúa.

Merino, M. (2019). Así es posible saber si un vídeo es un deepfake con sólo un abrir y cerrar de ojos, literalmente. Xataka. https://www.xataka.com/inteligencia-artificial/posible-saber-video-deepfake-solo-abrir-cerrar-ojos-literalmente-quizas-eso-no-sea-suficiente

Nacional De Los Derechos Humanos. https://www.corteidh.or.cr/tablas/r29904.pdf

OEA. (1978). Convención Americana sobre Derechos Humanos o Pacto de San José. https://cidh.oas.org/annualrep/78sp/indice.htm

Oliva, M. L. (2022). “Deepfake”: Cuando la inteligencia artificialamenaza el Derecho y la Democracia. https://www.researchgate.net/publication/368330820_Deepfake_Cuando_la_inteligencia_artificial_amenaza_el_Derecho_y_la_Democracia

ONU (2015). Declaración Universal de Derechos Humanos. https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Parlamento Europeo. (2024). Código de Procedimiento Civil. https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=333&modo=2&nota=0&tab=2

Parlamento Europeo. (2021). Ley de Inteligencia Artificial: aprobación del Parlamento Europeo. https://www.lexis.com.ec/noticias/parlamento-europeo-ue-sobre-ley-inteligencia-artificial-union-europea

Parlamento Europeo. (2021). Ley de Inteligencia Artificial: aprobación del Parlamento Europeo. https://www.lexis.com.ec/noticias/parlamento-europeo-ue-sobre-ley-inteligencia-artificial-union-europea

Quiroga, H. (1995) Derecho a la intimidad y objeción de conciencia. https://search.worldcat.org/es/title/derecho-a-la-intimidad-y-objecion-de-conciencia/oclc/318340283

Rana, M. S., & Sung, A. H. (2023). Deepfake Detection. IWSPA ’23: Proceedings of the 9th ACM International Workshop On Security and Privacy Analytics. Association For Computing Machinery. https://doi.org/10.1145/3579987.3586562

Redacción Vistazo. (2023). Alumnos de un colegio de Quito usaron inteligencia artificial para crear videos sexuales con los rostros de sus compañeras. www.vistazo.com. https://www.vistazo.com/actualidad/nacional/alumnos-de-un-colegio-de-quito-usaron-inteligencia-artificial-para-crear-videos-sexuales-con-los-rostros-de-sus-companeras-ME6107394

Redacción Vistazo. (2023). Alumnos de un colegio de Quito usaron inteligencia artificial para crear videos sexuales con los rostros de sus compañeras. https://www.vistazo.com/actualidad/nacional/alumnos-de-un-colegio-de-quito-usaron-inteligencia-artificial-para-crear-videos-sexuales-con-los-rostros-de-sus-companeras-ME6107394

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

Rössler, A., Cozzolino, D., Verdoliva, L., Rieß, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to Detect Manipulated Facial Images. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1901.08971

Rossler, et all. (2019) Learning to Detect Manipulated Facial Images. https://openaccess.thecvf.com/content_ICCV_2019/html/Rossler_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.html

Symantec. 2018. Informe sobre amenazas a la seguridad en Internet. Volumen 23, marzo. www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pd

Soler, E. (2023). *Retos jurídicos derivados de la Inteligencia Artificial Generativa*. Indret.

https://dialnet.unirioja.es/descarga/articulo/5456267.pdf

Somers, M. (2020). Deepfakes, explained. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

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

Tantaleán, R. (2016). Tipología de las investigaciones jurídicas. Revista digital Dialnet, (43)-.1-37.

Tellez, A. (2001) *Nuevas tecnologías, intimidad y protección de datos.* *https://books.google.com.ec/books/about/Nuevas_tecnolog%C3%ADas_intimidad_y_protecci.html?id=KpHqAAAACAAJ&redir_esc=y*

Tolsana et al. (2022). Detección de videos modificados por la técnica de intercambio de identidad DeepFake.

UNDOC. (2023). Estudio exhaustivo sobre el delito cibernético. https://indret.com/wp-content/uploads/2023/04/1767.pdf

Valpato, S. (2016). El derecho a la intimidad y las nuevas tecnologías de la información, 1. https://idus.us.es/bitstream/handle/11441/52298/EL%20DERECHO%20A%20LA%20INTIMIDAD%20Y%20LAS%20NUEVAS%20TECNOLOGI%cc%81AS%20DE%20INFOR.pdf?sequence=1&isAllowed=y

Vásconez, V. (2020). Las decimonónicas ideas del legislador ecuatoriano: política criminal y dolo en la reforma al COIP, 7(1) https://www.redalyc.org/journal/6002/600263428012/600263428012.pdf

Villabela, C. (2012). Los Métodos Jurídicos en la Investigación Jurídica. UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3983/46.pdf

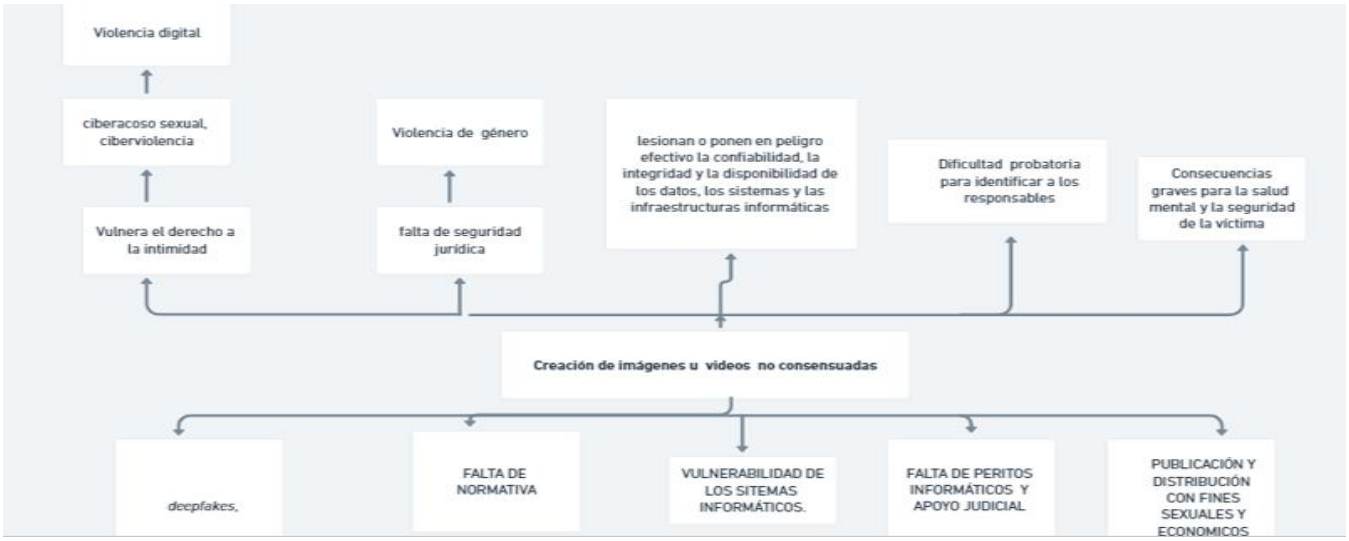
Villabella, C. (2020). Métodos de análisis y procesamiento de datos. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6226/12a.pdf

Viola, P. & M. Jones. (2001). “Rapid object detection using a boosted cascade of simple features,” Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. I-511-I-518. https://doi.org/10.1109/cvpr.2001.990517

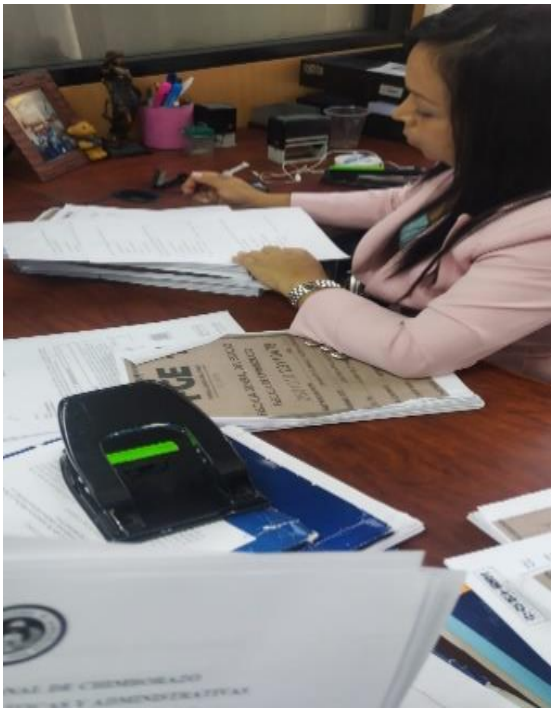
Vives, S. (2019). Posverdad. La nueva guerra contra la verdad y cómo combatirla. De Mattew d’Ancona, Alianza Editorial, 2019. Clivatge, 7, 286-297. https://doi.org/10.1344/clivatge2019.7.8

ANEXOS

Anexo 1: Árbol de problemas



Anexo 2: Realización de encuestas



Anexo 3
Encuestas

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

ENCUESTA

Destinatario: Fiscales Especializados en Violencia de Género de la ciudad de Riobamba, jueces de la Unidad Judicial Penal, y, defensores Privados Especializados en derecho penal.

Objetivo: Analizar el "Deepfake" como conducta informática no tipificada en el Código Orgánico Integral Penal y su incidencia en la violación al derecho a la intimidad que afectan a mujeres y a la sociedad.

Introducción: La presente encuesta tiene por objeto recabar información para la realización del proyecto de investigación titulado "Deepfakes", dificultades probatorias y su incidencia en la vulneración al derecho de intimidad" la misma que tendrá fines eminentemente académicos.

Preguntas

1. ¿Está familiarizado con el concepto de Deepfakes y su uso en contextos legales?

1. Muy familiarizado ( )
2. Familiarizado ( )
3. Neutral ( )
4. Poco familiarizado ( )
5. No familiarizado ( )

NOTA: Definición de "Deepfake". El **"**Deepfake"es la generación de imágenes o videos convincentes pero completamente falsos. Mediante el uso de la inteligencia artificial crean nuevas imágenes o vídeos basados en otros, sustituyendo a la persona que aparece en ellos, generalmente son usados para contenido pornográfico.

2. ¿Considera que el uso de Deepfakes se ha incrementado en los últimos tiempos?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

3. ¿Usted cree urgente la necesidad de incorporar regulaciones legales que aborden la problemática de los Deepfakes en el Ecuador?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

4. **NOTA :**Si su respuesta fue afirmativa, especifique cuales son los desafíos: ……
……
……

5. ¿Considera que la tecnología actual proporciona herramientas suficientes para detectar y autenticar Deepfakes?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

NOTA : Si su respuesta fue afirmativa, especifique cuales: ……
……
……

6. ¿Considera que el sistema judicial mantiene desaf importantes en la autenticidad de un contenido de Deepfake?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

    NOTA : Si su respuesta fue afirmativa, especifique cuales son los desafíos: ……
    ……
    ……

7. ¿En su opinión, cree que los Deepfakes representan una amenaza significativa para el derecho de intimidad de las personas?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

8. ¿Usted cree qué las víctimas han sufrido consecuencias emocionales o psicológicas debido a la difusión de Deepfakes?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

9. ¿Considera que la legislación actual en el Ecuador aborda adecuadamente los casos de Deepfakes y su relación con la vulneración del derecho de intimidad?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

10. ¿Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos?

    1. Totalmente en desacuerdo ( )
    2. En desacuerdo ( )
    3. Ni de acuerdo, ni desacuerdo( )
    4. De acuerdo ( )
    5. Totalmente de acuerdo( )

11. ¿Usted considera que se debe establecer como un tipo penal especifico al Deepfakes, en nuestro Código Orgánico Integral Penal?

1. Totalmente en desacuerdo ( )
2. En desacuerdo ( )
3. Ni de acuerdo, ni desacuerdo( )
4. De acuerdo ( )
5. Totalmente de acuerdo( )