UNIVERSIDAD CATÓLICA DE CUENCA

# UNIVERSIDAD CATÓLICA DE CUENCA

*Comunidad Educativa al Servicio del Pueblo*

## UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

### CARRERA DE DERECHO

### TÍTULO

# DELITO DE DEEPFAKE Y PORNOGRAFÍA INFANTIL GENERADA POR INTELIGENCIA ARTIFICIAL (IA) EN LA LEGISLACIÓN ECUATORIANA

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA**

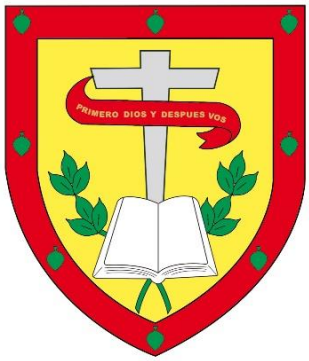
**AUTORA: RENATA CORREA PEÑA**

**DIRECTOR: DR. PABLO ARTURO POZO CABRERA, MGS**

**CUENCA - ECUADOR**

**2024**

**DIOS, PATRIA, CULTURA Y DESARROLLO**




# UNIVERSIDAD CATÓLICA DE CUENCA

*Comunidad Educativa al Servicio del Pueblo*

## UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

## CARRERA DE DERECHO

**TÍTULO**

DELITO DE DEEPFAKE Y PORNOGRAFÍA INFANTIL GENERADA POR INTELIGENCIA ARTIFICIAL (IA) EN LA LEGISLACIÓN ECUATORIANA

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA**

**AUTORA: RENATA CORREA PEÑA**

**DIRECTOR: DR. PABLO ARTURO POZO CABRERA, MGS**

**CUENCA - ECUADOR**

**2024**

**DIOS, PATRIA, CULTURA Y DESARROLLO**

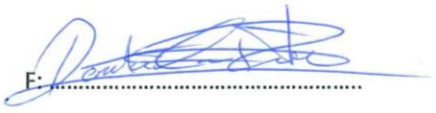
Universidad Católica de Cuenca

## DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

**Declaratoria de Autoría y Responsabilidad**

**Renata Correa Peña** portador(a) de la cédula de ciudadanía Nº **0107287450**. Declaro ser el autor de la obra: "DELITO DE DEEPFAKE Y PORNOGRAFÍA INFANTIL GENERADA POR INTELIGENCIA ARTIFICIAL (IA) EN LA LEGISLACIÓN ECUATORIANA" sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **10 de octubre de 2024**



F: .....

**Renata Correa Peña**

C.I. **0107287450**

Universidad Católica de Cuenca

**CERTIFICO**

Certifico que el presente Trabajo de Investigación fue desarrollado por **RENATA CORREA PEÑA**, con el Tema **"DELITO DE DEEPFAKE Y PORNOGRAFÍA INFANTIL GENERADA POR INTELIGENCIA ARTIFICIAL (IA) EN LA LEGISLACIÓN ECUATORIANA"**, bajo mi supervisión.

**DR. PABLO ARTURO POZO CABRERA**

Tutor

**Dedicatoria**

La culminación de mis estudios es un logro que rinde homenaje al amor y apoyo de quienes me rodean:

A mis amigos, por ser el refugio donde reí y lloré, sin miedo a ser juzgada.

A mi padrino Josué, por brindarme paz en los momentos oscuros, una canción y un abrazo a la vez.

A mis mascotas, Tortilla y Mordelón, por acompañarme en noches de desvelo durante mis últimos años de carrera.

A mis queridos abuelos, Piedad, Antonio y Juana, les agradezco de todo corazón por su inquebrantable orgullo y por enseñarme a creer en mí misma. A mi amada mamita Dacha, gracias por ser mi refugio, ese lugar seguro donde siempre encuentro amor y calidez. Y a papi Tuco, te agradezco por inculcarme el invaluable valor del trabajo; tus enseñanzas han sido pilares fundamentales en mi vida y crecimiento.

A mi ángel en el cielo, Angelica Vásquez, por enseñarme sobre la fe y amor.

A mi hermano Julián, por inspirarme a construir un futuro mejor no solo para mi sino para toda nuestra familia.

Finalmente, a las personas más importantes de mi vida

Jasmin Peña, la mujer más maravillosa, hermosa, paciente, fuerte, valiente e increíble que existe, quien me impulso a seguir y a no abandonar mis sueños, quien desde que era una niña me abrazo y con enorme ternura me enseñó a ser una mujer con valor y determinación, ella es mi motor, mi fortaleza, mi amiga, compañera e inspiración en cada aspecto de mi vida.

Renato Correa, el hombre por el cual llevo mi nombre, no solo lo amo, sino que lo respeto y lo admiro enormemente, él fue quien sin titubear apoyo mis sueños, quien me reta a tomar desafíos y quien no tiene miedo a apoyarme y creer en mi hasta cuando yo no logro hacerlo, herede su carácter, su fuerza y su determinación.

Este trabajo y todos los logros que vengan son para ustedes.

***Renata.***

## Agradecimiento

A mis queridos padres,

Esta etapa de mi vida es un reflejo del amor incondicional que siempre me han brindado. Ustedes nunca dudaron de mí; alimentaron mis sueños, secaron mis lágrimas y, con su esfuerzo diario, me ofrecieron la oportunidad de ser la profesional que soy hoy. Este éxito se los debo a ustedes.

Hoy, aunque solo tengo mis ganas de salir adelante, prometo luchar con todas mis fuerzas para darles todo lo que merecen. Los amo con todo mi ser y siempre llevaré su amor en mi corazón y mi trabajo.

**Resumen**

El delito de deepfake y la pornografía infantil generada por inteligencia artificial (IA) en Ecuador presentan serios desafíos legales y éticos. El uso de tecnologías avanzadas para crear imágenes o videos falsos puede afectar gravemente la reputación y la privacidad de las personas, además de facilitar la difusión de contenido sexual no consensuado. La legislación ecuatoriana, aunque ha avanzado en la tipificación de delitos relacionados con la pornografía infantil, enfrenta la dificultad de abordar específicamente los casos de deepfake. En 2021, se introdujeron reformas al Código Orgánico Integral Penal, incorporando penas para la producción y distribución de pornografía infantil. Sin embargo, la rápida evolución de la IA exige una constante actualización legal para abordar adecuadamente estos nuevos delitos. Es fundamental que las autoridades ecuatorianas fortalezcan su marco normativo, implementen medidas de prevención y promuevan la educación sobre el uso responsable de la tecnología, garantizando así la protección de los derechos de las víctimas y la integridad social.

***Palabras Claves:*** *pornografía infantil, deepfake, inteligencia artificial.*

**Abstract**

The crime of deepfakes and child pornography generated by artificial intelligence (AI) in Ecuador presents severe legal and ethical challenges. The use of advanced technologies to create fake images or videos can severely affect an individual's reputation and privacy, as well as facilitate the dissemination of non-consensual sexual content. Although Ecuadorian legislation has made progress in classifying crimes related to child pornography, it struggles to address cases involving deepfakes explicitly. In 2021, reforms were introduced to the Comprehensive Organic Penal Code, incorporating penalties for the production and distribution of child pornography. However, the rapid evolution of AI necessitates constant legal updates to address adequately these new crimes. It is essential for Ecuadorian authorities to strengthen their regulatory framework, implement preventive measures, and promote education on the responsible use of technology, thereby ensuring the protection of victims' rights and social integrity.

***Keywords:*** *child pornography, deepfake, artificial intelligence.*

# Índice

Declaratoria de autoría y responsabilidad ..... II

Certificado del Tutor ..... III

Dedicatoria ..... IV

Agradecimiento ..... V

Resumen ..... VI

*Palabras Claves* ..... VI

Abstract ..... VII

*Keywords* ..... VII

Índice ..... VIII

INTRODUCCIÓN ..... 1

CAPITULO I ..... 3

RIESGOS DEL DESARROLLO DESMEDIDO DE IA. ..... 3

1.1. Introducción a la tecnología de los deepfakes ..... 3

1.1. Orígenes del deepfake ..... 4

1.2. Etimología de deepfakes ..... 6

1.3. Deepfakes en la actualidad ..... 7

1.4 Implicaciones del uso de IA ..... 8

1.5 Implicaciones de los deepfake en ciberseguridad y politica ..... 8

1.6 Implicaciones de los deepfake en propiedad intelectual ..... 9

1.7 Vulnerabilidad de los softwares de IA ante delitos de pornografía infantil. ..... 10

1.8. Privacidad y Protección de datos .....11

1.9. Aspectos relevantes en torno a la seguridad informática ..... 12

1.10. Interacción de contenidos inapropiado generados por medio de IA redes sociales .... 13

1.11. recomendaciones ante la problemática de ciberseguridad ..... 14

CAPITULO II ..... 16

PROBLEMÁTICA LEGAL, SOCIAL Y PSICOLOGICA TORNO A PORNOGRAFÍA INFANTIL CREADA POR DEEPFAKE. ..... 16

2.1. Relación entre la inteligencia artificial y el desarrollo infantil ..... 16

2.2. Pornografía infantil generada por IA como delito informático ..... 17

2.3. Relación entre deepfake y pornografía infantil ..... 18

2.4. Panorama legal en ecuador ante el delito de pornografía infantil ..... 20

2.5. Leyes y organismos capaces de servir como jurisprudencia en casos de pornografía infantil creada por deepfakes ..... 22

2.6. Porque la pornografía elaborada con deepfakes es tan rentable..... 24

2.7. Casos de estudio relevantes ante la temática del Deepfake ..... 25

2.8. Consideraciones éticas y psicológicas en la manipulación de pornografía infantil ..... 27

2.8. Perfil de agresores sexuales consumidores de pornografía infantil: ..... 30

CAPITULO III ..... 32

CIBERDELITOS EN EL PANORAMA INTERNACIONAL ..... 32

3.1. Legislación comparada ante el problema de deepfakes ..... 32

3.2 Implicaciones del uso de IA ..... 32

3.3 Implicaciones de los deepfake en ciberseguridad y politica ..... 33

3.4. Implicaciones de los deepfake en propiedad intelectual ..... 34

CONLCUSIONES: ..... 36

BIBLIOGRAFÍA ..... 37

Anexos ..... 42

# INTRODUCCIÓN

El aumento de delitos informáticos ha incrementado exponencialmente con el paso de los años, tras el desarrollo de nuevas herramientas digitales y la creación de nuevas tecnologías, se ha generado también un desmedido crecimiento en torno a las problemáticas relacionadas a la violación de la seguridad e intimidad de los internautas, en Ecuador cada vez se vuelve más común observar nuevas modalidades delictivas, entre las actividades ilícitas más comunes encontramos, la suplantación de identidad, falsificación de documentos, fraude, robo, acoso, difusión de contenido íntimo, ataques informáticos y revelación de datos personales.

En la era digital, los deepfakes representan una dualidad fascinante y aterradora. Mientras que la tecnología nos maravilla con sus capacidades de manipulación visual sin precedentes, también nos sumerge en un abismo de riesgos, la creciente amenaza de la suplantación de identidad mediante deepfakes trasciende lo ficticio, poniendo en riesgo la integridad y reputación de individuos inocentes, la posibilidad de que rostros y voces sean hábilmente recreados en contextos comprometedores despierta inquietantes preocupaciones sobre la privacidad y la confianza en la era digital.

La frontera entre la realidad y la ficción se desdibuja peligrosamente, con deepfakes capaces de orquestar engaños a una escala global, desde manipulaciones políticas hasta extorsiones personales, la tecnología que permite estas recreaciones digitales desafía la autenticidad de la información que consumimos la sociedad se enfrenta a la tarea apremiante de desarrollar contramedidas efectivas, desde tecnologías de detección avanzadas hasta un mayor entendimiento público sobre los peligros que estos engaños pueden conllevar. En este cruce de innovación y riesgo, la vigilancia y la concienciación son cruciales para salvaguardar la confiabilidad de nuestra realidad digital.

El riesgo de estos “Deepfakes” radica en las amenazas que se generan a la integridad y a la privacidad de cualquier persona que posea información personal o contenido multimedia en la red, el constante uso de estos deepfakes han permitido su desarrollo y sofisticación(García Ull, 2021). Por lo que puede que resulte más complicada su identificación, lo que deja vulnerables a quienes son víctimas de estos mecanismos de falsificación y personificación, en torno a la pornografía infantil debemos mencionar lo riesgosa que resulta la inobservancia e inexistencia de leyes que penalicen el uso de la IA para este tipo de propósitos.

La penalización de estas actividades ilícitas se ven contempladas parcialmente en nuestro Código Orgánico Integral Penal, sin embargo la utilización de la Inteligencia Artificial no ha sido examinada en nuestras normativas, por lo que deja en la indefensión a quienes sufren delitos generados a partir de esta nueva modalidad criminal, este nuevo tipo de delitos configura imágenes, videos y audios creados a partir de inteligencia artificial, debido a su popularidad ya han adquirido nombre en el mundo digital y se les llama Deepfakes, cuyo concepto nace de la creación de contenidos hiperrealistas digitalmente manipulados, cuyo objetivo es representar a personas en situaciones inexistentes, las cuales en el contexto actual han servido para la proliferación de pornografía infantil.

Este estudio no solo procura enmarcar la legislación existente y señalar sus deficiencias, sino que también pretende ver el alcance de esta problemática en varios entornos de la sociedad, la psicología, la educación y la política.

# CAPITULO I

# RIESGOS DEL DESARROLLO DESMEDIDO DE IA.

## 1.1. Introducción a la tecnología de los deepfakes

La delincuencia informática ha experimentado un constante y significativo aumento a nivel global en las últimas décadas, lo cual ha llevado a la proliferación de numerosos actos delictivos que hacen uso indebido y abusivo de la tecnología, a medida que avanzamos en el tiempo, los delitos informáticos han ido evolucionando de manera alarmante, especialmente en lo que respecta a la creación y difusión de pornografía infantil, un fenómeno antiguo que sigue siendo extremadamente preocupante en la actualidad, la era de la informática y la implementación cada vez más amplia de la inteligencia artificial (IA) ha dado lugar a nuevas modalidades de este nuevo tipo delictivo, generando la necesidad imperante de abordarlo desde una perspectiva legal y social sólida.(SEON, 2023)

Es vital comprender que la delincuencia informática no solo afecta a las víctimas directas, como los niños involucrados en la pornografía infantil, sino que también tiene repercusiones mucho más amplias en la sociedad como conjunto, generando un impacto negativo en la seguridad, la privacidad y la confianza en la tecnología, así como en el desarrollo de políticas y medidas eficaces para combatir este tipo de delitos, es por ello que resulta fundamental abordar el delito de deepfake y la pornografía infantil generada por inteligencia artificial desde una perspectiva integral y multidisciplinaria, el fácil acceso a internet y la habilidad de los delincuentes para ocultarse en la red han facilitado la rápida expansión de estos delitos y su capacidad para evadir eficientemente las leyes establecidas, generando así un escenario desafiante y altamente complejo para las autoridades encargadas de combatirla y prevenirla. (World economic forum, 2024)

La proliferación de la IA también ha tenido un impacto extremadamente significativo en la forma en que se cometen y se investigan los delitos informáticos, los avances impresionantes y constantes en esta área han permitido a los delincuentes crear y distribuir contenido ilícito de manera aún más sofisticada y astuta , lo cual ha hecho que sea increíblemente difícil detectar y rastrear por parte de las autoridades competentes, además la IA también ha brindado nuevas oportunidades para el análisis forense digital y la identificación de patrones de comportamiento delictivo, lo que definitivamente puede ayudar a las autoridades en la lucha constante y apremiante contra estos crímenes.

Sin embargo, es importante destacar que este desarrollo tecnológico también supone un desafío adicional y una necesidad de adaptación constante por parte de los encargados de combatir la delincuencia informática, ya que los delincuentes también se actualizan y evolucionan para evitar las tecnologías de seguridad, para abordar de manera eficaz esta problemática cada vez más grave y menos predecible, es necesario que exista una cooperación más estrecha e integral entre los organismos encargados de hacer cumplir la ley, los profesionales del derecho y la sociedad en su conjunto.

La promulgación de leyes aún más estrictas, la asignación de recursos adecuados y la educación insistentemente, clara y concisa sobre los riesgos reales y los efectos negativos de la ciberdelincuencia son elementos fundamentales para combatir esta problemática, es fundamental e imprescindible contar con un marco legal sólido y bien fundamentado que se adapte sumamente rápido a todos los avances tecnológicos, logrando así permitir una persecución verdaderamente efectiva y justa de los delitos informáticos en todas las partes del mundo donde se presenten.

### 1.1.Orígenes del deepfake

Los orígenes de los deepfakes se remontan a principios de la década de 2010, cuando el rápido avance de los algoritmos de aprendizaje automático y la disponibilidad de grandes cantidades de datos sentaron las bases para el desarrollo de esta tecnología.

Se presume que los deepfakes han venido desarrollándose a la par que la industria del cine y las redes sociales, se le atribuye al 2017 como el año de principal difusión de videos y fotos hechos por inteligencia artificial, esto se debe al claro efecto promotor de las redes sociales, se ha establecido es que los deepfakes deben principalmente su fama al sitio web Reddit, en este página se dio el primer avistamiento de la palabra deepfakes y tras su descubrimiento por los internautas, ocasiono una ola de crecimiento de usuario que usaban este término, lo buscaban y compartían.(Arteaga, 2024)

Esta tecnología se mostró inicialmente a través de la creación de videos pornográficos falsos de celebridades, lo que generó inquietudes sobre su potencial de mal uso y manipulación.

La tecnología subyacente detrás de los deepfakes se basa en el aprendizaje profundo, un subconjunto de la inteligencia artificial que utiliza redes neuronales para analizar y aprender de

grandes conjuntos de datos, al alimentar estas redes en una gran cantidad de imágenes y videos, los desarrolladores han podido crear algoritmos que pueden manipular y generar contenido falso altamente realista.

Esto ha dado lugar a una amplia gama de aplicaciones, desde entretenimiento inofensivo hasta campañas de desinformación maliciosas, a medida que los deepfakes continúan evolucionando, es crucial comprender sus orígenes y desarrollo para abordar de manera efectiva los desafíos éticos y de seguridad que plantean.

Como planteamos anteriormente el primer uso de la tecnología Deepfake se produjo en la plataforma de redes sociales Reddit por parte de un usuario anónimo. Reddit cuenta con más de un millón de subreddits más pequeños dedicados a diferentes temas, formando comunidades para compartir y debatir contenido, en noviembre de 2017, un usuario llamado u/deepfakes creó una comunidad llamada r/deepfakes, donde comenzaron a circular los primeros vídeos de intercambio de caras utilizando el algoritmo Deepfake. (García Ull, 2021)

Al principio, la comunidad de Reddit ayudó a "deepfakes" a mejorar las creaciones, incluso creando un subforo para agrupar las contribuciones. Sin embargo, ese subforo fue cerrado el 7 de febrero de 2018 por violar las reglas de Reddit sobre intercambio sexual de imágenes de personas sin su consentimiento, comúnmente conocido como "pornografía vengativa". Sin embargo, en el cierre del subforo los moderadores les aclararon que "deepfakes" alentaban la sexpoinaje de las personas famosas y este tipo de comportamientos no es tolerado.

Por otro lado, el sitio Pornhub declaró que baneaba el contenido deepfake de su plataforma por violar sus términos de servicio, es evidente que una vez revelado al mundo el poder que tenían los "deepfakes", era inminente que se diera a primar su uso en favor de la pornografía vengativa. De ahí se desprenden los verdaderos peligros: manipulación, violación de condiciones de uso de las plataformas, pornografía no consensuada y mucho más.

Un video que tuvo gran popularidad en redes e incluso una amplia cobertura mediática fue en torno al ex presidente del partido demócrata Barack Obama, este video se tituló "President Obama Shocks The Nation With UFO Disclosure",

Este video género controversia debido a que el mandatario se exponía anunciando la noticia sobre cómo se iba a destapar la generación de informes secretos sobre platillos voladores, la

empresa Binary Pulse Studios fue la encargada de este contenido que se volvió tendencia, lo que los llevo a un crecimiento que a nivel profesional consolidándonos como negocio y permitiendo que se ofreciera un servicio comercial de creación de deepfakes

Recordemos que en 2008 aún no se había inventado el término “deepfakes”, y la denominación utilizada en el vídeo resulta "compelling simulations", simulaciones convincentes, sin embargo, aunque no lo sospechásemos se trataba del primer Obama deepfake en la historia.(Botha & Pieterse, 2020)

Esta tecnología ya va desarrollándose desde hace tiempo, Project InInterpersonal Dynamics, empezó la construcción de una serie de computadoras a finales de los años cincuenta para que interpretaran y respondieran a las entradas verbales reforzando a las personas que hacían que el ordenador funcionara adecuadamente (Inglada Galiana et al., 2024)

Lo que se sabemos con seguridad es que estos nuevos mecanismos de creación audiovisual en su inicio fueron destinados a generar entretenimiento y asombro en los visitantes de internet, pero con el tiempo nos hemos percatado que también pueden generar controversia y caos debido a la facilidad de su uso y malversación.

### 1.2. Etimología de deepfakes

Los análisis etimológicos de palabras de reciente creación suelen resultar minúsculos, y menos cuando se trata de anglicismos. de ahí que hayamos apreciado que algunas de las fuentes consultadas para este trabajo prestaran especial atención a la libre interpretación de los elementos que componen la palabra deepfake.

En inglés, a 'deep' se le atribuye el significado de "inmersión completa de la información", lo cual no se corresponde con el sentido originario de la palabra ni con su evolución lingüística. Según las completas bases de datos de inglés antiguo, la voz deep se encuentra ya registrada en los siglos VIII y X con el valor de "profundo" y ha conservado idéntico sentido hasta la actualidad, apareciendo desde siempre en expresiones como "the sea is deep" o "abundant". (Torres, 2020)

En el ámbito de los deepfakes, el significado de la voz cambia ligeramente, respecto a fake, designa cualquier cosa que sea "falsa" o "falsificación", tanto en forma como en contenido, en el contexto que nos ocupa, la voz fake se utiliza ya para designar la manipulación digital de la

realidad, habitualmente para imponer un lugar, un tiempo o un personaje que "no estaban allí. (Torres, 2020)

0tra interpretación puede provenir de la mezcla del Deep learning, o aprendizaje profundo, una nueva forma de inteligencia artificial que, al contrario que el machine learning o aprendizaje automático tradicional, utiliza una arquitectura de procesado basado en el cerebro humano mostrando cierta analogía al funcionamiento estructural del cerebro, basa su funcionamiento en reducir notablemente la complejidad y el tiempo necesario para resolver cierto tipo de problemas, dicho de una forma muy coloquial y simplificada, podría describirse como la lucha a través de intentos y errores del sistema y su idoneidad progresa y retrocede avanzando lentamente.

### 1.3. Deepfakes en la actualidad

En la actualidad, estos vídeos son fáciles de crear y se han convertido en representaciones extremadamente convincentes y difíciles de reconocer de personas genuinas, haciendo o diciendo cosas que en realidad nunca hicieron o dijeron, a medida que avanza la tecnología, aumentará la capacidad de crear vídeos falsos pero creíbles dirigidos a celebridades, políticos y gobiernos en general, las implicaciones de la tecnología Deepfake pueden ser perjudiciales para la sociedad o para la reputación e identidad individual.

Se han visto múltiples casos de videos Deepfake, la mayoría con propósitos únicamente de entretenimiento, no obstante, algunos ejemplos clave de estos videos ilustran el potencial poder de los videos como herramienta para llevar a cabo operaciones políticas o psicológicas, un ejemplo es un video en el que aparece el presidente estadounidense Donald Trump, instando a Bélgica a retirarse del acuerdo climático de París, durante el video, el presidente Trump hace la siguiente declaración: “Como saben, tuve el coraje de retirarme del acuerdo de París, y ustedes también deberían hacerlo”. El video fue publicado por un partido político belga tanto en Twitter como en Facebook, pero finalmente fue desacreditado por Lead Stories. (Véliz & Chavez, 2024)

En efecto, ha sido sin duda la constante irrupción de programas cada vez más potentes, eficientes y accesibles en términos de precios el principal aliciente para que su desarrollo e incremento se haya disparado en los últimos años, pero tal y como planteábamos en el inicio de este trabajo, el origen de los Deepfakes se encuentra en el estar subidos en hombros de gigantes,

porque es el aprendizaje profundo quien hace posible las increíbles innovaciones tecnológicas que estamos viviendo en los últimos años

Así como el reconocimiento de voz o texto, las recomendaciones productivas de plataforma a usuarios, o las recomendaciones productivas entre los propios contenidos, y ha sido esta área del mundo difícil por antonomasia la responsable a su vez de la revolucionaria irrupción de los Deepfakes, para entenderlo es necesario remontarse a la década de los cincuenta del siglo pasado.

### 1.4 Implicaciones del uso de IA

Algunas de las implicaciones que debemos tomar en cuenta son la privacidad y protección de datos, la inteligencia artificial suele necesitar grandes cantidades de datos para funcionar de manera efectiva, por lo que requiere la recopilación de datos personales para entrenar algoritmos puede poner en riesgo la privacidad si no se gestiona adecuadamente, es por eso que la transparencia es primordial ya que los ciudadanos tienen derecho a saber cómo se recopilan y utilizan sus datos.

Las políticas y regulaciones deben garantizar que las personas tengan acceso a esta información y puedan ejercer control sobre sus datos, así se garantizará la seguridad de datos y la protección de datos personales contra accesos no autorizados es fundamental, así será posible evitar las violaciones de seguridad pueden tener consecuencias graves para los individuos.

### 1.5 Implicaciones de los deepfake en ciberseguridad y politica

El delito de deepfake y la pornografía infantil generada por inteligencia artificial (IA) es un tema de relevancia en la sociedad contemporánea, en este sentido es importante analizar cómo la legislación ecuatoriana aborda esta problemática y qué medidas se han implementado para combatirla.

Así como las implicaciones legales y éticas que conlleva el uso de IA, la tecnología en nuestras manos se ha convertido en un arma de doble filo, y es un hecho debido que seguramente que al menos una vez hemos visto un video falso o una imagen manipulada y cada vez es más común en la era tecnológica actual, la proliferación de deepfakes y pornografía generada por IA plantea un desafío sin precedentes para la sociedad y la legislación ecuatoriana.

Es crucial comprender el alcance y las implicaciones de este fenómeno en el contexto local cada día se vuelve más repetitiva la frase "La tecnología cada día nos sorprende más". y es que a todos nos han llegado vídeos de deepfakes en los que se mezclan los rostros de políticos con otros cuerpos presentando discursos todavía más innovadores y creíbles que los propios. (Véliz & Chavez, 2024)

John K. Holum, antiguo subsecretario de la Marina de los Estados Unidos, afirmó que "La información es poder, hoy el control de información significa el control de su distribución, los EE. UU y el resto del mundo se encuentra en un encrucijada", si tomamos en cuenta este argumento en cuanto a la regulación de los delitos informáticos y la protección de los derechos de los niños y niñas, enfrentamos un enorme desafío, el avance tecnológico ha facilitado la creación y difusión de contenido que atenta contra la integridad de menores de edad y así como la información genera poder, su uso incorrecto genera amenazas contra la dignidad humana. (Fitzgerald, 2023)

### 1.6 Implicaciones de los deepfake en propiedad intelectual

Cuando hablamos de información, debemos referirnos a la digital que a lo largo de los años ha sido asimilada por el ser humano, pero que hoy se transformó en un conjunto de documentos o datos para tomar anotaciones y que posteriormente serán reemplazados por carpetas y cajas de almacenamiento virtual suplementarias para repartir y generar respuestas rápidas debido a la acumulación de información.

Se puede afirmar que los más interesados en la propiedad intelectual y los derechos de autor son, mayormente, aquellos que se encuentran en entornos profesionales, como artistas de diversas áreas, así como jueces, notarios y abogados. Estos últimos utilizan documentos fotocopiables como notación para establecer "propiedad" sobre el texto o el diseño original. (Arias et al., 2022)

Además, estos hechos pueden representar un inconveniente para quienes hacen uso recurrente de la inteligencia artificial en ambientes laborales. Esto se debe a que la mayoría de las barreras en la creación de documentos y fabricación de datos han sido superadas gracias al desarrollo abrumador de las denominadas Nuevas Tecnologías de la Información. (Arias et al., 2022) -

Resulta intrínseco mencionar la íntima relación de la IA con la propiedad intelectual, este planteamiento es necesario debido a que en términos legales y referentes a la creación de

pornografía infantil pueden verse ligada la culpabilidad de los “autores” de estas infracciones con el uso de herramientas de inteligencia artificial.

En los Estados Unidos y la Unión Europea, la propiedad de las creaciones producidas por inteligencias artificiales y computadoras se asigna al creador material o programador que ejerce control sobre ellas

Por otro lado, la normativa vigente en países como China, India y Rusia establece que, en ausencia de un contrato en sentido contrario, la titularidad recae en el primer inventor.

Recientemente, los sistemas legales anglosajón y europeo han comenzado a enfocarse en otorgar la propiedad a la persona natural que desarrolló la herramienta de inteligencia artificial. Mientras tanto, las legislaciones de China, India y Rusia destacan la importancia de establecer un acuerdo contractual entre las partes, ya sea de manera exclusiva o no, incluyendo aspectos como contraprestaciones u otras formas compensatorias relacionadas con las obras producidas por la inteligencia artificial (Osorio & Enerieth, 2020)

Si la atribución de la titularidad se lleva a cabo de manera errónea, se puede generar un daño potencialmente gigantesco tanto a nivel económico como incluso a nivel de explotación, frenando al mercado para creaciones que contienen alto contenido de innovación, a través de la exclusividad o dejando de obtener beneficios de creaciones innovadoras y distinguidas por la clientela respecto de los competidores, prestigiando a su titular respecto a los competidores, entre otros aspectos. (Lopez Sanchez, 2017)

También es posible que la atribución sea errónea en el sentido de atribuir cada obra generada por un proceso de IA a un autor distinto, en cuyo caso cada autor estaría en condiciones de desplegar la totalidad de los derechos propios de su condición, con lo que se corre el riesgo de sufrir acciones de infracción de derechos de terceros por carecer de la licencia necesaria para explotar legalmente la obra. (Lopez Sanchez, 2017)

### 1.7 Vulnerabilidad de los softwares de IA ante delitos de pornografía infantil.

Las vulnerabilidades en el mundo digital no son sinónimos de que la integridad de un sistema pueda verse totalmente comprometido, el concepto corresponde mejor el concepto de exploit (hacer uso de los puntos de vulnerabilidad), a mayor número de líneas de código, mayores puntos

débiles hay en el mismo, dichas vulnerabilidades pueden tener a su vez, iniciales o finales, lo que corresponderían a ser puntos de desarrollo en que una vulnerabilidad puede ser producida o no encontrada, este exploit en defecto puede falsificar solicitudes entre sitios o incluso configuraciones de seguridad erróneas.

Por otro lado, las líneas de código del software actual son exorbitantemente grandes y complejas, el software tiene actualmente un número creciente de características y de prestaciones, lo que requiere un mayor número de líneas de código, esto hace cada vez más difícil verificar su seguridad, y aumenta el número, su tamaño y la posición espacial de los posibles puntos de entrada que puedan ser descubiertos por un atacante.

El software y hardware que utilizan es muy variado y hay dispositivos novedosos que no tienen testados los suficientes controles de seguridad, todavía soportan tecnologías antiguas que no son compatibles con las nuevas, no se adaptan a las nuevas amenazas (malware, ciberdelincuencia), por lo que después con 18 años de funciones sigue sin conocerse la seguridad de muchos dispositivos que entra en juego durante el proceso de análisis y valoración.

En primer lugar, indicar que un sistema informático sirve para tratar y proteger la información, por lo que la confidencialidad, la integridad y la disponibilidad de la información de los menores son los pilares básicos sobre los que se asienta la seguridad de los sistemas informáticos.

### 1.8. Privacidad y Protección de datos

La protección de la privacidad y de datos de menores implica diversos desafíos debido a la velocidad del avance tecnológico, se deben dotar tanto de las herramientas necesarias para que puedan hacer un uso seguro, respetuoso y creativo de sus derechos en un mundo digital como de controlar los riesgos. es preciso que las autoridades tengan en cuenta las capacidades y necesidades de menores a la hora de abordar la protección de la privacidad.

Cuando hablamos de protección de datos no podemos excluir a los adultos quienes en diversas situaciones en las que son responsables de menores tienen un mayor desconocimiento de los alcances de la tecnología en sus vidas, por lo que se ven menos dotadas herramientas para tomar decisiones informadas, la dificultad para comprender cómo funciona una IA (inteligencia artificial) puede ser talvez la principal deficiencia al momento de proteger datos.

Estos sistemas se configuran a partir de datos personales (imágenes, audios, etc.), que por un lado los habilita para la acción, lo que puede resultar muy práctico e incluso útil en el caso de los asistentes virtuales para con discapacidad, de todas maneras, pueden suponer un riesgo adicional para los menores y ejercer un impacto en sus derechos, en tanto que se están transformando sus datos y con ello teniendo un mayor poder sobre la toma de decisiones.

### 1.9. Aspectos relevantes en torno a la seguridad informática

No son pocos los aspectos que se deban tomar en cuenta cuando hablamos respecto a la seguridad informática, esto es un tema necesario a tratar debido a que, si bien los deepfakes tienen sus implicaciones tecnológicas, debemos tener un panorama mucho más amplio al referirnos sobre la seguridad informática

Por ejemplo, el termino Consentimiento Informado, es valioso para la seguridad de los usuarios, las personas deben dar su consentimiento informado antes de que sus datos sean utilizados por sistemas de inteligencia artificial. esto implica entender cómo se utilizarán los datos y qué decisiones se tomarán en función de ellos, para que no se corran riegos innecesarios se debe aplicar la frase “leer las letras pequeñas” cualquier acuerdo en los entornos virtuales tiene el mismo peso que el de el de un acuerdo en forma de contrato, ya que puede eximir o responsabilizar a una persona natural o jurídica por hacer uso indebido de datos, no se trata de aceptar sin cuestionamientos cualquier tipo de términos y condiciones, sino que también implica aprender a racionalizar, cualquier tipo de acuerdos y sus posibles implicaciones.

Pese a las enormes herramientas que fomentan igualdad y respeto las herramientas tecnológicas como las redes sociales, es inevitable percibir la existencia de discriminación, no se trata de una discriminación “convencional” sino de una que se presenta por la forma en la que fueron establecidos los mecanismos de IA, los algoritmos de inteligencia artificial pueden reflejar y amplificar sesgos presentes en los datos con los que fueron entrenados, esto puede llevar a decisiones discriminatorias en áreas como contratación, crédito y justicia penal, al tratarse de algoritmos, la carencia de humanidad y raciocinio es evidente ante el enorme vacío de emociones que representan las decisiones de la inteligencia artificial.

Otro aspecto que se relaciona con la seguridad informática es la autonomía y toma de decisiones, como establecimos con anterioridad en el consentimiento informado , el tomar las medidas correctas al tratarse de la seguridad de nuestros datos es primordial , sin embargo al hablar de toma de decisiones en este punto nos referimos a una "autonomía" automatizadas por parte de sistemas de inteligencia artificial, que puede afectar la autonomía personal, es significativo garantizar que los individuos tengan la capacidad de revisar y apelar decisiones importantes que les afecten, los algoritmos de IA no gestionan un discernimiento entre lo ético y lo inmoral, por lo que si no está programado en su algoritmo no podrá ser evitado o en otro casos ejecutado.

Habiendo establecido conceptos como la autonomía y el consentimiento, debemos dar paso a la responsabilidad y rendición de cuentas, esta será la encargada de determinar quién es responsable cuando un sistema de inteligencia artificial causa daño o comete un error.

La responsabilidad puede recaer en los desarrolladores, implementadores o en los sistemas mismos, pese a que la IA no es un sujeto de derechos, esto no significa que no haya la posibilidad de penalizar conductas irresponsables generadas por esta tecnología.

Para ser más claros, la ley siempre procurará la protección de los derechos humanos y la dignidad, la implementación de inteligencia artificial debe respetar la dignidad humana y no utilizarse de manera que degrade o explote a los individuos, por ello es imperativo regular y crear políticas; los legisladores deben desarrollar normativas que equilibren la innovación en inteligencia artificial con la protección de los derechos personales (Gómez & Gómez, 2024).

Dado que la inteligencia artificial está en constante evolución, las normativas y regulaciones deben ser flexibles y adaptativas para abordar nuevas cuestiones y desafíos que surjan.

La interacción entre inteligencia artificial y derechos personales es un campo en rápida evolución que requiere una reflexión constante y un enfoque equilibrado para garantizar que los avances tecnológicos se utilicen de manera que respeten y protejan los derechos fundamentales de las personas . (Gómez & Gómez, 2024) –

### 1.10. Interacción de contenidos inapropiado generados por medio de IA redes sociales

La Inteligencia artificial ya logra detectar rostros y sonidos asociados con asaltos sexuales, suicidio y violencia, para bloquear contenidos a muchos en muchas plataformas, Facebook por

ejemplo utiliza un sistema de detección de hash (detección de contenidos nocivos por sus huellas binarias) para identificar imágenes cuyos pesos se encuentren en contenidos relativos y cercanos, si bien una cierta variante ha violado patentes, el sistema utiliza una sencilla regla de la incursión en la que el porcentaje de reciprocidad entre las imágenes es alto, esto tomando en cuenta la sensibilidad y cierto nivel humorístico e inteligencia del crimen que se perciba dentro del contenido, los patrones más habituales o frecuentes tienen una especie de "look de crimen" al respecto, sin embargo más allá de la calidad de los sistemas de vigilancia respecto de contenido violento, continua siendo un problema la confrontación de contenido infantil y adolescente ya que semejantes imágenes se mantienen circulando y a los menores no los suministra de la protección necesaria para que protejan sus datos, salvo que inevitablemente se trate de imágenes trágicas, información debida e inmediata percibida por el algoritmo (Pulido, 2023)

American Academy of Pediatrics considera que los chicos deberían poder contar con contenidos adaptados a su época en los que no aparezcan actos y consecuencias fatales , que dañen su psiquis y los conmocionen a tal grado que puedan generar traumas, es necesario abordar este tipo de opiniones debido a la existencia de sistemas de protección (filtros parentales) los cuales deben normalizarse y difundirse, ya que estos sistemas abrigan a la esperanza de que, seamos o no conscientes del riesgo del uso indebido de redes sociales, habrá alguien limpiando los rincones de la caótica jungla que es la red.

### 1.11. recomendaciones ante la problemática de ciberseguridad

Resulta absolutamente esencial concienciar y educar profundamente a todas las personas sobre las medidas de seguridad informática que deben tomar de manera constante y proactiva para protegerse a sí mismas y a sus familias, esto incluye entre otras cosas, el uso de contraseñas altamente seguras y complejas, la protección con diversas capas de seguridad de su información personal cada vez que se encuentre en línea, el no exponer de manera imprudente datos y fotografías que puedan ser utilizadas de manera inapropiada, y el estar siempre alerta a posibles amenazas cibernéticas, así como también alentar la prudencia cautelosa al descargar cualquier archivo o hacer clic en enlaces sospechosos en cualquier plataforma digital y a denunciar cualquier actividad sospechosa o delictiva.

Asimismo, es necesario fomentar de manera continua y sistemática la educación en el uso ético y responsable de la tecnología desde una edad temprana, para que las futuras generaciones estén debidamente preparadas para enfrentar los enormes desafíos que implica la delincuencia informática en todos sus ámbitos y consecuencias.

En resumen, la delincuencia informática es un desafío verdaderamente creciente y altamente peligroso que no puede ser ni debe ser subestimado de ninguna manera (Autor, año). Su impacto abarca tanto a nivel individual como a nivel colectivo y, por lo tanto, requiere un enfoque multidimensional, integral y completamente involucrado que necesariamente debe involucrar activamente a todos los sectores de la sociedad que puedan verse afectados por este problema.

Solo a través de una combinación precisa y adecuada de medidas legales sólidas, educativas permanentes y en constante evolución, y tecnologías vanguardistas y contundentes, podremos hacer frente y controlar de manera eficaz esta problemática gravísima y atacarla en todas sus dimensiones y complejidades.

Esto nos permitirá proteger a nuestras comunidades locales y también a nivel global de los peligros cada vez más poderosos y graves de la era digital, en la cual todos nos encontramos. Nuestro mundo es solo un gran escenario virtual, donde la colaboración abierta y la cooperación constante de todos los actores clave involucrados son fundamentales, esenciales y prioritarias para lograr un avance verdaderamente significativo en la lucha implacable y sin descanso contra esta problemática .

Además, es crucial garantizar un entorno verdaderamente seguro y confiable en todo el fascinante e inmenso mundo digital. Solo a través de una colaboración y cooperación constante podemos trabajar juntos para abordar esta creciente amenaza y proteger a nuestros ciudadanos.

Con la determinación y el compromiso adecuados, podemos enfrentar con éxito los retos de la delincuencia informática y construir un futuro digital más seguro para todos (Pailiacho & Amancha, 2024)

# CAPITULO II

# PROBLEMÁTICA LEGAL, SOCIAL Y PSICOLOGICA TORNO A PORNOGRAFÍA INFANTIL CREADA POR DEEPFAKE.

## 2.1. Relación entre la inteligencia artificial y el desarrollo infantil

El auge de la inteligencia artificial (IA) ha traído consigo avances significativos en varios aspectos de nuestras vidas, incluida la educación y el entretenimiento para niños, a medida que la tecnología de IA se integra cada vez más en nuestra vida diaria, es importante reconocer los riesgos y desafíos potenciales que plantea para los menores.

Es necesario abordar de forma objetiva la exploración de la compleja relación entre la IA y los niños, examinando los riesgos potenciales, las consideraciones éticas y las implicaciones para su desarrollo y seguridad.

Indiscutiblemente existe un enorme  impacto de la IA en el uso de todo tipo tecnologías, sin embargo quienes abrazan esta nueva tecnología como algo propio de su generación son los menores de edad, por lo mismo es lógico concluir que pueden ser los mas afectados o beneficiados en este tema, ya que se pueden nutrir de los enormes beneficios de la inteligencia artificial pero también es necesario establecer y entender que se encuentran en una etapa vulnerable de sus vidas y son susceptibles a la influencia de esta tecnología, con el uso cada vez mayor de dispositivos y plataformas impulsados por IA, los niños están expuestos a una amplia gama de contenidos e interacciones, lo que genera inquietudes sobre su seguridad, privacidad , e incluso sobre su desarrollo cognitivo, al profundizar en los principios fundamentales de la IA y sus aplicaciones en el contexto de los niños, podemos comprender mejor los posibles riesgos y desafíos que deben abordarse.

Es esencial considerar las implicaciones éticas del uso de la IA para interactuar con los niños, así como las posibles consecuencias para su bienestar emocional y social, al examinar los marcos y directrices éticos relevantes para la IA y los niños, podemos identificar las medidas necesarias para garantizar el uso responsable y beneficioso de la IA en sus vidas, a través de esta exploración, podemos sentar las bases para las secciones posteriores de este ensayo, que profundizarán en los riesgos específicos y las estrategias para mitigar los impactos negativos de la IA en los menores.

Los niños y niñas se ven rodeados de contenido artificial, el cual puede provocar una notoria disociación de la realidad , así como una alterada percepción del entorno en el que viven, el uso de inteligencia artificial no solo puede ser una herramienta que facilita la creación de todo tipo de contenidos, sino que también puede ser un paso al estancamiento creativo y el desarrollo de actividades lógicas, cognitivas, sociales y artísticas, por lo que replantearnos la libertad otorgada a niños y niñas en el uso de tecnologías no debería ser un tema que se deje fuera de discusión.

Es fundamental que los padres y cuidadores supervisen el tipo de contenido al que están expuestos los menores, ya que la inteligencia artificial puede facilitar el acceso a material inapropiado, pero no solo es un riego por el potencial consumo de información indebida, sino también por la influencia que puede tener en su desarrollo emocional y psicológico y por el riego a que niños, niñas y adolescentes sean víctimas de esta tecnología, que expone sus datos para crear contenido pornográfico, exponiéndolos a situaciones peligrosas o manipulación por parte de terceros.

## 2.2. Pornografía infantil generada por IA como delito informático

El crimen de pornografía infantil en el ámbito de los medios de comunicación es un fenómeno difícil de detectar y abordar, ya que las prácticas suelen ser minimizadas, ocultas o negadas por los adultos responsables de las víctimas, este tipo de abuso infantil refleja hechos que se han producido con asombrosa frecuencia durante la crianza de muchos niños y adolescentes, por lo que es esencial abordar este problema que representa el lado oscuro de internet y reconocer la existencia de este fenómeno de manera legal.

El impacto negativo de la modernización de las comunicaciones y el avance de las nuevas tecnologías se evidencia por el aumento de fraudes y delitos informáticos, todo está disponible para ser alquilado o comprado, lo que significa que ya no es necesario ser un experto para cometer robos, controlar o violar sistemas, además la crisis mundial actual facilita la participación de personas o grupos interesados en cometer estos delitos en línea.

Es de conocimiento público que los delitos informáticos se han vuelto cada vez más comunes, especialmente en esta nueva era digital en la que la gran mayoría de las personas almacena su información personal en dispositivos electrónicos, lo preocupante es la facilidad con la que se

pueden vulnerar la seguridad de celulares, computadoras y conexiones a internet, invadiendo así la privacidad de quienes hacen uso de dichos dispositivos. (Noguera et al., 2023)

En 2020, la necesidad de estar conectados a internet y redes sociales aumentó significativamente debido a la pandemia de covid-19, lo que ha llevado a un mayor uso de dispositivos electrónicos para conversar con amigos y familiares, realizar actividades desde casa y cumplir con responsabilidades laborales y académicas. (Noguera et al., 2023)

La pandemia ha exacerbado gravemente la situación actual, y uno de los problemas que ha visto un aumento notable es la pornografía infantil, aunque la pornografía y, en particular, la pornografía infantil no son fenómenos nuevos, la proliferación de las redes sociales en los últimos años ha intensificado este problema, la facilidad con la que los pedófilos pueden acceder a los menores y la falta de supervisión parental en muchos hogares han contribuido al crecimiento de este problema, además la consolidación del aprendizaje en línea y el uso extendido de redes sociales han amplificado estos riesgos.

A lo largo del último siglo, las profundas transformaciones en el ámbito económico, motivadas por la globalización, la apertura de mercados y la evolución creciente de nuevas estrategias delictivas, han dado lugar a nuevos fenómenos criminales, estos fenómenos se originan en el entorno mediático y han conducido a nuevas formas de interacción social y, en consecuencia, a la aparición de delitos innovadores, esta evolución ha generado la necesidad de reforzar los mecanismos de control social y desarrollar métodos para identificar, sancionar y prevenir estos comportamientos, especialmente en el contexto digital.

Algunos de los factores clave relacionados con la pornografía infantil como una forma de desviación social en la era moderna, este problema se presenta como una de las manifestaciones más oscuras de internet, que demanda estrategias de prevención no solo desde el ámbito legal, sino también desde otras disciplinas auxiliares, para mitigar tanto los efectos directos como los secundarios de este comportamiento en el núcleo social.

### 2.3. Relación entre deepfake y pornografía infantil

El delito de deepfake y pornografía infantil generada por inteligencia artificial (IA) en la legislación ecuatoriana es un tema que preocupa a las autoridades y legisladores, ya que representa

un desafío para la protección de los menores de edad y la privacidad de las personas, su relevancia radica en los avances de la tecnología y la necesidad de actualizar el marco legal para enfrentar esta problemática en este sentido, es importante analizar cómo la legislación ecuatoriana aborda esta problemática y qué medidas se han tomado para combatir estas violaciones, así como identificar posibles lagunas legales que requieran ser cubiertas, a fin de garantizar una protección efectiva y actualizada para la sociedad ecuatoriana. (Terol, 2023)

Actualmente, el uso de la inteligencia artificial para delitos como el deepfake representa un desafío para las leyes y la protección de los derechos de los niños y niñas (Autor, año). En el siguiente estudio, abordaremos distintos temas relacionados con la seguridad y la protección de la dignidad de niños, niñas y adolescentes, quienes pueden llegar a ser víctimas en este nuevo sistema delictivo.

El uso específico de inteligencia artificial (IA) conlleva, al menos en principio, un acto de creación. Lamentablemente, los delincuentes cibernéticos han tomado esta herramienta para una nueva modalidad de creación de pornografía infantil.

Esto se debe a que genera menos riesgo para los delincuentes, al no tratarse de tráfico humano, que está regulado y penalizado, con el uso de IA, se puede crear contenido que aparenta ser real, pero en realidad es generado de manera artificial, lo que dificulta su detección y persecución, además, esto representa un desafío para las autoridades encargadas de combatir este tipo de delitos (Granados Ferreira, 2022)

En este sentido, es importante analizar la legislación ecuatoriana en torno a esta problemática y proponer soluciones efectivas que permitan prevenir y sancionar el uso indebido de la IA para la generación de pornografía infantil.

La literatura ecuatoriana no abarca el tema de la Inteligencia Artificial en relación con la pornografía infantil sin embargo textos como "La ruta de protección de derechos de niñas, niños y adolescentes del distrito metropolitano de Quito", trata el tema haciendo referencia a como las personas adultas deben proteger a los menores, y es deber del estado precautelar mediante el estudio de nuevas modalidades del delito, el uso abusivo de dispositivos tecnológicos que atenten contra sus derechos a la privacidad, protección, imagen y honor, a medida que se desarrolle esta investigación se recopilaran datos de doctrina ecuatoriana referente a este tema.(Vestri, 2021)

## 2.4. Panorama legal en ecuador ante el delito de pornografía infantil

Cuando nos referimos a la pornografía infantil por medios digitales, nos enfrentamos a un desafío inmenso que se ha generado debido a las estrategias criminales, de organizaciones o personas que explotan este mercado sin importar la dignidad de niños niñas y adolescentes, el riesgo radica en el desconocimiento de las normativas y en que tecnológicamente se están dando pasos agigantados que rebasan la velocidad de promulgación de leyes.

El método y uso de organizaciones criminales o pedófilos es mediante la creación de escenarios simulados por inteligencia artificial, que además integran dentro de este contenido fotos de menores de edad, respecto a esta modalidad podemos racionalizar que existe un delito que se debe al ataque directo contra la integridad y la personalidad de menores, el problema está en que los delincuentes son mucho más sofisticados que la misma ley, es así que han ideado una estrategias que puede entorpecer la penalización de estas acciones.

Este nuevo tipo de tácticas criminales consiste en la creación de contenido audiovisual pornográfico en el que efectivamente se puede observar a niños niñas y adolescentes, sin embargo la problemática radica en que las imágenes de niños niñas y adolescentes también son creadas con inteligencia artificial, es decir que no hay una persona real detrás del rostro que se está utilizando para difundir o crear estas imágenes.

Otra forma de accionar es mediante la inteligencia artificial para crear rostros de niños niñas y adolescentes, hechos a base de rostros de adultos, los cuales si podrían consensuar o acordar vender su imagen para este tipo de fines, lo que lo volvería un negocio en donde existe un contrato o consentimiento de creación y distribución de material fotográfico y multimedia.

La ley exhibe a la pornografía infantil como un delito que puede tener como pena privativa de libertad de 10 a 13 años, la ambigüedad del artículo 104 del código orgánico integral penal no es del todo negativa, esto debido a que el mismo habla de la compra, porte, posesión, transmisión, almacenamiento, publicidad, exporte, importe y venta de material pornográfico, por lo que esto constituiría a cualquier tipo de contenido incluso que el que es generado por IA que tengan las características que podrían ser consideradas de material pornográfico.

Incluso si los niños y niñas no se encuentran en un riesgo físico por la producción de este material, el simple hecho de qué se ocupen niños niñas y adolescentes para promover prácticas

sexuales deplorables, debe ser penalizado por la ley que no fue clara al denotar la diferencia entre pornografía producida con personas reales y pornografía producida por inteligencia artificial.

Ahora si nos referimos al artículo 103 del código orgánico integral penal que habla concretamente de la pornografía infantil, encontraremos que el artículo establece que la persona que transmita, edite o reproduzca materiales visuales, informáticos y electrónicos o de cualquier soporte físico o formato que contenga presentación visual de desnudez o simulando la participación de niñas o niños o adolescentes en una actividad sexual deberá ser sancionado de 13 a 16 años de cárcel, en este artículo podemos ver muchísima más organización de la ley ante estas acciones, la misma que no diferencia que solamente se pueda establecer este delito si los menores han sido expuestos a situaciones físicas, sino que habla de la creación de estos videos o imágenes que al ser realizados mediante IA también involucran directamente a la persona que edite materiales informáticos o electrónicos, esclareciendo que efectivamente tendrá culpabilidad por incurrir en un delito de pornografía infantil. (ASAMBLEA NACIONAL, 2014)

La interpretación legal que se ha hecho y las reformas realizadas en el código orgánico integral penal ampliando los términos referentes a la pornografía utilizando niñas niños o adolescentes es correcta, estos delitos no afectan solamente a una víctima directa sino que indirectamente provocan un resquebrajamiento social en donde todos los niños niñas y adolescentes están expuestos a ser víctimas potenciales, de pedófilos y pederastas que estén consumiendo distribuyendo o ideando estrategias para poder continuar con estas prácticas criminales.

Pese a que nuestra legislación aborda los temas de protección de niños, niñas y adolescentes, el impacto directo que implican los deepfakes no está completamente regulado (Autor, año). No obstante, otros textos referentes a la legislación ecuatoriana también abordan el tema de la seguridad y los derechos concernientes a menores de edad.

Entre los mismos, encontramos que la Constitución ecuatoriana establece derechos fundamentales para los menores, en su artículo 44, se asegura el derecho de los niños, niñas y adolescentes a la protección y a la garantía de sus derechos, lo que podría incluir la protección frente a contenidos digitales perjudiciales como los deepfakes.

Es primordial establecer que la Constitución abarca los derechos de todos los ciudadanos, y aunque la raíz de esta investigación se centra en los delitos correspondientes a niños, niñas y

adolescentes, no podemos desentendernos del enorme riesgo al que se exponen todos los ciudadanos, sin importar edad, sexo, raza, etc. (Toro Hernandez, 2024)

Debemos abordar principalmente lo que establece el Código de la Niñez y Adolescencia, este establece la importancia en términos de la protección de los derechos fundamentales de los menores. en este sentido, cabe destacar que el artículo 1 instaura de manera categórica el propósito fundamental de garantizar y salvaguardar los derechos inalienables de los niños, niñas y adolescentes, otorgándoles una protección efectiva en contra de toda forma de violencia y explotación.

Es crucial resaltar que este código no solo abarca situaciones evidentes, sino que también brinda una protección integral en relación al mal uso de tecnologías, incluso en ámbitos que podrían implicar la aparición de deepfakes u otras formas de manipulación digital, las cuales potencialmente podrían afectar de manera significativa a los menores.

El objetivo primordial de estas medidas de seguridad es asegurar el bienestar y desarrollo saludable de los niños, niñas y adolescentes, resguardando su integridad y evitando cualquier tipo de daño físico, psicológico o emocional que pudiera surgir como consecuencia de circunstancias inapropiadas o actos peligrosos.

Abordar lo que expone la ley Orgánica de Comunicación también es vital, pues esta norma regula los medios de comunicación y el contenido que se difunde en ellos, en el artículo 14, se establece la responsabilidad de los medios de comunicación para proteger a los menores y evitar la difusión de contenido que pueda ser perjudicial para ellos, esto podría incluir la regulación del contenido generado por deepfakes

## 2.5. Leyes y organismos capaces de servir como jurisprudencia en casos de pornografía infantil creada por deepfakes

Ley de Protección de Datos Personales:

Aunque no se centra únicamente en los menores, esta ley establece principios sobre la protección de datos personales, los deepfakes pueden involucrar el uso indebido de datos personales, y esta ley puede ofrecer un marco para proteger la identidad y privacidad de los menores, finalmente es necesario entender en un contexto legal mas actualizado lo que dice la Ley

de Delitos Informáticos, esta aborda los delitos relacionados con la tecnología y la informática. Aunque no trata específicamente los deepfakes, sí incluye la protección contra el uso indebido de la tecnología que podría aplicarse a casos de manipulación digital que afecten a menores. (Godoy & Magdalena, 2023)

Consejo Nacional de la Niñes y Adolescencia.

El CNNA contempla la pena para las personas que, sin consentimiento, realicen cualquier conducta vinculada a las TIC: captación, captura, adquisición, grabación, difusión, posesión, comercialización, distribución, exposición, divulgación, ofrecimiento, intercambio, compartición, suministro, compra, venta, exhibición, facilitación o entrega de sucesos de connotación sexual, erótica, carnal o semejantes: prisión de 5 a 7 años por esos actos se impondría a quien capture, modifique, destruya, borre, permita o proporcione información a una niña, niño o adolescente que, en cualquier fase de su generación, exposición o transmisión, le cause perjuicio mental, moral o afecte sus derechos, incluido el derecho de acceder a información personal. (Ochoa Marcillo, 2024)

La misma pena corresponderá a aquel que genere un accidente informático consistente en la operación no autorizada o incorrecta sobre un dispositivo electrónico, entrega de datos electrónicos, mensajes, órdenes o señales de cualquier orden a un sistema informático, infiltrándose, distorsionando o usando información de los titulares, explotando sus errores. (Ayala Rivera, 2023)

Ministerio de Educación:

Son atribuciones de la Dirección de Estudios y Proyectos: Planificar, coordinar, promover y controlar acciones efectivas contra la explotación sexual y económica, trata de personas y pornografía infantil y adolescente.

Ministerio del Interior:

El Ministerio del Interior será un organismo de apoyo del sistema de protección integral de niñez y adolescencia, y tendrá como atribuciones, ejecutar acciones de control del ciberespacio para evitar la explotación sexual de niñas, niños y adolescentes por medio de las Tecnologías de la Información y Comunicación. (Artieda, 2022)

## 2.6. Porque la pornografía elaborada con deepfakes es tan rentable

La tecnología de deepfake, que emplea algoritmos avanzados de inteligencia artificial para crear contenidos audiovisuales falsos pero muy realistas, ha revolucionado varios sectores, desde el entretenimiento hasta la seguridad, sin embargo, uno de los usos más preocupantes y controvertidos de esta tecnología es la creación de pornografía no consensuada, que se ha convertido en un fenómeno alarmante en la era digital.

Esta sección explora las razones por las que la pornografía generada con deepfakes es tan rentable y la dificultad para detectarla, a pesar de los esfuerzos por mejorar las herramientas de detección.

La rentabilidad de la pornografía generada con deepfakes se debe a una combinación de factores tecnológicos y socioculturales, en primer lugar, la tecnología deepfake permite crear contenido extremadamente convincente utilizando imágenes y vídeos de personas sin su consentimiento, este tipo de contenido suele ser muy demandado en plataformas clandestinas y sitios web de contenido adulto, donde el anonimato y la ilegalidad crean un mercado negro lucrativo.

La creación de estos vídeos no requiere de grandes recursos financieros ni técnicos por parte de los creadores. A diferencia de las producciones pornográficas tradicionales, que implican costos significativos en términos de producción, actores y equipos, la creación de deepfakes puede realizarse con software relativamente accesible y, en muchos casos, con conocimientos técnicos básicos, esta accesibilidad reduce las barreras de entrada y aumenta el potencial de lucro para los productores ilegales.

Además, la pornografía con deepfakes a menudo se dirige a una audiencia específica interesada en el contenido que involucra a celebridades o figuras públicas, la explotación de la imagen de figuras conocidas sin su consentimiento aumenta la demanda y el precio del contenido, este fenómeno se ve exacerbado por la capacidad de la tecnología para replicar de manera convincente las características faciales y vocales de las personas, haciendo que el contenido sea difícil de distinguir del material auténtico

Uno de los principales desafíos en la detección de la pornografía con deepfakes es la mejora continua de las técnicas de generación de contenido, los algoritmos de deepfake están en constante evolución, y los creadores de estos contenidos falsificados a menudo emplean métodos sofisticados

para eludir las herramientas de detección existentes, a pesar de los avances en la tecnología de identificación de deepfakes, los sistemas actuales enfrentan varias limitaciones.

En primer lugar, la detección de deepfakes a menudo requiere una combinación de métodos técnicos y humanos, las técnicas automatizadas, como el análisis de la coherencia facial y el rastreo de anomalías en el vídeo, pueden ser eficaces pero no siempre precisas, los deepfakes de alta calidad pueden superar estos sistemas mediante la creación de contenido que imita perfectamente las características del material auténtica, además la falta de datos de entrenamiento adecuados para los algoritmos de detección puede limitar la capacidad de estos sistemas para identificar nuevas formas de manipulación.

Otro desafío importante es la rapidez con la que se distribuye el contenido, los vídeos deepfake pueden ser subidos a plataformas en línea y compartidos a una velocidad que supera la capacidad de las herramientas de detección para mantenerse al día, esto es especialmente problemático en plataformas de redes sociales y sitios de contenido para adultos, donde la moderación y la supervisión suelen ser insuficientes para abordar la magnitud del problema.

La proliferación de la pornografía con deepfakes plantea graves problemas éticos y legales, la creación y distribución de estos vídeos infringe los derechos de privacidad y consentimiento de las personas, y puede tener consecuencias devastadoras para las víctimas, que a menudo enfrentan acoso y daño a su reputación, además, la dificultad para detectar estos contenidos alimenta una industria clandestina que opera fuera del alcance de la regulación y la justicia.

Para abordar estos desafíos, es fundamental que se implementen medidas más rigurosas tanto a nivel tecnológico como legal, las mejoras en los algoritmos de detección, junto con una mayor colaboración entre empresas tecnológicas y autoridades legales, pueden ayudar a combatir la proliferación de contenidos deepfake, también es crucial promover la educación y la conciencia sobre el tema para que las personas puedan reconocer y reportar estos contenidos de manera más eficaz.

### 2.7. Casos de estudio relevantes ante la temática del Deepfake

El principio detrás de los deepfakes se basa en el uso de algoritmos sofisticados para intercambiar los rostros y las voces de personas en imágenes y vídeos, produciendo contenido que

parece auténtico a simple vista, este nivel de realismo puede ser usado tanto para fines creativos e inofensivos como para aplicaciones más problemáticas, sin embargo, el uso de deepfakes para crear vídeos y fotos de famosos, especialmente en contextos dañinos o invasivos, plantea serios dilemas éticos y legales.

Una de las aplicaciones más controversiales es la creación de material pornográfico no consensuado, al integrar el rostro de una celebridad en vídeos explícitos, los creadores de deepfakes pueden explotar la imagen pública de estas personas sin su consentimiento, lo cual no solo es una violación de la privacidad, sino que también puede tener consecuencias devastadoras para la reputación y el bienestar de las figuras afectadas, este tipo de contenido se distribuye a menudo en plataformas clandestinas, lo que dificulta la regulación y el control.

Uno de los casos más notorios involucra a la actriz Scarlett Johansson, en 2018 se descubrió que su imagen había sido utilizada en varios vídeos pornográficos deepfake sin su consentimiento, estos vídeos, que presentaban su rostro en situaciones explícitas, se distribuyeron ampliamente en la web, Johansson junto con otros actores, enfrentó un desafío considerable para que el contenido fuera retirado de Internet y para proteger su reputación, este caso subraya cómo la explotación de la imagen de las celebridades mediante deepfakes puede tener un impacto devastador en su privacidad y bienestar personal.

Otro ejemplo prominente es el caso de la figura pública y periodista Meghan Markle, en 2019 se filtraron varios vídeos falsificados que aparentemente mostraban a Markle en situaciones comprometedoras, estos deepfakes, que empleaban su rostro para propagar rumores falsos, no solo afectaron su imagen pública, sino que también generaron una ola de desinformación en las redes sociales, la rapidez con la que se difundió el contenido y la dificultad para rastrear a los responsables ilustran los retos asociados con la gestión de deepfakes.

La sofisticación de los deepfakes complica aún más la detección de tales contenidos. Los sistemas actuales de identificación se basan en técnicas que buscan inconsistencias o irregularidades en el contenido, pero la alta calidad de los deepfakes más avanzados puede superar estas barreras, los algoritmos utilizados para generar deepfakes evolucionan constantemente, haciendo que las herramientas de detección también necesiten actualizarse con frecuencia para mantenerse efectivas.

Además, la velocidad con la que se distribuyen los deepfakes en línea, junto con el anonimato de las plataformas que los albergan, agrava la dificultad de la detección y eliminación de estos contenidos, las víctimas de deepfakes pueden enfrentar desafíos significativos para obtener justicia y eliminar el material dañino de la web.

La tecnología de deepfake ofrece un abanico de posibilidades creativas y profesionales, pero su potencial para ser mal utilizado plantea un desafío urgente, es crucial que se desarrollen soluciones tanto tecnológicas como legales para abordar este problema, la mejora continua en la detección de deepfakes y una mayor cooperación entre plataformas tecnológicas y organismos reguladores son esenciales para mitigar los riesgos y proteger la privacidad y la integridad de las personas, especialmente de aquellas que son figuras públicas y cuya imagen puede ser explotada de manera maliciosa.

## 2.8. Consideraciones éticas y psicológicas en la manipulación de pornografía infantil

Al analizar las consideraciones éticas en la manipulación de imágenes de menores, es importante reconocer el daño potencial que puede causar la creación de deepfakes, la manipulación de imágenes de menores puede tener consecuencias psicológicas y emocionales graves para las personas retratadas, así como para sus familias, el uso no autorizado de la imagen de un menor puede invadir su privacidad, violar sus derechos y exponerlo a explotación o daño. Es esencial considerar el bienestar y la seguridad de los menores al participar en cualquier forma de manipulación de imágenes.(Hernandez Guaman, 2018)

Además, la creación de deepfakes de menores plantea cuestiones éticas complejas sobre el consentimiento y la autonomía, los menores no pueden dar su consentimiento informado para el uso de sus imágenes, lo que los hace particularmente vulnerables a la explotación y la manipulación.

Esta falta de consentimiento plantea importantes preocupaciones éticas sobre el potencial daño y la violación de los derechos individuales, es fundamental que los creadores y consumidores de deepfakes consideren las implicaciones éticas de sus acciones y prioricen la protección y el bienestar de los menores, en conclusión las consideraciones éticas en la manipulación de imágenes de menores deben examinarse cuidadosamente y priorizarse para prevenir daños y proteger los

derechos de las personas en un panorama digital en constante evolución. (Pietrzykowski & Smilowska, 2021)

Los perfiles psicológicos de agresores sexuales y pederastas pueden ser una fuente importante de datos, sobre la percepción del delito de pornografía infantil desde el punto de vista de sus principales consumidores, es primordial destacar que el numero de delincuentes sexuales ha crecido de forma alarmante por lo que el numero de pederastas y pedófilos han alcanzado nuevas y alarmantes cifras, esto forma parte de este estudio ya que es necesario enlazar a la psicología de los delincuentes, al mismo delito, por lo que también será necesario definir las diferencias entre pedófilo y pederasta.

La pedofilia es considerada como un trastorno asociado a las parafilias, esta misma se caracteriza por la atracción sexual, que involucra intensos impulsos sexuales, fantasías y conductas que generan un desmedido nivel de excitación por niños y niñas, este tipo de sujetos buscan a los menores como un objeto sexual, el cual se ve mas accesible por medio del internet, siendo la pornografía infantil un estimulante que permite la autosatisfacción sin contacto, ni relaciones sexuales con los menores, los pedófilos suelen catalogar a las caricias como algo ajeno al sexo por lo que son inofensivas, de igual forma estos individuos tienden a idealizar que sus acciones se deben al cariño que sienten por los niños y niñas. (Serranos Minguela, 2023)

La pederastia por otro lado es una inclinación erótica hacia menores, en la que el sujeto no solo consume pornografía infantil para satisfacer sus impulsos sexuales, sino que los lleva a la realidad, llevando acabo un acto de penetración entre un menor de edad y un adulto, este tipo de enajenados tienden a auto justificar sus acciones, por lo que comúnmente no tienen remordimiento por sus actos, e incluso pueden llegar a tener una postura en la que definen a sus actos como medios de aprendizaje que usaran los niños durante toda su vida.

Con el crecimiento de la pornografía infantil generada por IA se corre el riesgo de que los pedófilos se conviertan en pederastas, mismos que ya no solo querrán consumir actos computarizados generados por algoritmos, sino que desearan llevar a cabo aquellas fantasías macabras que disfrutan y almacenan.

frecuente la interrogante que nos hacemos como sociedad es: ¿porque niños? Y la respuesta puede radicar muchas veces en que, este tipo de personas trastornadas sienten atracción por menores debido a su incapacidad por mantener contacto sexual con adultos y sienten un enorme

miedo de no poder llenar las necesidades físicas presentes en relaciones con personas mayores, por lo que buscan a niños y niñas para tratar de sentirse superiores y llenar su vacío de incapacidad. (BELTRÁN JARAMILLO, 2023)

La psiquis de este tipo de delincuentes con frecuencia se ve plagada de traumas y abusos, la carencia de figuras paternales suele ser un patrón, al igual que la violencia en entorno familiares hostiles que afectan directamente en el desarrollo social de los individuos, existen varios tipos de abusadores los cuales por distintos motivos sienten una enorme fascinación por los menores de edad, sin embargo y debido a su naturaleza enlistaremos a los que usualmente son los principales consumidores de pornografía infantil

Entre ellos encontramos a:

Abusadores regresivos: este tipo de sujetos con frecuencia llevan relaciones de parejas heterosexuales con personas de su mismo rango de edad, sin embargo con la presencia de desgastes en las relaciones amorosas en sus intimidad o eventos traumáticos, empiezan a sentir una necesidad por querer tener el control de nuevas relaciones compensando aquellas que no fueron fructíferas con personas de su edad.

Este distanciamiento con un circulo de personas de la misma edad provoca que se genere una fijación por niños y niñas que tienden a manipular y seducir para de esa forma abusar sexualmente de ellos, compensado de esa forma el resquebrajamiento de sus relaciones interpersonales, usualmente los sujetos empiezan a consumir pornografía infantil, para definir sus nuevas inclinaciones y después abusar de los menores quienes por lo general se encuentran en un ambiente intrafamiliar. (HERNANDEZ CHAVEZ, 2023)

Abusador con disfunción sexual y tendencias agresivas: encuentras placer en el sufrimiento de sus victimas y por lo general demuestra gran fascinación por mujeres o menores con rasgos femeninos.

Abusadores subindividuados con diferenciación débil: usualmente los abusos generados en el presente son una forma de subsanar carencias pasadas y se han visto cifras tanto en entornos familiares y extrafamiliares, igualmente en este tipo de abusadores de puede notar diversidad en tendencias sexuales, siendo la heterosexual y homosexual la mas marcada.

**2.8. Perfil de agresores sexuales consumidores de pornografía infantil:**

Las tendencias criminales en los delincuentes sexuales han sido estudiadas ampliamente por el campo de la psicología, su estudio a permitido que se armen y desarrollen perfiles que representan rasgos masivamente detectados que crean patrones con los cuales es mas fácil entender los actos de desviación sexual hacia niños y niñas.

Los perfiles psicológicos de personas que sienten inclinaciones por niños y niñas suelen compartir ciertas particularidades psicológicas patológicas, los agresores sexuales no saben afrontar las crisis y el rechazo por lo que con frecuencia asocian sus conductas a la negación como un recurso, el cual ellos utilizan para manipular la ley, normalmente sufren una disociación de sus pensamientos por lo que tienen conductas impulsivas lo que impide el correcto desarrollo de la empatía y valores sociales

Los perfiles emocionales de los agresores sexuales usualmente se ven infestados de fantasías sexuales excesivas, las cuales tratan de suplantar las relaciones interpersonales inexistentes de los mismos, los agresores sexuales tienden a maximizar acciones pequeñas, lo que atribuye conceptos incorrectos de la imagen y rasgos de los niños y niñas.

Los pedófilos y pederastas también manifiestan altos niveles de hostilidad hacia personas adultas y al rechazo de sus víctimas, así también muestran un enorme interés y preocupación por todo lo que concierne a niños y niñas.

Se ha visto manifestado el patrón de qué este tipo de delincuentes tienden a tratar de rodearse de niños y niñas por lo que para esto buscan ambientes en los que se vean rodeados de menores, en escuelas, o ambientes en los que ellos se vean desprotegidos debido al contexto en el que se encuentran, los agresores sexuales tienden a presentar sentimientos de inferioridad esto es a causa de una baja autoestima y poca tolerancia al estrés.

Muchos de ellos también presentan un perfil narcisista e impulsivo con rasgos de introversión y neuróticos, así como también un enorme infantilismo que caracteriza a los agresores sexuales. el cual le sirve para engañar y manipular a los menores y atraer a sus potenciales víctimas.

En cuanto al consumo de pornografía este tipo de agresores almacenan fotos de niños y niñas, para poder auto satisfacerse, Tras descubrir su Desviación por los menores, los mismos tienden a gradualmente ir incrementando el consumo de pornografía, la misma que se volverá más violenta

según el nivel de desviación que tenga esta persona, los pedófilos y pederasta tienen a usar símbolos para identificar a niños y niñas usualmente usan un código en el que los triángulos representan a niños y los corazones representan a niñas, Se ha visto que muchos de ellos utilizan este tipo de simbología en objetos como anillos cadenas e incluso en tatuajes

Los pedófilos y pederastas usualmente no vengan los cuerpos de los niños como la atracción directa de su sexualidad sino que más bien esto es un potenciador sexual, este tipo de delincuentes fijan su interés en menores debido a que tratan de representar su niñez donde se invierten papeles, y ahora ya no son ellas las víctimas si no los victimarios por lo que necesitan encontrar alguien que supla su papel.

Generalmente los delitos sexuales no ocurren de forma imprevista sino que vienen a raíz de varios factores como, problemas psicológicos, maltrato físico, conflictos familiares, consumo excesivo de pornografía y privaciones extremas de cariño o recursos vitales, los delincuentes sexuales tienden a buscar niños que no tengan ambientes familiares cercanos o que no posean familiares quienes estén al pendiente de ellos, de esa forma no tendrán alguien de confianza con quien hablar de lo sucedido y por ende ellos se auto convencen de que la victimas aceptará la violación como algo positivo que al contrario de lo que es representará afecto y atención. (Hernandez Guaman, 2018) –

# CAPITULO III

# CIBERDELITOS EN EL PANORAMA INTERNACIONAL

## 3.1. Legislación comparada ante el problema de deepfakes

Países en Europa como España, han percibido un enorme crecimiento de esta temática, por lo que, dentro de este ámbito, en España el Administrador de la AGPD (agencia de protección de datos) debería establecer las medidas de protección adecuadas, regulaciones, procedimientos y controles para garantizar el correcto desarrollo del sistema IA sin perjuicio del ejercicio de los derechos, libertades e intereses legítimos de las partes interesadas. (Delgado, 2020)

El Comité Europeo de Protección de Datos (CEPD) especialmente debe establecer medidas técnicas y organizativas para garantizar que los datos personales de los menores no estén sujetos a ninguna forma no deseada de procesamiento de naturaleza estrictamente comercial, política o religiosa, o cualquier otra forma de segmentación de comportamiento que pueda ser perjudicial para los intereses o derechos de los menores. (Martínez-Pastor et al., 2022)

En México y Argentina, donde la tecnología avanza a pasos agigantados, los padres y tutores procuran estar cada vez más alerta y educar a sus hijos sobre los peligros que pueden encontrarse en internet y cómo proteger su información personal, además es fundamental que las autoridades fortalezcan las leyes y regulaciones en materia de protección de datos y privacidad, así como que se realicen campañas de concientización dirigidas a toda la sociedad. Solo así podremos asegurar un entorno seguro y protegido para menores, es crucial que tomemos acciones inmediatas para combatir esta preocupante tendencia y garantizar un futuro digital seguro para las próximas generaciones. (Bustamante Parodi, 2023)

## 3.2 Implicaciones del uso de IA

Algunas de las implicaciones que debemos tomar en cuenta son la privacidad y protección de datos, la inteligencia artificial suele necesitar grandes cantidades de datos para funcionar de manera efectiva, por lo que requiere la recopilación de datos personales para entrenar algoritmos puede poner en riesgo la privacidad si no se gestiona adecuadamente, es por eso que la transparencia es primordial ya que los ciudadanos tienen derecho a saber cómo se recopilan y utilizan sus datos.

Las políticas y regulaciones deben garantizar que las personas tengan acceso a esta información y puedan ejercer control sobre sus datos, así se garantizará la seguridad de datos y la protección de datos personales contra accesos no autorizados es fundamental, así será posible evitar las violaciones de seguridad pueden tener consecuencias graves para los individuos.

### 3.3 Implicaciones de los deepfake en ciberseguridad y politica

El delito de deepfake y la pornografía infantil generada por inteligencia artificial (IA) es un tema de gran relevancia en la sociedad contemporánea, en este sentido, es importante analizar cómo la legislación ecuatoriana aborda esta problemática y qué medidas se han implementado para combatirla, así como las implicaciones legales y éticas que conlleva, la era tecnológica, en nuestras manos se ha convertido en un arma de doble filo, seguro que al menos una vez hemos visto un video falso o una imagen manipulada y cada vez es más común en la era tecnológica actual, la proliferación de deepfakes y pornografía generada por IA plantea un desafío sin precedentes para la sociedad y la legislación ecuatoriana.

Es crucial comprender el alcance y las implicaciones de este fenómeno en el contexto local cada día se vuelve más repetitiva la frase "La tecnología cada día nos sorprende más". y es que a todos nos han llegado vídeos de deepfakes en los que se mezclan los rostros de políticos con otros cuerpos presentando discursos todavía más innovadores y creíbles que los propios.(Véliz & Chavez, 2024)

John K. Holum, antiguo subsecretario de la Marina de los Estados Unidos, afirmó que "La información es poder, hoy el control de información significa el control de su distribución, los EE. UU y el resto del mundo se encuentra en un encrucijada", si tomamos en cuenta este argumento en cuanto a la regulación de los delitos informáticos y la protección de los derechos de los niños y niñas, enfrentamos un enorme desafío, el avance tecnológico ha facilitado la creación y difusión de contenido que atenta contra la integridad de menores de edad y así como la información genera poder, su uso incorrecto genera amenazas contra la dignidad humana. (Fitzgerald, 2023)

### 3.4. Implicaciones de los deepfake en propiedad intelectual

Cuando hablamos de información, debemos referirnos a la digital que a lo largo de los años ha sido asimilada por el ser humano, pero que hoy se transformó en un conjunto de documentos o datos para tomar anotaciones y que posteriormente serán reemplazados por carpetas y cajas de almacenamiento virtual suplementarias para repartir y generar respuestas rápidas debido a la acumulación de información.

Puede afirmarse que mayormente los más interesados en propiedad intelectual y derechos de autor son aquellas personas que se encuentran en un entornos profesionales como artistas de diversas áreas o incluso como jueces, notarios, abogados, estos últimos utilizan los documentos fotocopiables como notación para hacer "propiedad" del texto o el diseño original, estos hechos para quienes hacen uso recurrente de la IA en ambientes laborales podría representar un inconveniente, debido a que la mayoría de barreras en la creación de documentos y fabricación de datos han sido superados gracias al desarrollo abrumador de las denominadas Nuevas Tecnologías de la Información, (Arias et al., 2022)

Resulta intrínseco mencionar la íntima relación de la IA con la propiedad intelectual, este planteamiento es necesario debido a que en términos legales y referentes a la creación de pornografía infantil pueden verse ligada la culpabilidad de los “autores” de estas infracciones con el uso de herramientas de inteligencia artificial.

En los Estados Unidos y la Unión Europea, la propiedad de las creaciones producidas por inteligencias artificiales y computadoras se asigna al creador material o programador que ejerce control sobre ellas, por otro lado, la normativa vigente en países como China, India y Rusia establece que, en ausencia de un contrato en sentido contrario, la titularidad recae en el primer inventor, recientemente, los sistemas legales anglosajón y europeo han comenzado a enfocarse en otorgar la propiedad a la persona natural que desarrolló la herramienta de inteligencia artificial. Las legislaciones de China, India y Rusia destacan la importancia de establecer un acuerdo contractual entre las partes, ya sea de manera exclusiva o no, incluyendo aspectos como contraprestaciones u otras formas compensatorias relacionadas con las obras producidas por la inteligencia artificial. (Osorio & Enerieth, 2020)

Si la atribución de la titularidad se lleva a cabo de manera errónea, se puede generar un daño potencialmente gigantesco tanto a nivel económico como incluso a nivel de explotación, frenando

al mercado para creaciones que contienen alto contenido de innovación, a través de la exclusividad o dejando de obtener beneficios de creaciones innovadoras y distinguidas por la clientela respecto de los competidores, prestigiando a su titular respecto a los competidores, entre otros aspectos. (Cristina López Sánchez, 2020)

También es posible que la atribución sea errónea en el sentido de atribuir cada obra generada por un proceso de IA a un autor distinto, en cuyo caso cada autor estaría en condiciones de desplegar la totalidad de los derechos propios de su condición, con lo que se corre el riesgo de sufrir acciones de infracción de derechos de terceros por carecer de la licencia necesaria para explotar legalmente la obra.(Cristina López Sánchez, 2020)

## CONLCUSIONES:

La creciente exposición de niños y niñas a contenido problemático en el entorno digital es una inquietud cada vez más notable. Los menores, que interactúan activamente con diversas plataformas en línea, son especialmente susceptibles a los efectos negativos de los deepfakes y otros contenidos generados por inteligencia artificial. La escasez de supervisión y la falta de educación sobre el uso seguro y responsable de la tecnología pueden resultar en situaciones de acoso, confusión y daños emocionales. Por ello, es fundamental abordar estos problemas desde una perspectiva preventiva, creando entornos digitales seguros y fomentando la alfabetización digital en la juventud.

Asimismo, el consumo de pornografía generada por deepfakes representa un fenómeno preocupante. Este tipo de contenido frecuentemente implica la manipulación no consensuada de imágenes de personas, lo que no solo suscita dilemas éticos, sino que también puede contribuir a normalizar comportamientos dañinos y a desensibilizar a la sociedad frente a la violencia sexual. La difusión de este tipo de materiales no solo impacta a las víctimas, sino que también afecta a quienes los consumen, quienes podrían desarrollar expectativas poco realistas y actitudes nocivas hacia la sexualidad.

En resumen, el desarrollo del contenido creado por inteligencia artificial, junto con la proliferación de deepfakes y la ausencia de regulación adecuada, presenta desafíos serios que requieren atención inmediata. Es crucial implementar políticas legislativas y programas educativos que protejan a los grupos más vulnerables, especialmente a los niños y niñas. Entender profundamente estos fenómenos y sus repercusiones es clave para establecer un entorno digital más seguro y responsable.

Solo a través de un esfuerzo conjunto podremos reducir los riesgos que conlleva el uso de estas tecnologías y asegurar que su evolución sea beneficiosa para la sociedad en general.

## BIBLIOGRAFÍA

Arias, C., Soto Montoya, C. L., & Sacón Martinez, E. E. (2022). Particularidades del uso de las Tecnologías de la Información y la Comunicación en la Educación. *Religación: Revista de Ciencias Sociales y Humanidades*, *7*(31), 1.

Arteaga, C. B. (2024). Deepfakes Sexuales: Impacto, prevención y perspectivas de género en el entorno digital. *Miguel Hernández Communication Journal*, *15*, 229-244. https://doi.org/10.21134/zt4eht31

Artieda, V. E. C. (2022). HACKTIVISMO DE ANONYMOUS EN EL ECUADOR: ANÁLISIS REALISTA DE LAS ESTRATEGIAS Y CONSECUENCIAS DE LOS ACTORES NO ESTATALES TRANSNACIONALES EN EL MODELO ECUATORIANO DE CIBERSEGURIDAD (2011-2020). *1*, *1*. https://repositorio.puce.edu.ec/server/api/core/bitstreams/3ba00396-d4a7-4f60-9e15-cf69ad297147/content

ASAMBLEA NACIONAL. (2014). *Código Orgánico Integral Penal*. Registro oficial. file:///C:/Users/andym/OneDrive/Escritorio/Andy/Carpeta%20Andy/normativas/leyes/coip%202023.pdf

Ayala Rivera, C. A. (2023). *Análisis de la vulneración del derecho a la intimidad y la difusión de materiales pornográfico de las personas*. DSPACE UNIANDES. https://dspace.uniandes.edu.ec/handle/123456789/16234

BELTRÁN JARAMILLO, S. G. (2023). *ANALISIS SOBRE LOS RIESGOS DE SEGURIDAD EN INTERNET Y REDES SOCIALES EN ADOLSECENTES Y MENORES DE EDAD DE LA PROVINCIA DE LOS RÍOS.* DSPACE. http://dspace.utb.edu.ec/bitstream/handle/49000/14160/E-UTB-FAFI-SIST.INF-000099.pdf?sequence=1

Botha, J., & Pieterse, H. (2020). *Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security*.

Bustamante Parodi, R. A. (2023). *La mediación parental en el uso de redes sociales de hijos adolescentes*. https://repositorio.ulima.edu.pe/handle/20.500.12724/19307

Cristina López Sánchez. (2020). *La indemnización del daño moral derivado de la infracción de derechos de propiedad intelectual e industrial*. Dspace Universidad Miguel Hernández; Dspace.UMH. https://dspace.umh.es/bitstream/11000/31644/1/2.%20IndeminizacDa%C3%B1oMoral.pdf

Delgado, J. M. C. (2020). Plataformas para el aprendizaje en línea: La protección de datos en el ámbito educativo. *Avances en Supervisión Educativa*, *33*, Article 33. https://doi.org/10.23824/ase.v0i33.680

Fitzgerald, D. (2023). *Uncertain Warriors: The United States Army between the Cold War and the War on Terror*. Cambridge University Press. https://doi.org/10.1017/9781009235822

García Ull, F. J. (2021). «Deepfakes»: El próximo reto en la detección de noticias falsas. *Anàlisi: Quaderns de comunicació i cultura*, *64*, 103-120.

Godoy, S., & Magdalena, M. (2023). *Producción de contenidos interculturales como política pública en Ecuador a través de la Ley Orgánica de Comunicación (LOC). Estudio del diario La Hora Esmeraldas y El Norte de Imbabura.* [masterThesis, Quito, Ecuador : Flacso Ecuador]. http://repositorio.flacsoandes.edu.ec/handle/10469/19038

Gómez, O. Y. A., & Gómez, W. O. A. (2024). Consideraciones éticas para el uso académico de sistemas de Inteligencia Artificial. *Revista Internacional de Filosofía Teórica y Práctica*, *4*(1), Article 1. https://doi.org/10.51660/riftp.v4i1.95

Granados Ferreira, J. (2022). Análisis de la inteligencia artificial en las relaciones laborales. *Revista CES Derecho*, *13*(1), 111-132. https://doi.org/10.21615/cesder.6395

HERNANDEZ CHAVEZ, M. L. (2023). *CONSECUENCIAS DEL ABUSO SEXUAL INFANTIL. UNA MIRADA PSICOANALITICA* [REPOSITORIO]. UVAQ. http://dspace.uvaq.edu.mx:8080/jspui/bitstream/123456789/2950/1/MARTHA%20LILIA%20HERNANDEZ%20CHAVEZ%20MTRIA%20PSICOTERAPIA%20PSICOANALITICA%20DE%20LA%20INFANCIA%20Y%20ADOLES.pdf

Hernandez Guaman, D. N. (2018). *PERFIL PERSONOLÓGICO DEL PEDÓFILO Y PEDERASTA, ASÍ COMO LOS TRATAMIENTOS PSICOLÓGICOS MÁS EFECTIVOS*. https://repositorio.utmachala.edu.ec/bitstream/48000/12749/1/ECUACS-2018-PSC-DE00023.pdf

Inglada Galiana, L., Corral Gudino, L., & Miramontes González, P. (2024). Ética e inteligencia artificial. *Revista Clínica Española*, *224*(3), 178-186. https://doi.org/10.1016/j.rce.2024.01.007

Lopez Sanchez, C. (2017). *Problemática actual de la tutela civil ante la vulneración de la propiedad industrial e intelectual* (1.ª ed.). Dykinson. https://doi.org/10.2307/j.ctt22nmcw2

Martínez-Pastor, E., Cetina Presuel, R., & Castelló-Martínez, A. (2022). Regulación y autorregulación en la creación de contenidos de menores en plataformas digitales. *Revista Mediterránea de Comunicación: Mediterranean Journal of Communication*, *13*(1), 13-15.

Noguera, M., Edotti, L., Galofre, A., Martínez, L., & González, P. G. (2023). La pornografía infantil en entornos digitales en Colombia. *Tejidos Sociales*, *5*(1), Article 1. https://revistas.unisimon.edu.co/index.php/tejsociales/article/view/6201

Ochoa Marcillo, A. C. (2024). Desafíos globales del cibercrimen. *2024*, *1*. https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Osorio, A., & Enerieth, N. (2020). *El derecho de autor en la Inteligencia Artificial de machine learning (Copyright Law in the Artificial Intelligence of Machine Learning)* (SSRN Scholarly Paper 3790753). https://papers.ssrn.com/abstract=3790753

Pailiacho, C. A. R., & Amancha, R. J. M. (2024). La regulación jurídica del ciberdelito del carding a través del derecho comparado. *DCSPACE UNACH*. http://dspace.unach.edu.ec/bitstream/51000/13452/1/Malo%20Amancha%2C%20R%20y%20Robalino%20Pailiacho%2C%20C%20%282024%29%20La%20regulaci%C3%B3n%20jur%C3%ADdica%20del%20ciberdelito%20del%20carding%20a%20trav%C3%A9s%20del%20derecho%20comparado%28Tesis%20dePregrado%29%20Universidad%20Nacional%20de%20Chimborazo%2C%20Riobamba%2C%20Ecuador.pdf

Pietrzykowski, T., & Smilowska, K. (2021). The reality of informed consent: Empirical studies on patient comprehension-systematic review. *Trials*, *22*(1), 57. https://doi.org/10.1186/s13063-020-04969-w

Pulido, I. G. (2023). El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: Ante el auge de los deepfakes. *IUS ET SCIENTIA*, *9*(2), Article 2. https://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

SEON. (2023). *Deepfake*. SEON ES. https://seon.io/es/recursos/glosario/deepfake/

Serranos Minguela, L. (2023). *ANÁLISIS CLÍNICO DEL USO DEL DIAGNÓSTICO DE PEDOFILIA EN LOS DELITOS DE ABUSO SEXUAL INFANTIL Y CORRUPCIÓN DE MENORES*.

https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/74200/Serranos%20Minguela%2C%20Laura%20-%20TFM.pdf?sequence=1

Terol, T. M. (2023). Innovación MedIÁtica: Aplicaciones de la inteligencia artificial en el periodismo en España. *Textual & Visual Media*, *17*(1), Article 1. https://doi.org/10.56418/txt.17.1.2023.3

Toro Hernandez, G. A. (2024). *Deepfake una amenaza para niños, niñas y adolescentes Ecuatorianos en el mundo digital*. DSPACE UNIANDES. https://rraae.cedia.edu.ec/Record/UNIANDES_9ec0ac2d5ef4105e7c977b7db7c50c15

Véliz, C. G., & Chavez, X. C. (2024). Desafíos y dimensiones de la desinformación en ALAC: Deepfakes y la urgencia de proteger los derechos de las mujeres. *Espacio I+D, Innovación más desarrollo*, *13*(36), Article 36. https://doi.org/10.31644/IMASD.36.2024.a19

Vestri, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, *56*, 368-398.

World economic forum. (2024, junio 2). *En un mundo de deepfakes, debemos defender los contenidos sintéticos de IA honestos*. Foro Económico Mundial. https://es.weforum.org/agenda/2024/06/en-un-mundo-de-deepfakes-debemos-defender-los-datos-sinteticos-de-ia-fiables/

# Anexos

Universidad Católica de Cuenca

# AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

**Renata Correa Peña** portador(a) de la cédula de ciudadanía Nº **0107287450**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"DELITO DE DEEPFAKE Y PORNOGRAFÍA INFANTIL GENERADA POR INTELIGENCIA ARTIFICIAL (IA) EN LA LEGISLACIÓN ECUATORIANA"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **10 de octubre de 2024**

F: .....

**Renata Correa Peña**

C.I. **0107287450**