UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

COMUNIDAD EDUCATIVA AL SERVICIO DEL PUEBLO

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TÍTULO

LA OMISIÓN DEL DELITO DE DEEPFAKE EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL EN ECUADOR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

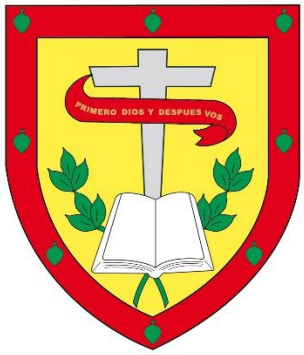
AUTORA: NATHALY LIZBETH AREVALO FERNANDEZ

DIRECTOR: DR. JUAN PABLO MARTÍNEZ ALBORNOZ

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

LA OMISIÓN DEL DELITO DE DEEPFAKE EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL EN ECUADOR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

AUTORA: NATHALY LIZBETH AREVALO FERNANDEZ

DIRECTOR: DR. JUAN PABLO MARTÍNEZ ALBORNOZ

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Nathaly Lizbeth Arévalo Fernández portador(a) de la cédula de ciudadanía **Nº 0104767090**. Declaro ser el autor de la obra: **"La omisión del delito de DEEPFAKE en el Código Orgánico Integral Penal en Ecuador"**, 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, **04 de julio de 2024**

F: .....

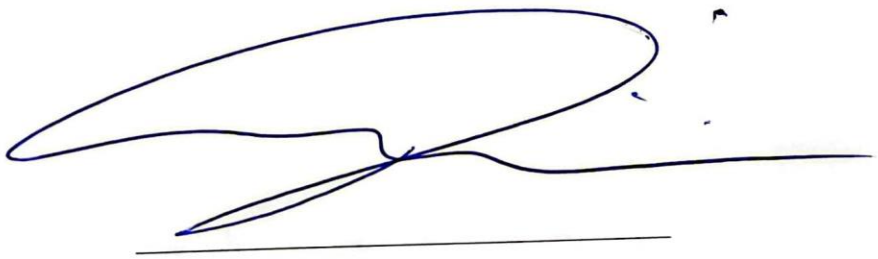
Nathaly Lizbeth Arévalo Fernández

C.I. 0104767090

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente trabajo de investigación desarrollado por la estudiante, **NATHALY LIZBETH AREVALO FERNANDEZ**, con numero de cedula, **0104767090**, con el tema, **"La omisión del delito de DEEPFAKE en el Código Orgánico Integral Penal en Ecuador."**, bajo mi supervisión.



Dr. Juan Pablo Martínez Albornoz

Tutor

Dedicatoria

El aprendizaje es uno de los pilares fundamentales del desarrollo humano. A través de la adquisición de conocimientos, no solo entendemos mejor el mundo que nos rodea, sino que también desarrollamos habilidades críticas para enfrentar los desafíos de la vida. La capacidad de aprender es una de las cualidades más valiosas que poseemos, ya que nos permite adaptarnos, innovar y progresar.

En este presente estudio de investigación se encuentra dedicado primeramente a Dios, ya quien es el motor de mi camino en lo largo de mi carrera que me ha permitido llegar a cumplir un logro más en mi etapa académica, iluminándome con su sabiduría así permitiéndome dar un gran paso en mi carrera en realizar una meta más dentro de mi vida con la guía de un Dios en mi entorno académico y mi vida cotidiana.

Mis padres, que, con su amor, ardo trabajo y el sacrificio a lo largo de estos años que están a mi lado dándome su apoyo y consejos me han permitido llegar hasta aquí, mi madre por ser mi consejera y quien me permite día a día ser una mejor mujer llena de principios y valores aplicándolos en mi educación académica que con gran esfuerzo me ha permitido alcanzar mi sueño de ser una mujer profesional, me apoyaste económicamente y psicológicamente con tu ejemplo me doy cuenta que sin una profesión no podría alcanzar lo que tú ya lo has hecho, n dándonos todo a pesar de que a ti te falte, protegiéndonos de todo sin importar las lágrimas que te ha tocado derramar por todo eso no tengo palabras para agradecerte pero si para demostrarte que te voy a apoyar ahora y siempre mamá.

A mi padre quien no cree que la educación es forjar a las personas para ser útil a la sociedad y demostrar con mis logros que puedo alcanzar lo que me propongo, no crees en mi educación, pero te puedo decir que eso me ayudo a luchar y te voy a demostrar que si se puede sobresalir te quiero a pesar de todo el tiempo tenemos gratos momentos que compartimos en mi niñez,

pero necesite tu mano al final, no importa ahora yo puedo ya extenderte la mía cuando mas lo necesites no dudes que ahí estaré.

A mi hermana y hermano, quienes he tenido que demostrar mi fortaleza y mi inspiración porque son mi ejemplo a seguir, gracias a ustedes soy más fuerte y termine mi carrera demostrándoles que con sacrificio y dedicación pueden lograr lo que se proponen a pesar de tantas adversidades siempre hemos luchado juntos y no será solo esta etapa vendrán más alegrías porque ahora les toca a ustedes demostrar lo que son ya que me dieron su apoyo mediante sus palabras siempre estando presente en cada logro de mi etapa académica como en mi vida brindándome la ayuda necesaria para llegar a la obtención de este título.

Mis abuelos maternos, papi Víctor, aunque está ausente recuerdo que un día me dijo que me quería ver graduada y aquí estoy si pude si lo logre, gracias por haberme motivado con pequeñas cosas tengo tantos recuerdos que me faltarían para escribirlos solo me queda decirle en donde este que lo logre. Mami Gladys gracias por abrirnos las puertas de su casa permitiéndonos que cumplamos con nuestros sueños lo logre como usted siempre me dice ESTO TE VA ASERVIR A VOZ y así es mamita gracias por ayudarnos y permitirnos alcanzar lo que nos proponemos usted es un ejemplo de lucha incansable por eso seguiré sus pasos siempre como luchar para sobresalir.

Mis amigos que me ayudaron a contribuir en este logro de mi meta académica que sin esperar nada me permitieron el compartir conocimiento, alegrías a lo largo del desarrollo de este estudio de investigación con el objetivo de hacer del aprendizaje una manera bonita de desarrollarme en mi entorno académico.

Finalmente, a todos aquellos que, de una manera u otra, han contribuido a que este proyecto sea una realidad, mi más sincero agradecimiento. A mis familiares, que han sido una fuente constante de apoyo y cariño; a las personas, por sus consejos y colaboración; y a todas las personas que han creído en mí y me han apoyado en este viaje. Este logro es un reflejo de

vuestro apoyo y de la red de afecto y conocimiento que me ha rodeado al cumplir un logro más en mis objetivos de vida.

Agradecimiento

En este proceso investigativo una frase de Sofocles (497-406 a.C.): "El agradecimiento da sentido a nuestro pasado, trae paz para hoy y crea una visión para el mañana."; El agradecimiento es una poderosa herramienta en la que encontramos un sentido a nuestro pasado, eso no lleva atraer una paz a nuestro presente y crea una visión para el futuro de las personas. Pues cuando reflexionamos sobre nuestras experiencias pasadas con agradecimiento, transformamos cada momento en una lección valiosa. Los desafíos y las dificultades se convierten en oportunidades de crecimiento, y los momentos de alegría y éxito se destacan como bendiciones que han enriquecido nuestras vidas.

Una frase la cual marco una razón por la cual estudiar y poder desenvolverme es: “Si quieres cambiar tu vida, intenta dar las gracias. Cambiará tu vida poderosamente.”; el dar las gracias es el reconocer que atrás de cada logro se encuentra el esfuerzo y el apoyo de las personas que por más pequeño sea para la para la persona que lo realiza es grande ya que no hay regalo más bonito en la vida que el poder agradecer de una manera sincera.

Nunca dejaré de agradecer por hacer de mí una mejor persona cada día. A Dios, le doy gracias por la felicidad que ahora tengo en mi vida, el cumplir un objetivo más en mi vida académica y por las personas que están a mi lado, Por una oportunidad más de ser mejor y aprender de mis errores.

En primer lugar, quiero agradecer a mis padres por su apoyo incondicional que me ha permitido alcanzar todas mis metas personales y académicas. Siempre me animaron con su amor a perseguir mis objetivos y nunca rendirme ante las dificultades. También me brindaron apoyo material y económico para que pudiera concentrarme en mis estudios y nunca rendirme con el esfuerzo de día a día hacen para ver crecer a sus hijos uno de ellos soy yo quienes han estado desde inicio hasta el final de mis estudios académicos.

En segundo lugar, estoy agradecida con mis hermanas los cuales con su apoyo en pequeñas cosas marcaron algo especial en dentro de este ámbito académico haciéndome ver que el amor, cariño y la perseverancia en un objetivo a pesar las dificultades que se presenten a lo lardo de la misma me permitieron aprender de ellas y a crecer como una mejor mujer para el mundo académico y de igual manera al mundo laboral.

En tercer lugar, con las persona que me apoyaron en el desarrollo de este presente estudio el cual con su perseverancia me enseñaron que toda persona es capaz de llegar a donde quiere cuando la persona se lo propone llega a cumplir sus metas, pues aprendí que las caídas académicas y todas las malas noches son el esfuerzo de una meta más en mi vida académica permitiéndome poder llegar al punto de mi carrera en el cual me encuentro sintiendo una alegría de agradecer la existencia de las personas así con un noble corazón capaz de hacer ver lo bonito que es el estudio y la satisfacción de disfrutar al final un logro más adquirido en mi vida.

Estoy sumamente agradecida con mi mentor por su dedicación y paciencia, sin sus palabras y correcciones precisas no podría haber llegado a culminar con esta etapa académica. Gracias por su orientación y todos sus consejos, siempre los recordaré en mi futuro profesional.

Por último, agradecer a la universidad que me ha exigido tanto en mi desarrollo académico, pero al mismo tiempo me ha permitido obtener mi tan ansiado título de ser una profesional capaz de demostrar mis conocimientos en mi proceso académico conjunto con las personas que me rodean y me enseñan. Agradezco a cada directivo por su trabajo y por su gestión, sin lo cual no estarían las bases ni las condiciones para la finalidad de mi proyecto de investigación

Resumen

El delito de *deepfake* implica la creación y difusión de contenido audiovisual manipulado mediante inteligencia artificial para falsificar la identidad de individuos. La presente investigación examina la falta de tipificación en el Código Orgánico Integral Penal, centrándose en la vulneración del derecho de imagen, honra, dignidad, buen nombre con el uso inadecuado de la inteligencia artificial generando un efecto negativo en el titular de la información.

Analizando riesgos asociados, como la desinformación, el fraude y la invasión de la privacidad, explora casos relevantes para ilustrar las consecuencias legales y éticas, proponiendo mediante la normativa se considere un mejor control sobre el uso de la inteligencia artificial. Se concluye que, para enfrentar este delito, es esencial una colaboración interdisciplinaria que combine avances en inteligencia artificial con un marco legal del Código Orgánico Integral Penal del Ecuador para una mayor concienciación pública. El delito de *deepfake* lleva a vulnerar los derechos del titular de la información dando un uso inadecuado de la Inteligencia Artificial. Se recomienda la aplicación de leyes específicas que penalicen el uso indebido de *deepfakes.*

Palabras clave*: deepfake,* Inteligencia Artificial, privacidad, derecho a la imagen, omisión.

Abstract

The crime of *deepfake* involves creating and disseminating manipulated audiovisual content using artificial intelligence to fake individuals' identities. This research examines the lack of classification in the Comprehensive Organic Criminal Code (COIP by its Spanish acronym). It focuses on violating the right to image, honor, dignity, and good name through the improper use of artificial intelligence, which negatively impacts the information holder.

Analyzing associated risks such as misinformation, fraud, and invasion of privacy, it explores relevant cases to illustrate the legal and ethical consequences, proposing that regulations should consider better control over the use of artificial intelligence. It is concluded that to combat this crime, interdisciplinary collaboration is essential, combining advances in artificial intelligence with a legal framework from the Comprehensive Organic Penal Code of Ecuador for greater public awareness. The crime of *deepfake* leads to violating the rights of the information's holder by the inappropriate use of Artificial Intelligence. Implementing specific laws that penalize the misuse of *deepfakes* is recommended.

Keywords*: deepfake,* Artificial Intelligence, privacy, right to image, omission.

Índice

Capítulo I

1. Antecedentes

> |Los *deepfake*s aparecieron por primera vez en 2017, uno de los años del boom de las fake news. El usuario de reddit /r/deepfakes publicó sus primeras creaciones pornográficas utilizando algoritmos y librerías de imágenes de libre acceso con resultados asombrosos. En sincronía con la aparición de TikTok y las apps de envejecimiento o rejuvenecimiento facial, la técnica de este usuario anónimo se popularizó y pronto surgió la primera app abierta para incorporar un rostro cualquiera a un video existente. Desde Bolsonaro como el Chapulín colorado hasta Cristina Kirchner como una Drag Queen de Ru Paul, Internet se llenó de videos con propósitos básicamente humorísticos, aunque la abrumadora mayoría seguían siendo pornográficos. (Ansorena, 2020)

Se estima el surgimiento de la *deepfake* en el año de 2017 estableciendo los primeros videos en uso de la imagen de personas ficticias obtenidas por libros, revistas, etc, con finalidades de reproducir videos pornográficos por lo cual con la popularización de aplicaciones como Tik Tok videos con el uso de la imagen de personas genero un gran impacto en la sociedad además que los videos con finalidades pornográficas percisten por el mismo hecho inicio de esa forma.

> La pandemia llevó nuestra relación con las imágenes virtuales a niveles insospechados. Entrevistas laborales, clases, bautismos, consultas médicas, audiencias judiciales, sesiones legislativas, y hasta sexo. La «presencia» es un requisito cada vez más prescindible en los rituales e instituciones que nos constituyen como sociedad. A la inversa, la identidad virtual, su «huella digital», se vuelve cada vez más relevante, y no solo en términos jurídicos sino también prácticos. (Ansorena, 2020)

A inicios de la pandemia por Covid-19, el uso de la imagen en sistemas informáticos y aplicaciones móviles alcanza una gran amplitud ya que el sistema laboral, educativo, medicinal y diferentes ramas que requiera un uso intelectual y práctico en el área digital estableciendo rastros de la determinada "Huella Digital", no obstante, la huella digital consiste en el rastro informático que cada persona al utilizar sistemas informáticos y aplicaciones móviles.

1.2.Conceptos

> El llamado *deepfake* consiste en imágenes o videos que se generan por medio de una técnica de inteligencia artificial. Se trata de un "aprendizaje automático" llamado en inglés deep learning (en español: aprendizaje profundo), explica la Universidad de Virginia (Estados Unidos) en su sitio web. (NATIONAL GEOGRAPHIC, 2023)

El uso de *deepfake*, implica un aprendizaje determinado con herramientas informáticas por lo cual el uso de datos es constante produciendo distintos tipos de videos u imágenes a libre arbitrio de la persona que utiliza los datos para generar el contenido.

> Tal como señala la Enciclopedia Britannica, *deepfake* se compone de dos términos ingleses: deep, que refiere a la inteligencia artificial, un aprendizaje automático que a su vez se compone de muchos niveles de procesamiento; y de fake, que alude a lo falso del material que se obtiene como resultado. (NATIONAL GEOGRAPHIC, 2023)

La etimología de la palabra *deepfake* constituye dos aspectos importantes, en primer orden expresa la palabra "Deep" como: el sistema informático cuyo uso comprende aplicar diferentes técnicas de aprendiza en el uso de la inteligencia artificial correspondiente a generar las imágenes y videos a antojo de quien la use y como la divulgue y en segundo orden la palabra "Fake", que determina que el contenido proporcionado u obtenido proveniente del uso de la inteligencia artificial se determina como falso o inexistente en la vida real ya que estos aspectos son meramente informáticos sea para divulgar aspectos de aprendizaje, entretenimiento u vulgar como pornografía y diferentes aspectos.

> Un *deepfake* es una técnica de inteligencia artificial que se utiliza para crear o alterar contenido audiovisual, el cual se caracteriza por su hiperrealismo y su capacidad para replicar la apariencia y la voz de personas reales. (Sarmiento, 2023)
>
> Tal tecnología puede ser usada en aplicaciones benéficas como el cine, pero también puede usarse con fines malintencionados, como la generación de noticias falsas o difamaciones. (Sarmiento, 2023)

El uso de *deepfake* puede tener usos positivos, como en la industria cinematográfica, también puede ser utilizada de manera perjudicial, como en la creación de información falsa o en difamaciones.

1.3.Ventajas

En lo que respecta al área del cine, se puede volver a la vida a artistas que han fallecido o cambiar el diálogo sin la necesidad de volver a grabar la escena. En el campo del marketing, los casos de Sra. Rushmore y Ogilvy son casos en los que esta tecnología busca enviar un mensaje positivo a la sociedad. En el área de los videojuegos, se busca más inversión para el desarrollo de este tipo de tecnología. (Domínguez, 2021)

- En la industria del cine, existe la capacidad de revivir a artistas fallecidos o modificar diálogos sin necesidad de regrabar escenas.
- En el ámbito del marketing, los casos de Rushmore y Ogilvy son ejemplos donde esta tecnología pretende transmitir un mensaje a la sociedad tomando en consideración que sea positivo.
- Para avanzar el desarrollo de este tipo de tecnología, se está buscando aumentar la inversión en el sector de los videojuegos.

1.4. Desventajas.

La falta de privacidad y respeto hacia las personas, como la creación de videos para mayores de 18 años con la cara de celebridades, es un mal uso de esta tecnología.

Creación de noticias falsas por medio del *deepfake*. No existe un método de autorización por parte de la persona a la cual están suplantando la identidad. Falta de control para detectar si un video utiliza o no este tipo de tecnología. (Sarmiento, 2023)

- La ausencia de privacidad y el irrespeto hacia las personas, como la creación de vídeos que utilizan rostros de celebridades mayores de edad, constituye un abuso de esta tecnología.
- Se generan noticias falsas mediante el uso de *deepfake*s, sin contar con ningún consentimiento por parte de la persona cuya identidad se ve afectada.
- Además, para ello no se deberá tomar en cuenta el método de autorización para los individuos de cuya identidad se muestra, y resulta difícil detectar si un vídeo utiliza esta tecnología.

1.5. Tipos de *deepfake*.

1.5.1. Deep Face.

Los deepfaces son *deepfake*s que consisten en crear imágenes convincentes, aunque completamente falsas, desde cero. Por medio del aprendizaje automático de la inteligencia artificial, se manipulan y generan nuevas imágenes o vídeos a partir de otros y se reemplaza a la persona que aparece en ellos. (Alumnos, LISA Institute, s.f.)

El objetivo es generar diferentes imágenes estáticas para crear una secuencia de vídeo, de modo que, como objetivo final, se obtenga un vídeo falso que parezca 100% real." (Alumnos, LISA Institute, s.f.)

Cuando hacemos referencia a este primer tipo debemos considerar que es el crear imágenes mediante ellas lleven al convencimiento de las personas, aun sabiendo que estas imágenes pueden ser falsas, en este aprendizaje del uso de una inteligencia artificial consiste en remplazar a una persona haciendo que parezcan real ante las personas que sea expuesto.

1.5.2. Deepvoices.

> Este tipo de *deepfake*s suplantan la voz de una persona en un audio, haciendo que parezca que la persona realmente algo que no dijo, ya que falsifican su voz real.
>
> En 2019 se produjo el primer delito cibernético por medio de la inteligencia artificial. Unos cibercriminales hicieron creer, utilizando deepvoices, a un ejecutivo que estaba hablando con el CEO de su empresa, haciendo que les transfiriese más de 250.000 dólares. (Alumnos, LISA Institute, s.f.)

Es aquella suplantación de voz de una persona mediante un audio, así generando que la persona hubiera sido quien manda dicho audio a otra persona. En el año 2019 se dio un primer caso del delito cibernético de "DeepVoice" con el uso de la inteligencia artificial genero un daño a un ejecutivo el cual se presumió que solicito altas cantidades de dinero bordeando los 250.000$ dólares.

1.6. Deepfake en la sociedad.

> El usuario "*deepfakes*" publicó vídeos pornográficos usando los rostros de celebridades como Aubrey Plaza, Gal Gadot, Maisie Williams, Taylor Swift y Scarlett Johansson, consiguiendo popularidad mediante votaciones (Cole, 2017). Aunque omitiendo su verdadera identidad, prestó declaraciones al periódico Vice y explicó que el software buscaba imágenes de varios archivos bibliotecarios abiertos y que, para crear las caras de las celebridades, usó la búsqueda de imágenes de Google, fotos de archivo y vídeos de YouTube (Cole, 2017). El concepto de *deepfake* surge después de la generación de textos automatizados y de la generación de las imágenes falsas. En la primera, con recurso al GPT (transformador generativo pre-entrenado), que es un nuevo modelo de inteligencia artificial, es posible generar textos que pueden ser usados de forma engañosa como siendo escritos por humanos. En la segunda, gracias a las redes generativas antagónicas, se pueden crear rostros de personas que no existen. (Jiménez-Marín, 2022)

El creador de las *deepfake*s, fue reconocido al publicar videos de contenido pornográfico en los que insertaba los rostros de celebridades como Aubrey Plaza, Gal Gadot, Maisie Williams, Taylor Swift y Scarlett Johansson el individuo alcanzó notoriedad mediante la votación del público (Cole, 2017), la información obtenida corresponde a librerías, búsqueda de imágenes de libre acceso además de ser obtenida en plataformas como YouTube, Facebook, X, por consiguiente con la creación de "GPT" la herramienta de la inteligencia artífica crece potencialmente en la sociedad.

1.7. La inteligencia artificial.

1.7.1. Concepto.

La inteligencia artificial (IA) es un conjunto de tecnologías que permiten que las computadoras realicen una variedad de funciones avanzadas, incluida la capacidad de ver, comprender y traducir lenguaje hablado y escrito, analizar datos, hacer recomendaciones y mucho más. La IA es la columna vertebral de la innovación en la computación moderna, lo que libera valor para las personas y las empresas. Por ejemplo, el reconocimiento óptico de caracteres (OCR) usa la IA para extraer texto y datos de imágenes y documentos, y convierte el contenido no estructurado en datos estructurados listos para las empresas, además de brindar estadísticas valiosas (Cloud, s.f.)

La inteligencia artificial (IA) comprende un conjunto de tecnologías que capacitan a las computadoras para realizar diversas funciones avanzadas, como la capacidad de comprender y traducir tanto el lenguaje hablado como escrito, analizar datos, ofrecer recomendaciones y más. (Cloud, s.f.)

La Inteligencia Artificial (IA) constituye el motor principal de la innovación en la informática contemporánea, generando valor tanto para individuos como para empresas. Por ejemplo, el reconocimiento óptico de caracteres (OCR) emplea Inteligencia Artificial (IA) para extraer texto y datos de imágenes y documentos, transformando contenido no

> estructurado en datos organizados que resultan útiles para las empresas, así como proporcionando estadísticas valiosas. (Cloud, s.f.)
>
> La inteligencia artificial es un campo de la ciencia relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar de una manera que normalmente requeriría inteligencia humana o que involucre datos cuya escala exceda lo que los humanos pueden analizar. (Cloud, s.f.)
>
> La IA es un campo amplio que abarca muchas disciplinas diferentes, incluidas la informática, el análisis de datos y las estadísticas, la ingeniería de hardware y software, la lingüística, la neurociencia y hasta la filosofía y la psicología. (Cloud, s.f.)

La inteligencia artificial comprende un ámbito científico específico en el desarrollo y optimización de computadoras y sistemas que tienen la capacidad de razonar, aprender y tomar decisiones de manera similar a la inteligencia humana, o incluso para utilizar los conjuntos de datos de una escala que sobrepasa la capacidad de análisis humana.

Este campo multidisciplinario abarca diversas áreas como la informática, el análisis de datos, las estadísticas, la ingeniería de hardware y software, la lingüística, la neurociencia, e incluso la filosofía y la psicología.

1.7.2. Evolución.

> Desde la Antigüedad, la especie humana ha soñado con la máquina, con diseñar y construir ingenios que le hicieran más fáciles las tareas más frecuentes. Incluso para el mero entretenimiento se desarrollaron mecanismos autómatas que reproducían figuras de seres vivos y realizaban movimientos de forma repetitiva. A finales del siglo XV personajes como Leonardo da Vinci esbozaron nuevos artificios, pero no consta que llegaran a materializarse. En cambio, en el XVII y XVIII no solo se proyectaron, si no que se construyeron. Fue finalmente en el XX cuando la robótica comenzó a extenderse enfocada hacia la actividad industrial. (ENAE, s.f.)

Desde tiempos antiguos, la humanidad ha imaginado la creación de máquinas para facilitar sus quehaceres cotidianos. Incluso se idearon autómatas para el simple entretenimiento, imitando movimientos de seres vivos. Aunque figuras como Leonardo da Vinci esbozaron ideas innovadoras en el siglo XV, no hay evidencia de que se materializaran. Sin embargo, en los siglos XVII y XVIII, no solo se concebían estas máquinas, sino que también se construían. Fue en el siglo XX cuando la robótica empezó a expandirse, principalmente en el ámbito industrial.

> Además de la industria, las máquinas, transformaron otras actividades económicas y de la vida más allá de lo laboral. Y sin embargo, la auténtica revolución se produjo cuando el hombre afrontó el reto de aportar a los ingenios la capacidad de aprender, de razonar como podría hacerlo la especie humana, sacar sus propias conclusiones y actuar de forma autónoma. (ENAE, s.f.)
>
> Muy lejos de imaginar a los robots humanoides de las películas de ficción, la ciencia –especialmente la informática- ha desarrollado otros ‘cerebros’. Pero vayamos por partes. La palabra robot tiene un origen checo y el primero en utilizarla fue el escritor Karel Capek en 1921 (ahora se cumple un siglo de su acuñación) y en su lengua original significa servidumbre o trabajo forzado. (ENAE, s.f.)

La inteligencia artificial al impactar en la industria, las máquinas también han transformado otras áreas económicas y aspectos de la vida más allá del trabajo. Sin embargo, la verdadera revolución surgió cuando la humanidad se enfrentó al desafío de dotar a estas máquinas con la capacidad de aprender y razonar, similar a la capacidad humana, permitiéndoles sacar conclusiones por sí mismas y actuar de manera autónoma.

Aunque las representaciones de robots humanoides en películas de ficción están muy alejadas de la realidad, la ciencia, especialmente la informática, ha creado otros tipos de "cerebros" para estas máquinas.

Ahora bien, en cuanto al origen de la palabra "robot", esta proviene del checo y fue utilizada por primera vez por el escritor Karel Capek en 1921 (se está cumpliendo un siglo desde su acuñación). En su idioma original, la palabra significa servidumbre o trabajo forzado. Por lo tanto, un robot se define como aquel destinado a realizar las tareas más arduas en servicio del ser humano.

1.7.3. Características.

Cuadro 1

Aprendizaje automático Cuenta con algoritmos y modelos que permiten a las máquinas aprender y realizar tareas sin ser programadas de forma explícita.	**Automatización** Es la capacidad de las máquinas de realizar tareas sin la necesidad de intervención humana.
Ingestión de datos Es la adquisición de conocimiento desde fuentes como bases de datos, archivos, sensores, dispositivos móviles y redes sociales.	**Análisis de datos** Examina, transforma y modela datos para descubrir patrones y tendencias útiles para la toma de decisiones.
Almacenamiento en la nube Permite acceder a recursos de hardware y software a través de	**Procesamiento del lenguaje natural** Procesan el lenguaje humano por medio de tendencias y keywords para proveer

internet. En vez de contar con instalaciones locales, los recursos se encuentran en servidores remotos.	respuestas automáticas en función de la conversación o solicitud del usuario.

Fuente; (Londoño, 2023)

En el presente cuadro 1 encontramos algunas características del *deepfake*, en **primer orden** posee un aprendizaje autónomo en relación a que el sistema de forma automática y sistematizada puede gestionar la acción de diferentes mandos que se ordene con la capacidad de aprender lo que realiza, en un **segundo orden** encontramos la automatización refiriéndose a que no necesita de la interacción humana para gestionar sus actividades, en **tercer orden** encontramos la ingestión de datos, refiriéndose a que adquieren información y la almacenan en su base de datos con la finalidad de gestionar la información y usarla cuando sea el caso, en un **cuarto orden**, encontramos al análisis de datos refiriéndose a la toma de decisiones que va a realizar con la información proporcionada, en un **quinto orden** encontramos a almacenamiento en la nube que permite guardar la información obtenida y utilizarla mediante el uso de internet y en un **sexto orden** encontramos el procesamiento de lenguaje natural, relacionándose directamente con la interacción del sistema y la persona para la obtención de respuestas.

1.7.4. ¿Cuál es el funcionamiento de la inteligencia artificial?

> Las Inteligencias artificiales utilizan algoritmos y modelos matemáticos para procesar grandes cantidades de datos y tomar decisiones basadas en patrones y reglas establecidas a través del aprendizaje automático, que es la capacidad de una máquina para aprender de forma autónoma a partir de datos sin ser programada específicamente para hacerlo. De esta manera la Inteligencia artificial, puede mejorar su precisión y eficiencia con el tiempo. (Resilencia, 2023)

Las inteligencias artificiales emplean algoritmos y modelos matemáticos para analizar extensas cantidades de datos y tomar decisiones fundamentadas en patrones y reglas predefinidas,

utilizando el aprendizaje automático. Este último se refiere a la habilidad de una máquina para aprender de manera autónoma a partir de datos, sin requerir una programación específica para ello. De este modo, la inteligencia artificial puede perfeccionar su precisión y eficacia a medida que pasa el tiempo.

Ejemplos

Las compras en línea y la publicidad se benefician de la inteligencia artificial para generar recomendaciones personalizadas, mejorar los productos, planificar el inventario y optimizar los procesos logísticos, entre otras funciones.

Los motores de búsqueda utilizan los datos proporcionados por los usuarios para ofrecer resultados de búsqueda relevantes, aprendiendo y ajustando sus algoritmos continuamente.

Los asistentes personales digitales en los smartphones aprovechan la inteligencia artificial para brindar servicios personalizados y mejorar la experiencia del usuario.

Los programas de traducción de idiomas, tanto escritos como hablados, se basan en la inteligencia artificial para ofrecer y perfeccionar las traducciones. Además, la Inteligencia Artificial, se utiliza en otras aplicaciones como el subtitulado automático.

1.7.5. Propósito de la inteligencia artificial según los tipos.

Cuadro 2

Tipos	**Propósito**
Machine Learning (aprendizaje automático)	*"Es la capacidad que tiene una inteligencia artificial para aprender por sí misma. Se basa en un ciclo de aprendizaje a partir de datos, entrenamiento y resultados. Existen varios subtipos en función de si su aprendizaje requiere la supervisión de un ser humano o se permite que la IA aprenda de forma autónoma, según*

	unas reglas establecidas. Se suele utilizar en asistentes virtuales y chatbots, entre otros."
Deep Learning (aprendizaje profundo)	*"Su objetivo es recrear la forma en la que aprenden los humanos a través de lo que se denominan redes neuronales, que consisten en nodos interconectados que emulan la red de neuronas de un cerebro humano. Se emplea, por ejemplo, en la búsqueda de productos basada en imágenes."*
Natural Language Processing (procesamiento del lenguaje natural)	*"Investiga la manera en que las máquinas se comunican con las personas, con el objetivo de lograr que aquellas comprendan y extraigan la información relevante. Sus aplicaciones son múltiples, desde el análisis de sentimiento u opinión hasta la anonimización de documentos, pasando por el entrenamiento de chatbots."*
Knowledge Graph (grafo de conocimiento)	*"El grafo es una manera de representar relaciones entre entidades y crear vínculos entre datos y metadatos. Cuando el contenido de los grafos se enriquece y se logra que realicen un procesamiento automático «inteligente» de los datos, se convierten en grafos de conocimiento. Son muy populares en sistemas de organización de la información."*
Augmented Reality (realidad aumentada)	*"Se trata de un conjunto de tecnologías que permiten que el usuario interactúe con el mundo real mediante dispositivos que añaden información gráfica virtual, de modo que el usuario ve al mismo tiempo el mundo que le*

> *rodea, pero con objetos virtuales superpuestos. Se utiliza en un amplísimo número de aplicaciones, desde operaciones hasta pruebas virtuales de colores de maquillaje o recreaciones de cómo quedará un mueble determinado en tu hogar."*

Fuente, (¿Qué es la inteligencia artificial y cómo nos ayuda?, 2023)

El cuadro 2 expresa los tipos de *deepfake* y su finalidad siendo en **primer orden** el Machine Learning expresando que la inteligencia artificial puede aprender por sí misma en base a los datos que adquiere y puede variar sus funciones ya que está destinada para el aprendizaje y entretenimiento del usuario, en **segundo orden** encontramos la Deep Learnign cuya finalidad es revivir lo que el usuario en su pensamiento lo idealiza en relación a los estímulos neurosensoriales que poseemos, en **tercer orden** encontramos la Natural Languaje Processing relacionando que los sistemas se relaciona con la persona intrínsecamente para la obtención de información que proporciona y determinar la finalidad que busca como un ejemplo expreso es el uso de chat boot que determina la finalidad para la que le usuario la utiliza, en **cuarto orden** encontramos a Knowledge expresando que su finalidad es relacionar los datos y metadatos para un mejor rendimiento de la información, y en un **quinto orden** encontramos la Augmented Reality, que se relaciona en diversas herramientas tecnológicas por la cual el ser humano puede interactuar en relación a la sistematización para generar hipotéticamente modelos que se desea.

Ahora bien, cuando hablamos sobre el propósito que quiere cumplir el uso de la inteligencia artificial es importante tomar en consideración que existe la presencia de una capacidad en la que se basa en un ciclo de aprendizaje para las personas que tengan un dominio de redes neuronales para generar una búsqueda u investigación de la máquina de comunicación como de igual forma establecer un vínculo con los datos y metadatos con junto con la sociedad.

Pues bien, haciendo que se comprenda u extraiga la información que se tenga en un rango con más relevancia; presenciando la relación que se da entre entidades para que se tenga un dominio sobre el conjunto de dicha tecnología la cual ha llegado a grandes avances para que se llegue a interactuar con las personas que conforman dicha sociedad.

1.7.6. ¿Cuáles son las posibles consecuencias favorables?

> La tecnología *deepfake* se desarrolló originalmente a partir del trabajo del científico informático Ian Goodfellow en redes generativas adversas (GAN). Las GAN generan imágenes convincentes mediante un algoritmo en el que dos GAN intentan "engañarse" entre sí para que piensen que una imagen es "real". Hoy en día, las GAN pueden recrear de manera convincente a una persona utilizando solo un videoclip suyo. (Deepfakes: ¿Cuáles son los potenciales impactos positivos?, 2020)
>
> Existe una extendida preocupación por el incremento exponencial de las expresiones de *deepfake*, realizadas con programas de inteligencia artificial cada vez más accesibles y fáciles de usar, al alcance de cualquiera que quiera producirlos con fines de entretenimiento, acoso, chantaje, propagandísticos, para construir una política o para generar fake news." (Deepfakes: ¿Cuáles son los potenciales impactos positivos?, 2020)

Los algoritmos compiten para generar imágenes convincentes, lo que resulta en una creación de imágenes que pueden engañar incluso a observadores humanos. Hoy en día, estas GAN pueden recrear de manera sorprendentemente realista a una persona utilizando solo un videoclip suyo como referencia.

Sin embargo, el texto también señala una creciente preocupación debido al aumento exponencial en la creación y difusión de *deepfake*s. Esto se debe a la accesibilidad y facilidad de uso de los programas de inteligencia artificial, que ahora están al alcance de cualquier persona que desee producirlos. Esta tecnología se utiliza para una variedad de propósitos, desde entretenimiento hasta actividades maliciosas como el acoso, chantaje, propagandísticos,

manipulación política y la creación de noticias falsas. Esta preocupación surge debido al potencial de los *deepfake*s para socavar la confianza en la información y afectar negativamente a individuos, instituciones y sociedades enteras.

> Las principales preocupaciones provienen del ámbito de los medios de información, medios y plataformas digitales, redes sociales, los ámbitos del poder político, la legislación, la ética y la tecnología. Los *deepfake*s, entendidos como documentos falsos o falsificados que se hacen pasar por auténticos, pueden tener un amplio e irreversible alcance mediático. Estas preocupaciones se fundan en el hecho de que los *deepfake*s minan la credibilidad de los documentos audiovisuales, principalmente vídeos, como medios de información o certificación de hechos, que ponen en entredicho su veracidad o generan riesgos de desinformación, difamación o chantaje social. (Deepfakes: ¿Cuáles son los potenciales impactos positivos?, 2020)

Las principales inquietudes se originan en áreas como los medios de comunicación, las plataformas digitales, las redes sociales, el ámbito político, la legislación, la ética y la tecnología. Las *deepfake*s, que son documentos audiovisuales falsificados que se presentan como auténticos, pueden ganar una exposición amplia e irreversible en los medios. Estas preocupaciones se fundamentan en el hecho de que los *deepfake*s erosionan la confiabilidad de los medios audiovisuales, especialmente los vídeos, como herramienta para transmitir información o verificar hechos. Se plantea la duda sobre su autenticidad y se genera un riesgo de desinformación, difamación o extorsión social.

1.8. Objeto y finalidad de la Ley de Protección de Datos Personales en Ecuador.

> Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para

> dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela (Nacional, Ley Organica de la Ley de Protección de Datos Personales, 2021)

Implica que las personas tienen el derecho de acceder a su información personal, tomar decisiones sobre ella y que dicha información esté protegida adecuadamente, la ley establecerá normas y procedimientos que deben seguir tanto los individuos como las entidades que manejan datos personales, y proporcionará mecanismos para garantizar que se cumplan estos requisitos y que se protejan los derechos de las personas en relación con sus datos personales.

> Art. 66.- Se reconoce y garantizará a las personas:
>
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la Decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (Constituyente, 2008)

La constitución de la republica garantiza dos finalidades en primer orden el **acceso** que posee cada uno de los titulares de su información y en un segundo orden encontramos la **protección** cual garantiza el acceso y la decisión de los titulares para su debida protección ante accesos no autorizados por terceras personas.

La recolección y procesamiento de la información requiere el consentimiento previo del titular, no obstante, las entidades que recopilan, almacenan, procesan, distribuyen o divulgan datos personales deben obtener el consentimiento de la persona a la que pertenecen esos datos, o deben actuar de acuerdo con lo que establece la ley. Este requisito protege la privacidad y los derechos de las personas en relación con sus datos personales.

Capítulo II

2. Finalidad del Código Orgánico Integral Penal (COIP)

> Art. 1.- Finalidad. - Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas. (Nacional, Código Orgánico Integral Penal, 2024)

La finalidad es regular y limitar el poder punitivo del Estado para sancionar a las personas que cometan infracciones penales constituyendo así los delitos correspondiendo a que se considera delito y que no tomando en cuenta el entorno social para determinar lo que se considera delito, el Estado garantiza el derecho a la defensa de la persona que presuntamente haya cometido una infracción penal para garantizar un proceso penal adecuado en base al debido proceso, la función principal del Estado es reinsertar al infractor penal en la sociedad con la garantía de que este no volverá a cometer ninguna infracción considerando que debe responder por la reparación integral de la víctima o victimas que se haya determinado en la infracción.

2.1. Tipo penal.

Se toma en consideración una estructura en la que se presenta un supuesto hecho y sobre todo la consecuencia jurídica. Dentro del caso de las leyes en un esquema el cual el hecho se puede llegar a convertir en un comportamiento mediante el cual lo describe ya que debemos entender que la ley es la que manda o prohíbe y es de importancia llegas a considerar la presencia de una consecuencia jurídica de la pena se puede considerar en un caso de la existencia del cumplimiento con un comportamiento.

Para esto es de importancia que la ley en general tiene muchos caracteres entre ellos tenemos a los siguientes:

a. **Exclusiva:** se busca a establecer de una manera taxativa o específica del hecho que pasan en las dichas circunstancias, así surgiendo una pretensión punitiva por parte del Estado.
b. **Obligatoria**: debe de cumplir cada uno de los requisitos para atacar como es debido.
c. **Irrefragable:** se llega a derogar solamente por una modificación generada por otra norma.
d. **Igualitaria**: una aplicación a todas las personas de manera igual con la constitución aplicando justicia según la norma.

Ahora se identifica el comportamiento de las personas para así llegar a decidir supuesto delito, ya que es un instrumento de lógica para así predominar de manera descriptiva de conductas detalladas la cual presenta una descripción hasta un punto de analizar cada uno de los puntos.

2.2.Función del tipo penal.

Se lo debe de considerar una valoración, para esto se existe la presencia de una relación antijuridica en la que se contempla en el ordenamiento jurídica, así considerando los distintos tipos, entre ellos tenemos:

a. **Función de garantía:** cuando en la normativa se encuentra escrito. Así solamente llega a cumplir una sanción de dicho hecho, tomando en consideración que se llegue a una aplicación del principio de legalidad considerando como un límite a determinadas comisiones. Para este tipo es importante que la conducta se dispone de la manera adecuada para esto se usa el lenguaje adecuado según lo indica la ley.
b. **Función indiciaria:** se toma una descripción de las acciones antijuridica en la que nos permita dar una buna selección referente entre ilícito punibles y los que no son punibles; así como determinar dicho juicio para un carácter antijuridico.

c. **Función sistemática:** en la que todos los elementos forman parte particular de un delito llegando a describir según la medida de los limites en los sujetos los cuales intervienen una relación causal.

2.3.Delito.

Desde un enfoque formal, se considera delito a la transgresión de una norma penal específica. Sin embargo, esta definición limitada no proporciona una comprensión completa de las características reales del delito. Entre los numerosos intentos de definir el delito desde una perspectiva sustantiva, sobresale la concepción que lo vincula con la conducta que causa daño socialmente. Aunque esta noción es bastante abstracta, es innegable que, para un sistema legal penal basado en los principios examinados en el primer módulo, el concepto de daño social debe ser fundamental para considerar una conducta como delictiva.

2.4.Delito de Deepfake.

> El término "*deepfake*" resulta de una combinación de dos palabras "deep" ("profundo", pero con origen en deep learning) y "fake" (falso). Los *deepfake*s son medios visuales o de audio manipulados o sintéticos que parecen auténticos, y que presentan a personas que parecen decir o hacer algo que nunca han dicho o hecho, producidos mediante técnicas de inteligencia artificial, como el aprendizaje automático (machine learning) y el aprendizaje profundo (deep learning) (Djurre et al., 2021). (Goncalves, 2022)

La terminología de *deepfake* procede de dos terminologías siendo la palabra "Deep", que significa aprendizaje profundo este tipo de aprendizaje toma en consideración la creación automática de algoritmos permitiendo la creación de figuras y la palabra "Fake" que se considera como "falso", esta combinación es el resultado de la producción de videos con el uso de la inteligencia artificial como fuente generadora.

> Un *deepfake* es un vídeo que superpone la cara de una persona en el cuerpo de otra, algo posible gracias a algoritmos gratuitos y fáciles de usar (Cerdán Martínez y Padilla Castillo, 2019). (Goncalves, 2022)

La finalidad del uso del "*deepfake*" es utilizar la imagen de personas en otras para así plasmar videos arbitrarios creados por las personas y de forma gratuita determina la creación masiva de los videos, un ejemplo común de *deepfake* es un video que sobrepone el rostro de una persona sobre el cuerpo de otra, siendo posible gracias a algoritmos gratuitos y de fácil acceso.

> Desde el punto de vista de la desinformación, los *deepfake*s, una nueva forma de fake news, permiten cumplir algunos objetivos políticos y financieros de los interesados, por lo que se espera que esta nueva tecnología se convierta en el principal proceso de difusión intencional de bulos, sobre todo porque estos son más devastadores que los falsos contenidos de textos, audios o imágenes (Masood et al., 2021). (Goncalves, 2022)

El *deepfake* es una nueva fuente de desinformación para el público en general por lo cual la generación y producción de los videos falsos en parte posee finales políticos y financiero por la promoción y divulgación al público en general.

En los últimos tiempos, ha habido un notable avance en la generación de *deepfakes*, especialmente en cuanto a la producción de videos y audios sintéticos mediante inteligencia artificial. Estos pueden ser empleados para propagar desinformación a nivel global, especialmente a través de las plataformas de redes sociales, lo que podría representar en el futuro una seria amenaza en forma de noticias falsas; se anticipa que esta innovadora tecnología se convierta en el principal medio de difusión deliberada de información errónea, especialmente debido a su capacidad para causar un impacto más perjudicial que los contenidos falsos basados en texto, audio o imágenes estáticas.

2.5.Teoría de la Posverdad y DeepFakes.

> La posverdad tiene un rango de mediación variable, se sirve de mecanismos de viralización de información y articula la intervención de líderes de opinión, celebridades, actores políticos relevantes, medios electrónicos y digitales de información, comunidades en plataformas digitales y redes sociales. Podríamos decir que existe una arquitectura mediática de la posverdad, empleada en hacer creer que documentos falsos son auténticos y los *deepfakes* engranan perfectamente en esta arquitectura. (Carrera, 2018)

La posverdad se apoya en una amplia gama de medios para difundir información, utilizando estrategias de viralización y la participación de figuras influyentes como líderes de opinión, celebridades y políticos destacados, así como medios de comunicación electrónicos y digitales, comunidades en plataformas en línea y redes sociales. Esta forma de comunicación construye una estructura mediática que busca persuadir al público haciendo pasar documentos falsos como verídicos, donde los *deepfake*s se integran de manera perfecta en esta dinámica.

2.6.DeepFake pornográfico.

> Los ataques hechos con *deepfakes* pornográficos se centran en mujeres, músicos, actores y las nacionalidades de estos personajes son británicos, surcoreanos, norteamericanos e israelíes en mayor medida (Ajder, 2019). Los *deepfakes* porno, no sólo atacan a celebridades como Scarlett Johansson, Gal Gadot, Taylor Swift, Maisie Williams, Jessica Alba o periodistas como Rana Ayyub o Bharatiya Janata, sino que involucran a personalidades privadas con fines de extorsión. La suma de avatars y *deepfakes* porno dará la posibilidad de hacer una industria de este género a la carta y aumentará los riesgos de acoso y chantaje en los próximos años. (Carrera, 2018)

Los ataques de *deepfakes* pornográficos se dirigen predominantemente a mujeres, incluyendo a músicos y actores, y destaca que las nacionalidades más afectadas son británicas, surcoreanas,

norteamericanas e israelíes, según Ajder. Estos *deepfake*s no solo afectan a celebridades como Scarlett Johansson, Gal Gadot, Taylor Swift, Maisie Williams y Jessica Alba, así como a periodistas como Rana Ayyub y Bharatiya Janata, sino que también se utilizan para extorsionar a personas privadas. La combinación de avatares y *deepfake*s pornográficos puede dar lugar a una industria personalizada de este tipo de contenido.

2.7.Deep Fake político.

> El campo discursivo más propiamente mediático es el dedicado a los *deepfakes* de políticos, ya que adquiere eco en medios electrónicos y digitales. Los personajes más relevantes en este campo son en 2018- 2019 Donald Trump, Barack Obama, Vladimir Putin y Nancy Pelosi. (Carrera, 2018)

Los *deepfake* políticos toman relación a su uso de imagen con la finalidad de promover contenido relacionado a su partido político en cuando a las conferencias discursos que exponen en sus labores.

Esquema 1

Esquema 1. Escenario socio-mediático del *deepfake*.
Elaboración propia, 2020.

Fuente; (Carrera, 2018)

En el presente esquema 1 expone los diferentes tipos de *deepfake* que se presentan en diferentes ámbitos y actividades exponiendo que este delito se encuentra no solo en el ámbito de medios digitales que por regla general se encuentran en contenido pornográfico y en el uso de redes sociales.

2.8. Problemas legales.

> Como los *deepfakes* fueron usados inicialmente para vídeos falsos de cariz pornográfico, y luego para campañas políticas esencialmente difamatorias, inmediatamente se levantaron varios problemas legales sobre su utilización (Kugler & Pace, 2021). (Goncalves, 2022)

Los *deepfakes* se utilizaron inicialmente para crear videos pornográficos falsos y, posteriormente, para publicidad políticas difamatorias. Esto degenera una serie de problemas legales relacionados con su uso.

2.9.Legislación y ética del DeepFake.

> La evolución legal ante el *deepfake* ha sido lenta. Existen iniciativas y advertencias legales realizadas principalmente en el marco legal estadounidense. Algunas plataformas como Reddit, YouTube y Facebook comienzan a incluir en su política de publicación cláusulas que prohíben la difusión de *deepfakes*. Sin embargo, los *deepfakes* maliciosos que persiguen fines de extorsión, chantaje, acoso, o fines comerciales principalmente difundidos en sitios pornográficos, se extienden sin control legal o con anuencia de la administración de las plataformas. (Alumnos, LISA Institute, s.f.)

> La evolución legal ante el *deepfake* ha sido lenta. Existen iniciativas y advertencias legales realizadas principalmente en el marco legal estadounidense. Algunas plataformas como Reddit, YouTube y Facebook comienzan a incluir en su política de publicación cláusulas que prohíben la difusión de *deepfakes*. Sin embargo, los *deepfakes* maliciosos que persiguen fines de extorsión, chantaje, acoso, o fines comerciales principalmente

> difundidos en sitios pornográficos, se extienden sin control legal o con anuencia de la administración de las plataformas. (Alumnos, LISA Institute, s.f.)

La progresión legislativa frente al fenómeno del *deepfake* ha sido gradual. Se han visto iniciativas y advertencias legales, mayormente dentro del marco jurídico estadounidense. Algunas plataformas como Reddit, YouTube y Facebook están empezando a incorporar cláusulas en sus políticas de publicación para prohibir la difusión de *deepfakes*. Sin embargo, los *deepfakes* malintencionados, que tienen como objetivo la extorsión, el chantaje, el acoso o propósitos comerciales, y que principalmente se difunden en sitios pornográficos, continúan propagándose sin un control legal efectivo o con la aprobación tácita de la administración de las plataformas.

2.10. Efectos.

> Es indudable que el sector jurídico se enfrenta hoy a una revolución sin precedentes, en la que tecnologías como la inteligencia artificial tiene un peso cada vez mayor en nuestras vidas. Su uso, en paralelo al auge de las redes sociales, ha favorecido el surgimiento de distintos fenómenos que plantean importantes retos desde un punto de vista legal, como las fake news y más recientemente, los *deepfakes*. (Díez, 2021)

En el área judicial el uso de los diferentes tipos de herramientas informáticas como el uso de redes sociales, inteligencia artificial ha concatenado una serie de cambios drásticos en la sociedad considerando las diferentes perspectivas jurídicas, la creación de contenido inapropiado altera la perspectiva cognitiva de la sociedad sin poder considerar que el contenido difundido sea real u ficticio o denominados como “fake news” y los llamados “*deepfakes*”.

> Una de las consecuencias legales más importantes de esta práctica es la vulneración al derecho fundamental al honor de la persona afectada, así como la constitución de delitos de injurias o calumnias. La libertad de expresión no es un derecho absoluto, teniendo sus límites en los preceptos de las leyes que lo desarrollan, en el derecho al honor, a la

> intimidad, a la propia imagen y en la protección de la juventud y la infancia. (Díez, 2021)

Tenemos que tener en cuenta que tiene consecuencias en el campo legal en las que con el uso de la inteligencia artificial las personas se ven expuestas a una vulneración de los derechos esenciales, por ello se constituye un delito a los derechos a la intimidad, honra, ante la publicación de video y su difusión como efecto principal al daño social de la persona frente a su derecho a la imagen en su desarrollo personal.

> Si bien la legislación española no regula específicamente la producción y difusión de *deepfakes*, la Comisión Europea ya ha presentado un borrador de Reglamento de IA que se discutirá en el Parlamento Europeo en los próximos meses para armonizar su uso, estableciendo normas de transparencia para los sistemas de IA destinados a interactuar con personas físicas y los utilizados para generar o manipular contenidos de imagen, audio o vídeo. (Díez, 2021)

La legislación española no posee una regulación del delito de *deepfake*, no obstante, la Comisión Europea ostentó un proyecto de ley ante el reglamento del uso de la inteligencia artificial cuyo objetivo es establecer la claridad regulatoria y sancionatoria de la inteligencia artificial para evitar manipulaciones indebidas al momento de crear contenido relacionado al *deepfake*.

> Asimismo, países como China y Estados Unidos están incorporando regulaciones sobre el uso de este software, incluyendo penas de hasta un año de prisión y 2.500 dólares de multa en casos de difusiones de vídeos falsos. (Díez, 2021)

Además, que, en los Estados de China y Estados Unidos, son los primeros gobiernos en presentar las primeras regulaciones del uso de la inteligencia artificial expresando en su regulación sanciones como penas de hasta 1 año de prisión y consigo una multa de 2.500 en la difusión y creación del deepfake.

> En nuestra legislación, el derecho de imagen se considera un derecho personal regulado por la Ley Orgánica 1/1982, si bien no se extingue tras el fallecimiento de la persona, sino que se prologa a quien ésta hubiera designado en su testamento, en su defecto a los parientes supervivientes, y en último término, al Ministerio Fiscal con una limitación temporal. (Díez, 2021)

En nuestra legislación, el derecho a la publicidad es un derecho personal, regulado por la ley orgánica 1/1982. Este derecho no termina con la muerte de la persona, sino que pasa a las personas nombradas en el testamento o, en su ausencia, a los familiares sobrevivientes y, en última instancia, al procesamiento y prescripción durante un período de tiempo.

Capítulo 3

3. Principio de legalidad.

> **Art. 5.- Principios procesales. -** El derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, se regirá por los siguientes principios:
>
> **1. Legalidad:** no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas disposiciones legales para integrar. (Nacional, Código Orgánico Integral Penal, 2024)

Para la sanción de un determinado delito el poder punitivo del Estado se guía estrictamente en el principio de legalidad para determinar la tipificación de un delito que se cometa no obstante, el principio de legalidad determina la protección de derechos fundamentales, la seguridad jurídica, para así evitar arbitrariedades que se presume que realice el Estado con su capacidad legal para sancionar todo relacionado siempre y cuando esté tipificado en el Código Orgánico Integral Penal como un delito caso contrario no se determina la capacidad del Estado para sancionar conductas penalmente relevantes.

3.1. Función del principio de legalidad.

Hablando sobre la importancia del principio de legalidad en el cuál es importante que se considere como uno de los pilares fundamentales en lo que tanto como el derecho como la justicia toman un papel fundamental así generando un sistema jurídico para el mundo. Una de sus funciones importantes es dar una garantía sobre el poder punitivo del Estado y cada órgano que forman parte del mismo garantizando la protección de los derechos reconocidos en la constitución evitando arbitrariedades en el sistema penal.

La función penal en la que podemos distinguir entre **Nullum Crimen, Nulla Poena Sine Lege** mediante el cual lo definimos que “no hay crimen ni pena sin ley”, lo cual tiene un significado que si dicha conducta puede llegar a ser considerada delictiva si se encuentra en la ley pero en

el caso de no existir una ley previa a dicha conducta el delito no es considerado y no tiene un castigo como tal; por otro lado tenemos **Proporcionalidad y Legalidad de las Penas** en la que la pena debería ser proporcional a la conducta delictiva que es cometida mediante la legislación.

> Los autores García Sergio y Morales Julieta, dicen que se instala la "legalidad" y se establece al amparo de los progresos de la democracia y los derechos humanos; porque estos permiten “controles sobre la autoridad" y “límites de la libertad". Ya que unos y otros residen en la ley. La voluntad del soberano señala hasta donde puede extenderse la fuerza del poder y el curso libre y responsable de la libertad. (Pila & Caiza, 2022)

Según García Sergio y Morales Julieta, la "legalidad" se consolida gracias a los avances en democracia y derechos humanos. Estos progresos permiten establecer mecanismos de control sobre las autoridades y definir los límites de la libertad individual, todo enmarcado en la ley. La ley, reflejando la voluntad del soberano, determina hasta dónde puede llegar el poder del Estado y cómo debe ejercerse la libertad de manera responsable.

3.2.Infracción penal.

“Art. 18.- Infracción penal. - Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código. “ (Nacional, Código Orgánico Integral Penal, 2024)

La infracción penal en Ecuador compone cuatro aspectos importantes encontrando en primer lugar la **conducta típica**, determinando que las acciones u omisiones de la persona debe coincidir con lo que describe el tipo penal ya que si no coincide la conducta con la infracción penal no se puede sancionar, en segundo orden encontramos el aspecto **antijurídico**, determinando que la conducta de la persona es contraria a derecho ya que implica la violación de un bien jurídico protegido determinado y este ser protegido por la ley, en un tercer aspecto encontramos la **culpabilidad**, este determina que la persona puede ser culpable tanto por acción como por omisión y que dicho acto sea sancionado por la ley y en un cuarto aspecto encontramos la **sanción prevista en el código,** la sanción como su expresión lo indica

corresponde a la sanción que conlleva el acto u omisión cometido por la persona con la finalidad de cometer un delito penal.

3.3.Figura de *deepfake* en Ecuador.

La figura penal del *deepfake* no está reflejada o tipificada en un determinado delito puesto que el estado de Ecuador no lo reconoce como tal pese a la existencia de manipulaciones de videos publicados en internet con el uso de estas alterando la información y/u imagen de las personas afectadas, no obstante, el delito de *deepfake* engloba diferentes delitos que sí se encuentran determinados en el Código Orgánico Integral Penal.

> A nivel internacional tenemos: Hernández (2019) en su investigación titulada La Suplantación de Identidad Cibernética en el Ecuador. Tuvo como objetivo de estudio, determinar que la legislación ecuatoriana no es suficientemente amplia para proteger los derechos de sus habitantes. Enfoque de estudio cualitativo y el corpus analizado fue la Legislación Ecuatoriana y Derecho Comparado en Chile; los instrumentos empleados fueron entrevistas. (de Derecho, s.f.)
>
> Se concluyó que:
>
> Nunca se tomó en cuenta el crecimiento acelerado de la internet y la aparición de nuevas formas de delinquir mediante su uso, por ende, aquellos que están bajo esta jurisdicción no poseen las garantías y seguridades pertinentes para navegar tranquilamente por el ciberespacio. (de Derecho, s.f.)

El estudio realizado por Hernández en 2019, titulado "La Suplantación de Identidad Cibernética en el Ecuador", tuvo como propósito principal evaluar la efectividad de la legislación ecuatoriana en proteger los derechos de los ciudadanos frente a la suplantación de identidad en el ámbito cibernético. Utilizando un enfoque cualitativo, el estudio se centró en analizar tanto la legislación ecuatoriana como el derecho comparado en Chile. Para recopilar datos, se emplearon entrevistas como método principal de investigación.

Como resultado de este análisis, se concluyó que la legislación vigente en Ecuador no está lo suficientemente actualizada ni adaptada para hacer frente al crecimiento rápido de Internet y las nuevas modalidades delictivas asociadas a su uso. Esto significa que los ciudadanos que se encuentran bajo la jurisdicción de estas leyes no cuentan con las garantías necesarias para navegar de manera segura por el ciberespacio, lo que los expone a diversos riesgos y vulnerabilidades en línea.

3.3.1. Derecho a la Intimidad.

> Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
>
> No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (Nacional, Código Orgánico Integral Penal, 2024)

1. **Definición del Delito:**

- Se considera violación a la intimidad cuando una persona realiza cualquiera de las siguientes acciones sin el consentimiento o autorización legal de la persona afectada:

- Acceder

- Interceptar

- Examinar

- Retener

- Grabar

- Reproducir

- Difundir

- Publicar

2. Ámbito de Protección:

- Datos personales

- Mensajes de datos

- Voz, audio y vídeo

- Objetos postales

- Información contenida en soportes informáticos

- Comunicaciones privadas o reservadas

3. Medios de Comisión:

- Cualquier medio utilizado para realizar las acciones mencionadas.

4. Sanción:

- La persona culpable de este delito será sancionada con una pena de prisión de uno a tres años.

5. Excepciones:

1. Participación Personal:

- Las normas no se aplican a la persona que divulgue grabaciones de audio y vídeo en las que ella misma interviene personalmente. Esto significa que, si alguien graba una conversación o un evento en el que está participando y luego lo divulga, no estará cometiendo el delito de violación a la intimidad.

2. Información Pública:

- Las normas tampoco se aplican cuando se trata de información pública según lo previsto en la ley. Esto implica que, si la información ya es de acceso público conforme a la legislación vigente, su divulgación no constituye una violación a la intimidad.

3.3.2. Honra.

> Art. 182.- Calumnia. - La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años. (Nacional, Código Orgánico Integral Penal, 2024)
>
> No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.
>
> No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo. (Nacional, Código Orgánico Integral Penal, 2024)
>
> No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye

una forma de aceptación de culpabilidad. (Nacional, Código Orgánico Integral Penal, 2024)

1. **Definición del Delito**:
    - Se considera calumnia cuando una persona realiza una falsa imputación de un delito en contra de otra persona por cualquier medio.
2. **Sanción**:
    - La persona culpable de calumnia será sancionada con una pena de prisión de seis meses a dos años.

3.4.2.1. Excepciones y Aclaraciones:

1. **Pronunciamientos ante Autoridades**:
    - No constituyen calumnia las imputaciones hechas ante autoridades, jueces y tribunales cuando estas se realizan en el contexto de la defensa de una causa. Esto significa que, durante un proceso judicial o administrativo, si una persona hace una imputación como parte de su defensa, no se considerará calumnia.
2. **Prueba de Veracidad**:
    - No será responsable de calumnia quien pueda probar la veracidad de las imputaciones. Si la persona que hizo la imputación demuestra que lo dicho es cierto, no será sancionada por calumnia.
    - Sin embargo, no se admitirá prueba de veracidad sobre la imputación de un delito que ya ha sido objeto de una sentencia ratificatoria de la

inocencia del procesado, de sobreseimiento o archivo. Esto significa que, si un tribunal ya ha declarado la inocencia del acusado o ha cerrado el caso, no se puede presentar prueba para justificar la imputación del delito.

3. **Retractación Voluntaria**:

    - No habrá responsabilidad penal si el autor de las calumnias se retracta voluntariamente antes de que se dicte sentencia ejecutoriada (definitiva).
    - La retractación debe cumplir con ciertos requisitos:
        - Debe hacerse antes de la sentencia ejecutoriada.
        - La publicación de la retractación debe ser a costa del responsable.
        - Debe hacerse en el mismo medio y con las mismas características en que se difundió la imputación.
    - La retractación no constituye una forma de aceptación de culpabilidad. Esto significa que retractarse no implica admitir que se cometió calumnia, sino que se está corrigiendo la afirmación falsa.

3.3.3. Carácter Sexual.

Art. 172.1.- Extorsión sexual. - La persona que, mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo, será sancionada con pena privativa de libertad de tres a cinco años. (Nacional, Código Orgánico Integral Penal, 2024)

1. **Definición del Delito**:

    - Se considera extorsión sexual cuando una persona utiliza violencia, amenazas o chantaje para inducir, incitar u obligar a otra persona a exhibir su cuerpo desnudo, semidesnudo o en actitudes sexuales.

2. **Propósito del Delito**:

    - El objetivo de la extorsión sexual es obtener un provecho personal o para un tercero, que puede ser de carácter sexual o de cualquier otro tipo.

3. **Métodos Utilizados**:

    - Violencia: Uso de fuerza física para coaccionar a la víctima.
    - Amenazas: Uso de advertencias de daño para coaccionar a la víctima.
    - Chantaje: Uso de presión psicológica o emocional, generalmente basada en la amenaza de revelar información perjudicial, para coaccionar a la víctima.

4. **Sanción**:

    - La persona culpable de este delito será sancionada con una pena de prisión de tres a cinco años.

3.3.4. Publicación sexual de videos.

Art. 172.1.- Extorsión sexual. - (Agregado por el Art. 9 de la Ley s/n R.O. 526-4S, 30-VIII-2021). - La persona que, mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de

cualquier otro tipo, será sancionada con pena privativa de libertad de tres a cinco años. (Nacional, Código Orgánico Integral Penal, 2024)

1. **Definición del Delito**:

    - Se considera extorsión sexual cuando una persona utiliza violencia, amenazas o chantaje para inducir, incitar u obligar a otra persona a exhibir su cuerpo desnudo, semidesnudo o en actitudes sexuales.

2. **Propósito del Delito**:

    - El objetivo de la extorsión sexual es obtener un provecho personal o para un tercero, que puede ser de carácter sexual o de cualquier otro tipo.

3. **Métodos Utilizados**:

    - Violencia: Uso de fuerza física para coaccionar a la víctima.
    - Amenazas: Uso de advertencias de daño para coaccionar a la víctima.
    - Chantaje: Uso de presión psicológica o emocional, generalmente basada en la amenaza de revelar información perjudicial, para coaccionar a la víctima.

4. **Sanción**:

    - La persona culpable de este delito será sancionada con una pena de prisión de tres a cinco años.

3.3.5. Difusión de imagen.

Art. 179.- Revelación de secreto o información personal de terceros. - (Sustituido por el Art. 11 de la Ley s/n R.O. 526-4S, 30-VIII-2021). - La persona que, teniendo

conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación cause daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año. No habrá delito en aquellos casos en que el secreto divulgado verse sobre asuntos de interés público.

Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad. (Nacional, Código Orgánico Integral Penal, 2024)

1. **Primera Situación**: Revelación de secretos por razón de estado, oficio, empleo, profesión o arte
    - **Definición del Delito**:
        - Se considera delito cuando una persona, debido a su posición, oficio, empleo, profesión o arte, tiene conocimiento de un secreto cuya divulgación puede causar daño a otra persona y lo revela.
    - **Sanción**:
        - La persona culpable de este delito será sancionada con una pena de prisión de seis meses a un año.
    - **Excepción**:
        - No se considera delito si el secreto divulgado se refiere a asuntos de interés público. Esto implica que, si la información

revelada tiene relevancia para la sociedad en general, la divulgación no será penalizada.

2. **Segunda Situación**: Revelación o divulgación de contenido íntimo de carácter sexual
    - **Definición del Delito**:
        - Se considera delito cuando una persona revela o divulga a terceros contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de otra persona en contra de su voluntad.
    - **Sanción**:
        - La persona culpable de este delito será sancionada con una pena de prisión de uno a tres años.

El texto establece dos tipos de delitos relacionados con la revelación de secretos o información personal:

1. **Revelación de secretos por razón de posición profesional**:
    - Este delito ocurre cuando alguien, debido a su posición profesional, revela un secreto que causa daño a otra persona. La sanción es de seis meses a un año de prisión, con la excepción de que la revelación no es punible si se trata de asuntos de interés público.
2. **Revelación de contenido íntimo de carácter sexual**:

- Este delito ocurre cuando alguien revela contenido íntimo de carácter sexual sin el consentimiento de la persona afectada. La sanción es de uno a tres años de prisión.

- Una vez analizado los tipos penales que engloban el delito de *deepfake* determinamos que existe una protección determinada de la información personal, no obstante, el Ecuador, no adopta medidas adecuadas para poder plantear la regulación del Delito de *deepfake*.

> El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana. (Del deepfake sexual, s.f.)

Derecho a la propia imagen es una protección legal diseñada para garantizar que cada persona tenga un espacio personal y reservado que esté libre de la intrusión y el conocimiento no deseado por parte de otros teniendo el control de su imagen ante su desarrollo integro y personal para su bienestar.

3.4.DeepFake en China.

China puso en vigencia la primera regulación sobre las '*deepfakes*', es decir el uso de inteligencia artificia para editar contenido que aparentan ser reales, pero en realidad son falsos, como por ejemplo cuando se arma un video de una persona haciendo algo ridículo y mediante el programa se le coloca la cara de un famoso, dejándonos con un video hiperrealista de ese famoso en situación ridícula. Este tipo de videos se han viralizado en las redes sociales con rostros mundialmente reconocidos de actores de Hollywood o incluso presidentes de países,

llevando esta tecnología a terrenos oscuros, al violar derechos de múltiples personas y prestarse para la comisión de delitos. (Judicial, 2018)

En China se ha implementado la primera normativa sobre las *deepfake* ', que consiste en el uso de inteligencia artificial para alterar contenido de manera que parezca real cuando en realidad es falso u engañoso. Por ejemplo, se pueden crear videos donde se inserta el rostro de una persona famosa realizando acciones ridículas. Estos videos se han vuelto virales en redes sociales, utilizando rostros reconocidos mundialmente, como actores de Hollywood o incluso presidentes de países. Sin embargo, esta tecnología ha generado preocupación al infringir los derechos de las personas y facilitar la comisión de delitos.

> El gobierno chino busca proteger los derechos e intereses de los ciudadanos, empresas y otras organizaciones, y prevenir el uso de esta tecnología para actividades ilegales o peligrosas que puedan amenazar la seguridad nacional o alterar el orden social.
>
> Los proveedores de estos servicios deben reforzar la gestión de la tecnología, garantizar que el tratamiento de los datos sea legal y correcto, adoptar medidas para salvaguardar la seguridad de los datos y obtener el consentimiento por separado del sujeto de la información personal que se está editando de conformidad con la ley. (Judicial, 2018)

Haciendo referencia al gobierno chino dentro del cual se busca que se proteja cada uno de los derechos a de los ciudadanos, empresa afectando a una persona con el uso de la tecnología en determinadas actividades ilegales así generando un daño.

Los proveedores de este tipo de servicios deben mejorar la gestión tecnológica, asegurando que el manejo de los datos sea legal y apropiado. Además, deben implementar medidas para proteger la seguridad de los datos y obtener el consentimiento explícito del individuo cuya información personal está siendo editada, de acuerdo con las leyes vigentes.

> Los proveedores de estos servicios deben reforzar la gestión de la tecnología, garantizar que el tratamiento de los datos sea legal y correcto, adoptar medidas para salvaguardar la

> seguridad de los datos y obtener el consentimiento por separado del sujeto de la información personal que se está editando de conformidad con la ley. (Judicial, 2018)

Los proveedores de servicios de *deepfake* tienen la responsabilidad de gestionar adecuadamente la tecnología que utilizan. Esto implica garantizar que cualquier manipulación de datos se realice dentro de los límites legales y éticos establecidos. Además, deben implementar medidas de seguridad para proteger la integridad de los datos y evitar su uso indebido o acceso no autorizado. Es fundamental obtener el consentimiento explícito de cualquier persona cuya información personal se vea afectada por la creación de contenido de *deepfake*, asegurándose de que comprendan cómo se utilizará su información y tengan la oportunidad de dar su aprobación de manera separada y voluntaria, de acuerdo con las leyes y regulaciones aplicables.

> Se prohíbe su uso para actividades ilegales y peligrosas…las autoridades supervisaran y administraran los servicios de *deepfake* de acuerdo a la ley y tomaran las medidas necesarias para garantizar la seguridad y protección de los derechos, clasificando los servicios y realizando inspecciones. (Judicial, 2018)

El empleo de tecnologías de *deepfake* para llevar a cabo actividades ilícitas o riesgosas está expresamente prohibido. Las autoridades estarán a cargo de supervisar y regular los servicios relacionados con *deepfake* en estricto cumplimiento de la ley. Además, tomarán las acciones pertinentes para garantizar tanto la seguridad como la protección de los derechos de las personas. Esto implica llevar a cabo una clasificación detallada de los servicios de *deepfake* y realizar inspecciones periódicas para asegurar su cumplimiento con las normativas establecidas.

> Artículo 11 Si los proveedores de servicios de información de audio y vídeo en línea y los usuarios de servicios de información de audio y vídeo en línea utilizan nuevas tecnologías y aplicaciones basadas en el aprendizaje profundo, la realidad virtual, etc. para producir,

> publicar y difundir información de audio y vídeo no real, deberán estar marcado de manera visible. Los proveedores de servicios de información de audio y video en línea y los usuarios de servicios de información de audio y video en línea no pueden utilizar nuevas tecnologías y aplicaciones basadas en aprendizaje profundo, realidad virtual, etc. para producir, publicar y difundir noticias falsas. Cualquiera que produzca, publique o difunda contenido informativo prohibido por leyes y reglamentos debe detener la difusión de información de acuerdo con la ley y tomar medidas como la eliminación para evitar la difusión de información, conservar registros relevantes e informar la información, la cultura y el medio ambiente. Sector Turismo de Internet, Radio y Televisión. (Rimaicuna Torres, 2021)

El "Reglamento sobre la gestión de servicios de información de audio y video en línea" entró en efecto el 1 de enero de 2020. Este reglamento tiene como objetivo fomentar el desarrollo saludable y ordenado de los servicios de información de audio y video en línea, proteger los derechos e intereses legítimos de los ciudadanos, las entidades legales y otras organizaciones, y preservar la seguridad nacional y los intereses públicos. En los artículos 11 y 12 de dicho reglamento se establece lo siguiente:

El artículo 11 aborda el tema de los *deepfake*, que son contenidos de audio y video en línea creados utilizando tecnologías y aplicaciones basadas en la realidad virtual para generar contenido que no es real. Se establece que quienes produzcan o difundan estos videos con el fin de transmitir información deben etiquetarlos de manera prominente. Esto garantiza que los espectadores puedan identificar fácilmente que el contenido que están viendo no es auténtico, sino que ha sido generado mediante esta tecnología para transmitir información.

El texto establece regulaciones para los proveedores y usuarios de servicios de información de audio y video en línea en China. Estas regulaciones requieren que cualquier contenido de audio y video que no sea real y que haya sido creado utilizando tecnologías emergentes como el

aprendizaje profundo y la realidad virtual sea claramente identificado como tal. Además, prohíben el uso de estas tecnologías para crear, publicar o difundir noticias falsas.

> Por su parte en su artículo 12, detalla las medidas adoptadas por aquellos que han producido, publicado o difundido este tipo de contenido *deepfake* prohibido, obligándolos a detener la transmisión de dicha información falsa, eliminarlo para evitar mayor difusión de dicha información, guardar los registros relevantes e informar a los departamentos de Información, Cultura y Turismo de Internet, Radio y Televisión, estos últimos serán los encargados de llevar el registro correspondiente de los casos suscitados en China y así hacer frente a esta nueva modalidad de suplantación de identidad. (Rimaicuna Torres, 2021)

En cuanto al artículo 12, se especifican las acciones que deben tomar aquellos responsables de la producción, publicación o difusión de contenido *deepfake* prohibido. Estos individuos están obligados a cesar la transmisión de la información falsa, eliminarla para evitar su propagación adicional, conservar registros relevantes y notificar a los departamentos de Información, Cultura y Turismo de Internet, Radio y Televisión. Estos departamentos serán responsables de mantener un registro completo de los casos relacionados en China y abordar esta nueva forma de suplantación de identidad.

> En países desarrollados como Estados Unidos y China, se adoptaron ciertas medidas legislativas para hacer frente a los videos *deepfake*; así pues, en los Estados de Texas y California, entraron en vigencia la Ley SB 751 y la Ley AB-730, respectivamente, con las cual se buscaba evitar una contienda política maliciosa. Y en China entró en vigencia el "Reglamento sobre la administración de servicios de información de audio y vídeo en línea", con el que se pretendió salvaguardar la seguridad nacional y los intereses públicos. (Rimaicuna Torres, 2021)

En naciones avanzadas como Estados Unidos y China, se han implementado medidas legislativas específicas para abordar el fenómeno de los videos *deepfake*. Por ejemplo, en

los estados de Texas y California en Estados Unidos, se han promulgado la Ley SB 751 y la Ley AB-730, respectivamente, con el objetivo de prevenir la manipulación maliciosa en el ámbito político. En China, se ha establecido el "Reglamento sobre la gestión de servicios de información de audio y video en línea", que tiene como propósito principal proteger la seguridad nacional y los intereses públicos.

3.5.Falsificación profunda.

Las disposiciones legales chinas sobre falsificación profunda involucran principalmente áreas como derechos de retrato, regulaciones de Internet e información personal. En primer lugar, el artículo 1019 del Código Civil estipula: “Ninguna organización o individuo podrá infringir los derechos de retrato de otros vilipendiando, desfigurando o utilizando medios informáticos para falsificar sin el consentimiento del titular de los derechos de retrato, ninguna organización o. El individuo puede producir, utilizar o divulgar los derechos del retrato La imagen de la persona con derecho al retrato, a menos que la ley disponga lo contrario "Según esta disposición, incluso si no existe ningún propósito de lucro y malicia subjetiva, profunda la falsificación sin el consentimiento de la persona aún puede infringir el derecho de retrato. (Song} & Dexin, 2023)

Conforme al Art. 1019 del Código Civil Chino, expresa que ninguna entidad u persona debe vulnerar el derecho a la imagen de las personas sin previo consentimiento del mismo esta acción determina vulneración a su derecho de imagen.

Al mismo tiempo, la tecnología de falsificación profunda necesita obtener una gran cantidad de datos característicos en imágenes faciales, y la información facial es información biométrica que está especialmente protegida por la ley. El uso de información facial requiere una autorización separada del propietario del retrato. El "Reglamento de Gestión de la Síntesis Profunda de los Servicios de Información de Internet" emitido en diciembre de 2022 (en adelante, el "Reglamento de Gestión"), y

> las "Medidas de Gestión de los Servicios de Inteligencia Artificial Generativa (Borrador para Comentarios)" emitido en abril de 2023 (en adelante (conocido como "Solicitud de Comentarios") "Borrador") y otras regulaciones y documentos normativos departamentales han presentado diversos grados de requisitos reglamentarios para contenido profundamente falso que infringe los derechos de imagen de otros." (Song} & Dexin, 2023)

Además, la tecnología de *deepfake* requiere una gran cantidad de datos biométricos, como información facial, que está legalmente protegida. Se necesita autorización expresa del titular del derecho de imagen para utilizar estos datos. Normativas como el "Reglamento de Gestión de Síntesis Profunda de Servicios de Información en Internet" y el "Reglamento de Gestión de Servicios de Inteligencia Artificial Generativa (Borrador para Comentarios)" imponen diferentes requisitos de regulación para el contenido de *deepfake* que viola los derechos de imagen de otras personas.

3.6.Gestión de Servicios de Información de Audio y Vídeo en Red.

> Artículo 18 Si los proveedores de servicios de información de audio y video en línea o los usuarios de servicios de información de audio y video en línea violan estas regulaciones, los departamentos de información, cultura y turismo, radio y televisión de Internet y otros departamentos deberán cumplir con la "Ley de seguridad de redes de la República Popular China". " y "Medidas de gestión de servicios de información de Internet", "Reglamento de gestión de servicios de información de noticias de Internet", "Reglamento provisional sobre gestión de la cultura de Internet", "Reglamento de gestión de servicios de programas audiovisuales de Internet" y otras leyes y reglamentos pertinentes se abordarán sí; constituye una violación de la gestión de la seguridad pública, se impondrán sanciones de conformidad con la ley; si constituye un delito, será sancionado de conformidad con la ley. (Gov.cn, 2019)

El artículo 18 establece las consecuencias para los proveedores y usuarios de servicios de información de audio y video en línea que incumplan las disposiciones del reglamento. Si se produce una infracción, las autoridades competentes, como los departamentos de ciberseguridad, cultura y turismo, radio y televisión, aplicarán las sanciones correspondientes de acuerdo con varias leyes y regulaciones, incluyendo la Ley de Seguridad Cibernética de la República Popular China y las regulaciones relacionadas con la gestión de servicios de información en Internet, la gestión de servicios de noticias en Internet, la gestión cultural en Internet y la gestión de servicios de programación de audio y video en Internet, entre otras. Si el incumplimiento constituye una violación de la gestión de la seguridad pública, se impondrán sanciones administrativas de acuerdo con las leyes de gestión de seguridad pública. En casos en los que se cometa un delito, las personas responsables serán procesadas judicialmente y enfrentarán las consecuencias legales según lo establecido en la legislación penal china. En resumen, el artículo establece un marco legal completo para abordar y sancionar las violaciones relacionadas con los servicios de información de audio y video en línea.

> Artículo 9: Ninguna organización o individuo podrá utilizar servicios de información de audio y video en línea y tecnología de la información relacionada para participar en actividades que pongan en peligro la seguridad nacional, socaven la estabilidad social, alteren el orden social, infrinjan los derechos e intereses legítimos de otros u otras actividades prohibidas por leyes y regulaciones, y no puede producir, publicar o difundir información que incite a la subversión. Contenido de información prohibido por leyes y regulaciones como el poder estatal, que ponga en peligro la seguridad política y la estabilidad social, rumores en línea, obscenidad e infracción de los derechos de reputación de otros., derechos de retrato, derechos de privacidad, derechos de propiedad intelectual y otros derechos e intereses legítimos. (Gov.cn, 2019)

Si los proveedores o usuarios de servicios de información de audio y video en línea incumplen estas regulaciones, los departamentos de información, cultura y turismo, radio y televisión en Internet, así como otros organismos pertinentes, deberán aplicar la "Ley de Seguridad de Internet de la República Popular China" y otras regulaciones como las "Medidas de Gestión de Servicios de Información en Internet", el "Reglamento de Gestión de Servicios de Información de Noticias en Internet", el "Reglamento Provisional de Gestión Cultural en Internet" y el "Reglamento de Gestión de Servicios de Programas Audiovisuales en Internet". En caso de que la infracción constituya una violación de la seguridad pública, se aplicarán sanciones de acuerdo con la ley; si constituye un delito, se impondrán las sanciones correspondientes de acuerdo con la ley.

3.7.Tipos de peligros.

Cuadro 3

PRIMER PELIGRO No se puede garantizar la seguridad de la privacidad del usuario	Las aplicaciones basadas en tecnología de audio y video de inteligencia artificial recopilan una gran cantidad de información personal, como iris, huellas dactilares y voces, si se usan de manera maliciosa, pondrán en peligro la privacidad y la seguridad de la propiedad de los ciudadanos.
SEGUNDO PELIGRO Preocupaciones por derechos de autor y falta de supervisión	Muchas plantillas de vídeo involucran cuestiones de derechos de autor de figuras públicas y usuarios de obras de cine, televisión y música también pueden cruzar líneas rojas legales en la difusión secundaria; por ejemplo, alguien puede cambiar el rostro de una celebridad en una transmisión en vivo para defraudar regalos o hacer videos eróticos; con fines de

	lucro, etc.; videos falsos de figuras públicas importantes con motivos ocultos y comportamientos que crean caos.

Elaboración propia

Fuente; ({高孟阳}, s.f.)

El cuadro 3, expresa de forma original señalando la incapacidad de garantizar la seguridad de la privacidad del usuario, lo que implica que existen riesgos y vulnerabilidades en cuanto a la protección de los datos personales cuando se utilizan ciertas aplicaciones. Luego, menciona que las aplicaciones que utilizan tecnologías de inteligencia artificial para procesar información de audio y video recopilan una amplia variedad de datos personales, como el iris, las huellas dactilares y las voces. Además, advierte sobre el peligro potencial que representa el uso malicioso de esta información para la privacidad y la seguridad de los ciudadanos.

Expone dos preocupaciones principales: los derechos de autor y la falta de supervisión en el contexto de la creación y difusión de videos digitales.

En cuanto a los derechos de autor, menciona que muchas plantillas de video involucran obras protegidas por derechos de autor de figuras públicas, así como obras de cine, televisión y música. Esto sugiere que el uso no autorizado de este contenido puede infringir los derechos de propiedad intelectual y generar problemas legales.

Por otro lado, la falta de supervisión se refiere a la ausencia de control o vigilancia sobre el contenido generado por los usuarios. Esto puede llevar a situaciones problemáticas, como la manipulación de videos para propósitos fraudulentos, como defraudar regalos o crear contenido inapropiado con imágenes de celebridades. Además, menciona la posibilidad de que se creen videos falsos de figuras públicas importantes con motivaciones ocultas, lo que podría generar confusión y caos en la opinión pública.

3.8.Función de la figura penal en ecuador y china.

3.8.1. China

La figura penal en China tiene varias funciones fundamentales que se enmarcan dentro del sistema de justicia penal del país. Estas funciones incluyen la preservación del orden social, la protección de los derechos y bienes de los ciudadanos, la disuasión del crimen, la reeducación de los delincuentes y la promoción de la estabilidad política y social. A continuación, se describen estas funciones en detalle:

Cuadro 4

Mantenimiento del orden y la seguridad.	• **Objetivo:** Una de las funciones principales de la figura penal en China es mantener el orden y la seguridad pública. Las leyes penales están diseñadas para prevenir y sancionar comportamientos que amenacen la estabilidad social. • **Aplicación:** Las autoridades judiciales y de seguridad pública utilizan las leyes penales para combatir delitos como el robo, el fraude, la violencia y otros actos que perturban el orden público.
Salvaguardia de los derechos y propiedades de los ciudadanos:	• **Objetivo:** Las leyes penales en China buscan proteger los derechos humanos básicos y la propiedad de los individuos.

	• **Aplicación:** Se aplican penas severas para delitos que involucren daños a la vida, la integridad física y la propiedad, como el homicidio, el secuestro y el vandalismo.
Prevención del crimen a través de sanciones	• **Objetivo:** La figura penal actúa como un disuasor del comportamiento delictivo mediante la imposición de castigos significativos para aquellos que infringen la ley. • **Aplicación:** Las penas incluyen desde multas y prisión hasta la pena de muerte, dependiendo de la gravedad del delito. La estricta aplicación de la ley busca desalentar a potenciales delincuentes.
Reeducación y reintegración de los delincuentes:	• **Objetivo:** Además de castigar, el sistema penal chino tiene un enfoque en la reeducación y rehabilitación de los delincuentes para que puedan reintegrarse en la sociedad.

	• **Aplicación:** Los programas de reeducación a través del trabajo y otras medidas correccionales son comunes, con el objetivo de reformar el comportamiento delictivo.
Control político y social:	• **Objetivo:** La figura penal en China también se utiliza para mantener la estabilidad política y social, asegurando la lealtad al gobierno y al Partido Comunista Chino (PCCh). • **Aplicación:** Las leyes penales incluyen sanciones severas para delitos políticos y actividades consideradas como subversivas, como el separatismo, el terrorismo y la disidencia política. Esto incluye el control de la disidencia y la represión de movimientos que puedan amenazar la autoridad del PCCh.
Proceso judicial y administrativo:	• **Objetivo:** Garantizar un sistema judicial que administre justicia de manera efectiva y eficiente.

	• **Aplicación:** La figura penal implica la implementación de procedimientos judiciales específicos, incluyendo la investigación, el juicio, la sentencia y la apelación, con el objetivo de asegurar que los culpables sean adecuadamente juzgados y castigados
Proceso judicial y administrativo	• **Objetivo:** Garantizar un sistema judicial que administre justicia de manera efectiva y eficiente. • **Aplicación:** La figura penal implica la implementación de procedimientos judiciales específicos, incluyendo la investigación, el juicio, la sentencia y la apelación, con el objetivo de asegurar que los culpables sean adecuadamente juzgados y castigados.

Elaboración propia

La función de la figura penal del estado de China como se refleja en el cuadro 4 explica la capacidad del poder punitivo del Estado con múltiples funciones que van desde la preservación del orden social y la protección de derechos, hasta la disuasión del crimen y la reeducación de

delincuentes. Además, tiene un papel crucial en la promoción de la estabilidad política y social, reflejando el control del Estado sobre la sociedad y la política. El marco legal y los procedimientos judiciales están diseñados para asegurar la aplicación efectiva de estas funciones, aunque también están influenciados por el contexto político y las prioridades del gobierno chino.

3.8.2. Ecuador.

La figura penal en Ecuador, cumple varias funciones esenciales dentro del sistema de justicia, estas funciones incluyen la preservación del orden social, la protección de los derechos y bienes de los ciudadanos, la disuasión del crimen, la rehabilitación de los delincuentes, y la promoción de la justicia y el bienestar social. A continuación, se detallan estas funciones en el contexto ecuatoriano;

Cuadro 5

Preservación del Orden	En Ecuador está destinado a la aplicación del poder punitivo del Estado para sancionar conductas típicas jurídicas y culpables con la finalidad de evitar el cometimiento de delitos.
Protección de Derechos	El estado garantiza la protección de los derechos fundamentales de cada individuo con la finalidad de prevenir u ocasionar temor al accionar de la persona.
Disuasión del Crimen	La finalidad del Código Orgánico Integral Penal es que la sociedad en general evite cometer delitos con la función de sancionar aquellos que la infrinjan.
Rehabilitación y Reinserción Social.	Con la implementación de programas de reinserción social se determina la rehabilitación de la persona para que no vuelva a cometer delitos con el objetivo de reformar su comportamiento.
Promoción de la Justicia y el Bienestar Social	El sistema de justicia penal sea justo y equitativo, protegiendo los derechos de todas las partes involucradas y promoviendo el bienestar social y la aplicación de las leyes penales debe ser transparente y justa,

	asegurando que los procesos judiciales respeten los derechos humanos y las garantías constitucionales.
Ejecución de la Ley y Administración de Justicia	Determina que el Estado garantice de manera efectiva la figura penal en los procedimientos específicos en todo su proceso desde inicio a final.
Protección de la Sociedad y Derechos Humanos	Las leyes penales y los procedimientos judiciales buscan asegurar que los derechos de los acusados sean respetados, incluyendo el derecho a un juicio justo y el acceso a la defensa legal.

Elaboración propia.

El cuadro 5 refleja que la figura penal en Ecuador cumple funciones esenciales para mantener el orden social, proteger los derechos y bienes de los ciudadanos, disuadir el crimen, rehabilitar a los delincuentes y promover la justicia y el bienestar social. El marco legal establecido por el Código Orgánico Integral Penal y otras normativas complementarias proporciona la estructura necesaria para la aplicación de estas funciones, con un enfoque en la justicia, la equidad y el respeto a los derechos humanos.

3.9.Análisis comparativo del *deepfake* en Ecuador y China.

Una vez analizado el delito de *deepfake* en relación a China y Ecuador encontramos diferencias notables en el presente capítulo 3 para esto debemos determinar la importancia al momento del cometimiento del delito de *deepfake* para ello se determina un análisis comparativo entre ambas legislaciones.

3.9.1. Ecuador.

En la legislación ecuatoriana debemos tener claro que no existe un tipo penal que individualice el delito de *deepfake* ya que únicamente existe normativa que engloba el delito pero no determina u demuestra la tipificación como tal, para esto en su artículo 179; 172.1; 182; 178; conforme a cada uno de ellos explica sobre el uso del derecho de imagen, intimidad, honra,

hacia el cometimiento en contra de ellos tanto en el uso del derecho a la imagen únicamente así demostrando la presencia de una extorción realizada mediante amenazas y/o chantajes las cuales afecta a dichos derechos mencionados hacia la persona u sujeto de derecho ante el uso inadecuado y ante la falta de consentimiento además en un ámbito sexual ante extorciones realizadas resalta este detalle ante la falta de protección ante la difusión de contenido sexual por parte del sujeto activo sin considerar riesgos inminentes que genera al titular de su información que está siendo expuesta hacia fines delictivos.

La falta de interés de la legislación ecuatoriana ha sido notable a lo largo de los años por el hecho que el uso inadecuado ante la falta del consentimiento de los titulares de la información de su imagen, honra y dignidad atentando así el bien jurídico de la imagen en aspectos generales ya que el Estado trata temas del uso del derecho a la imagen mas no en efectos de audio ni voz, Ecuador así entra en una lista más de acceso fácil a la vulneración de los derechos ya mencionados con el uso de la Inteligencia Artificial como fuente creadora del contenido y sin expresar regulaciones y sanciones ante el uso y difusión del contenido denotando la falta de aplicación de la norma legislativa para garantizar la protección de dichos derechos mencionados.

3.9.2. China.

Cuando hacemos referencia en el Estado de China considera el uso y regulación la inteligencia artificial de tal forma que considera estos derechos mencionados en su legislación esencialmente a la información privada dentro de su población, reconociendo que mediante el uso de la Inteligencia Artificial enfocado a la imagen, voz, audio y sonido posee una gama mucho más amplia y regulada concatenado así un reglamento ante el delito de *deepfake* sin expresar de forma tipificada el delito como un tipo penal en específico sino más bien englobando tipos penales que considera pertenecen a la difusión y creación del *deepfake* en China.

China considera la presencia de dos peligros primero, ante la no garantía de seguridad y la privacidad del usuario, considerando que el uso de la tecnología ante la recopilación de la información no es tratada de forma adecuada vulnerando así la seguridad y privacidad de los titulares de su información además de esto como segundo punto de peligro corresponda ante la falta de supervisión y ante los derechos de autor, existiendo planillas que vulneran como figura pública en determinados lugares ante el entorno social relacionado a música, videos, etc, degenerando el peligro del uso de imagen de las celebridades con fines de lucro para beneficio propio sin considerar el consentimiento de los titulares de la información personal.

En China expresa la importancia en cuanto a su legislación el regular las acciones del uso, creación y difusión de contenido audiovisual que influya ante un interés colectivo en la sociedad, China expresa el interés de forma concurrente en su reglamento con las regulaciones ante el uso de la Inteligencia Artificial garantizando así la protección de los derechos mencionados.

Capítulo 4

4. Análisis del caso de Giorgia Meloni.

> Con quince 15 años, se afilió al Fronte de la Gioventù, organización juvenil del Movimento Sociale italiano - Destra Nazionale. Como miembro del Fronte destacó en la movilización y coordinación de organizaciones estudiantiles en un momento en que el MSI era el único partido de derecha activo en las universidades dominadas por la izquierda. (Moreno, Ramírez, de la Oliva, & Moreno y otros, s.f.)
>
> Fundadora de la asociación Gli Antenati, que participó en la protesta contra el proyecto de reforma de la educación pública. En 1996, asumió la dirección de Azione Studentesca, el movimiento estudiantil de Alleanza Nazionalez (Moreno, Ramírez, de la Oliva, & Moreno y otros, s.f.)

A la edad de 15 años, Giorgia Meloni la cual se unió al Fronte della Gioventu, el ala juvenil del Movimiento Social Italiano. Como miembro del Frente, se buscó una distinguió en cuanto a lo que es el movilizar y una buena coordinar organizaciones estudiantiles en las que se toman en consideración cada uno de los momentos los cuales se destacaban por ser únicos en presencia de un partido de la derecha activo en cuanto a la universidad predominantemente de izquierda.

Esta una fundadora de la asociación Gli Antenati, en la que decidió participar para realizar una protesta en la que se encontraba en contra de un plan nacional mediante lo que es una reforma educativa en la que busco dar a conocer sobre la opinión en la que basaba su conocimiento. Para ello en el año 1996 en el cual tomo un papel importante en cual era llegar a convertirse a una líder en la que es la asociación nacional en la que realizaba movimientos con junto con los estudiantes con una forma de pensar al respecto con los estudiantes del movimiento, Azione Studentesca el cual marco una diferencia en busca de generar un cambio.

> Hace apenas unas semanas sucedía lo inevitable. Tras más de un año sin parar de subir en los sondeos, Fratelli d'Italia (FdI), el partido de Giorgia Meloni, se colocaba por primera vez en una encuesta como primera fuerza, superando a la Lega de Matteo Salvini. Un sorpasso que algunos analistas consideran precipitado, pero que, sin duda, refleja la tendencia al alza de los de Meloni, y la progresiva pérdida de hegemonía de la Lega de Salvini en la centroderecha.) (Gil, 2024)

Hace apenas unas semanas sucedió lo inevitable. Después de más de un año de encuestas, la Orden Fraternal de Italia (FdI) sigue subiendo en las encuestas, superando al partido Lega de Matteo Salvinicon un numero alto en lo que son las encuentas que esto llevo a que se pudiera convertir en por primera vez formando parte de la Orden de la Fraternal de Italia con la mayoría de votos dentro de la población. Algunos analistas ven la medida un poco apresurada, pero no hay duda de que refleja el ascenso del partido de Meloni y la pérdida gradual de hegemonía de la coalición de centroderecha de Salvini.

> Fratelli d'Italia llevaba más de un año subiendo en las encuestas, y su escalada durante las últimas semanas ha coincidido en el tiempo con la publicación de la autobiografía de Giorgia Meloni, que se ha convertido en todo un fenómeno editorial en Italia. Casi dos meses después de su publicación, el libro continúa como número uno en la sección de política en Amazon Italia, y a finales de mayo ya se habían superado las 100.000 copias vendidas. Una cifra impresionante para tratarse de la biografía de un líder político. (Gil, 2024)

El partido de Giorgia Meloni, Fratelli d'Italia (FdI), quedó primero en las encuestas, superando al partido Lega de Matteo Salvini, después de más de un año de aumentos en las encuestas. Aunque algunos analistas consideran que este cambio es prematuro, sin duda demuestra que la inversión extranjera directa está ganando popularidad y perdiendo terreno frente a la Liga de centroderecha.

El ascenso electoral de Fratelli d'Italia coincide con la publicación de la biografía de Giorgia Meloni, que encuentra éxito en Italia. Casi dos meses después de su publicación, el libro sigue siendo el libro político número uno en la Amazonia italiana, vendiendo más de 100.000 copias a finales de mayo; Este es un logro extraordinario para un político.

> La primera ministra de Italia, Giorgia Meloni, comparecerá el 2 de julio ante un tribunal de Cerdeña tras denunciar a dos hombres por la presunta fabricación y difusión de un vídeo pornográfico falso en el que aparecía la imagen manipulada de la mandataria italiana a través de un programa de inteligencia artificial. La abogada de la jefa del Ejecutivo italiano solicitó una indemnización de 100.000 euros por difamación. (Melguizo, La Razón, 2024)

El 2 de julio, la primera ministra italiana, Giorgia Meloni, comparecerá ante el tribunal en Cerdeña. Esta marca se produjo después de que Meloni acusara a los dos hombres de crear y distribuir videos pornográficos falsos; Estos videos usaban su propia imagen usando un programa inteligente y actuando como si él estuviera en el video. El abogado de Meloni exigió una indemnización de 100.000 euros por el insulto provocado por estos vídeos falsos.

> Los hechos se remontan a cuatro años atrás, cuando Meloni no estaba aún al frente del Gobierno. Los presuntos autores del delito son dos hombres de 73 y 40 años, padre e hijo respectivamente, procedentes de la provincia de Sassari, en la isla de Cerdeña. Según la acusación, los imputados colocaron el rostro de la líder de Hermanos de Italia sobre los cuerpos de unas actrices porno utilizando un programa de inteligencia artificial y difundieron las imágenes a través de varias páginas de Internet de Estados Unidos con contenido para adultos. Los vídeos, considerados como «publicaciones de marcada vulgaridad», fueron vistos «millones de veces» en todo el mundo durante los meses que permanecieron en línea. (Melguizo, La Razón, 2024)

Los hechos que ahora se investigan tuvieron lugar hace cuatro años, cuando George Meloni no era Primer Ministro. Los presuntos autores son un padre de 73 años y su hijo de 40 de la provincia sarda de Sassari. Los fiscales dicen que los hombres utilizaron un programa de inteligencia artificial para superponer el rostro de Meloni al cuerpo de la actriz porno. Luego distribuyeron las imágenes a varios sitios de contenido para adultos en todo Estados Unidos. Los vídeos, considerados extremadamente vulgares, fueron vistos millones de veces online en todo el mundo cuando fueron publicados.

> La primera ministra, que se presenta al proceso como parte civil, fue convocada a declarar ante el tribunal el próximo 2 de julio. La abogada de la mandataria italiana, María Giulia Marongiu, solicitó una indemnización de 100.000 euros para su defendida en concepto de daños y perjuicios para su imagen. Una petición que, según explicó la letrada en una audiencia previa, tiene el objetivo de lanzar «un mensaje dirigido a todas las mujeres víctimas de este tipo de abusos para que no tengan miedo a denunciar». En caso de ganar el proceso, la indemnización será donada al fondo del Ministerio del Interior para las mujeres víctimas de violencia en Italia. (Melguizo, La Razón, 2024)

Es el primer ministro actúa como parte civil y ha sido llamado a declarar el 2 de julio. La abogada del presidente italiano, María Giulia Marongiu, la cual pidió a su cliente una indemnización de 100.000 euros por el daño causado a su imagen degenera una afectación el uso de la imagen dentro de un entorno social en el cual se encuentra en contra de su consentimiento el cual no se tomó en cuenta al instante en que se usó para un fin malicioso hacia la ministra. Según explicaron los abogados en la audiencia anterior, el objetivo de la solicitud es "enviar un mensaje a todas las mujeres que han sufrido este tipo de violencia, para que no tengan miedo de denunciarlo". Si el caso tiene éxito, la indemnización se donará al fondo del Ministerio del Interior italiano para las víctimas de la violencia contra las mujeres.

> Según la prensa italiana, los hechos se remontan a 2020, cuando la Policía Postal de Sassari abrió una investigación y consiguió llegar hasta quienes habían publicado los vídeos en Internet. A través del nickname del autor de la publicación, rastrearon el número de teléfono del que se habían originado los datos y así pudieron identificar a los presuntos autores de la estafa. Según la acusación de la Fiscalía, el hombre de 40 años habría sido el responsable de modificar los vídeos pornográficos a los que añadió la imagen de Meloni a través de un software específico. Mientras, su padre está imputado por ser el propietario de la línea telefónica utilizada para la publicación de los vídeos. (Melguizo, La Razón, 2024)

La primera ministra italiana, Giorgia Meloni, fue citada a declarar como parte civil en la audiencia del 2 de julio. En este caso, su abogada Maria Giulia Marongiu exigió una indemnización de 100.000 euros por dañar la imagen de Meloni. El objetivo es enviar un mensaje de apoyo a todas las mujeres que han sido sometidas a este tipo de violencia y animarlas a denunciarlo sin miedo. Si Meloni gana el caso, se pagará una indemnización al fondo para las víctimas femeninas del Ministerio del Interior italiano.

Según medios italianos, el incidente comenzó en 2020. La Policía Postal de Sassari inició una investigación que permitió identificar a los responsables de la publicación de los vídeos falsos. Utilizando el nombre del autor y el número de teléfono correspondiente, pudieron identificar a los presuntos autores: un hombre de 40 años y su padre de 73, que utilizó un programa especial para editar los escandalosos vídeos e insertar la foto de Meloni. El dueño de la línea telefónica estaba montando el video.

> Giorgia Meloni solicitó a través de su abogada una indemnización en concepto de "daños y perjuicios". La indemnización que exige es de 108.000 euros y serán donados a una organización benéfica para las mujeres víctimas de violencia, según lo comunicó la magistrada. ({urgente}, 2024)

A través de su abogado, Georgia Meloni pidió "daños y perjuicios". Según el juez, se buscó mediante una solicitud lo que es una indemnización de 108.000 euros, que se donarán a una organización en la que se buscara que dicha donación sea para una benéfica para mujeres maltratadas para mejorar la vida las mujeres que sufren del maltrato.

> La petición pretende ser un mensaje dirigido a todas las mujeres víctimas de este tipo de abuso para que no tengan miedo de denunciarlo», explicó la abogada de Meloni, Maria Giulia Marongiu. «La figura es simbólica y pretende contribuir a la protección de las víctimas. Mujeres que, muchas veces sin saberlo, son blanco de este tipo de delitos», agregó en diálogo con la prensa italiana. ({urgente}, 2024)

Giorgia Meloni exigió una indemnización por "daños" a través de su abogado. La cantidad requerida es de 108.000 euros que, según el juez, se donarán a una organización benéfica que apoya a mujeres víctimas de violencia.

La abogada de Meloni, Maria Giulia Marongiu, explicó que el objetivo de la solicitud es enviar un mensaje a todas las mujeres que son víctimas de este tipo de abuso, animándolas a denunciar sin miedo. Marongiu subrayó que la imagen es simbólica y pretende promover la protección de las víctimas, señalando que muchas mujeres son a menudo blanco involuntario de estos crímenes.

> Cuando en 2019 entró en vigor la ley del ‘revenge porn’ no estaba incluida la extensión a los contenidos virtuales”, asevera. En el caso de que esté relacionado con menores, la ley prevé expresamente que, ahí sí, sea delito y la pena puede llegar a dos años de cárcel. (Diéguez, 2024)

Entra en vigencia lo que es una ley de pornografía de venganza en 2019, así buscando que dicha aplicación genere una ampliación para determinar el contenido virtual en cual no deberá ser considerado, con un argumento en el que se refleje que un menor de edad se encuentre

involucrado, la ley es clara en que sí, es un delito y la pena puede ser de hasta dos años de prisión.

> Si además también hay amenazas a las víctimas para no difundir el vídeo se añade también extorsión que está penado con reclusión de 5 a 10 años", añade. Pero, para los mayores de edad, perseguir este tipo de delitos, hasta ahora, era mucho más difícil. (Diéguez, 2024)

Además, si se realizan amenazas para evitar la difusión del material, se añade el cargo de extorsión, que conlleva penas de 5 a 10 años de prisión. Esto refleja la gravedad adicional de coaccionar a alguien bajo la amenaza de difusión de su contenido íntimo.

Para los adultos, la persecución de estos delitos ha sido más complicada porque la ley no estaba diseñada inicialmente para abarcar los contenidos virtuales o manipulados digitalmente, lo que ha dificultado la aplicación de penas severas en casos como el de los *deepfakes*. Esta brecha legal ha hecho que sea más difícil para los adultos obtener justicia en casos de pornografía no consensuada si no hay amenazas directas involucradas.

> Se podría perseguir la difamación, agresiones, actos persecutorios o extorsión si la víctima decide denunciar e indicar la plataforma donde han sido subidos esos vídeos", detalla. En ese caso el contenido será retirado, por eso, señala la experta, denunciar lo antes posible es importante para que desaparezca ese contenido. En el caso de Meloni la acusación es, precisamente, por difamación. (Diéguez, 2024)

Se pueden perseguir delitos como la difamación, agresiones, actos persecutorios o extorsión si la víctima decide denunciar y proporciona información sobre la plataforma donde se han subido los videos comprometidos. La experta subraya la importancia de denunciar lo antes posible para que el contenido pueda ser retirado rápidamente de la plataforma.

En el caso específico de Giorgia Meloni, la acusación es por difamación. Esto significa que los videos *deepfake* que se crearon y difundieron usando su imagen dañaron su reputación. Al

denunciar y proporcionar detalles de la plataforma, Meloni no solo busca la eliminación de los videos, sino también responsabilizar a los culpables de difundir contenido difamatorio.

Esta estrategia de denuncia inmediata y específica ayuda a asegurar que el contenido dañino sea retirado de la web, minimizando el daño y permitiendo que las autoridades actúen contra los responsables. En resumen, la rapidez y precisión en la denuncia son clave para combatir efectivamente estos delitos.

4.1. Revenge Porn

> Las víctimas son fundamentalmente mujeres jóvenes y, en muchos casos, los instigadores son exparejas u otras personas que pretenden humillar y atacar su reputación mediante la publicación de este tipo de imágenes."
>
> En los últimos años el aumento de actividades como el sexting (envío de imágenes y otro tipo de contenido íntimos a través plataformas online) han multiplicado los casos de Revenge Porn. (Revenge Porn, s.f.)
>
> El revenge Porn es un delito castigado por la ley. En España la Agencia de Protección de Datos recuerda que "amenazar o chantajear con difundir vídeos o grabaciones íntimas de la pareja (fotografías, vídeos o audios) sin su consentimiento puede constituir un delito de violencia de género". Cualquiera que participe en su publicación o los comparta se expone a multas y penas de prisión de tres meses a un año. artículo 197.1 del Código Penal (Revenge Porn, s.f.)

Las víctimas de "revenge porn" suelen ser principalmente mujeres jóvenes, y a menudo los perpetradores son exparejas u otras personas que buscan humillar y dañar su reputación mediante la publicación de imágenes íntimas sin consentimiento. Este tipo de actos son motivados por deseos de venganza o control, y se utilizan como una forma de agresión emocional y social.

En los últimos años, el aumento de actividades como el sexting, que implica el envío de imágenes y contenido íntimo a través de plataformas online, ha incrementado significativamente los casos de "revenge porn". La facilidad con la que se puede compartir y difundir contenido íntimo ha exacerbado este problema, afectando a muchas personas que confiaron en la privacidad de sus comunicaciones.

El "revenge porn" es considerado un delito en muchos países, incluyendo España. La Agencia Española de Protección de Datos ha recordado que amenazar o chantajear con la difusión de vídeos o grabaciones íntimas sin el consentimiento de la persona afectada puede constituir un delito de violencia de género. Según el artículo 197.1 del Código Penal español, cualquier persona que participe en la publicación o difusión de dicho contenido puede enfrentarse a multas y penas de prisión que varían de tres meses a un año.

Este marco legal subraya la gravedad del delito y la necesidad de proteger a las víctimas, incentivando la denuncia de estos actos para que el contenido perjudicial sea retirado rápidamente y los responsables sean sancionados.

> De manera que si alguien publica fotos íntimas de otra persona -grabadas con o sin autorización- está cometiendo un delito de violencia sexual, ya que, aunque no exista una agresión física sí hay un daño psicológico, castigado por la ley. Se puede denunciar ante los organismos pertinentes, tanto la Brigada de Investigación Tecnológica de la Policía Nacional, como el Grupo de Delitos Telemáticos la Guardia Civil. También se puede acudir a webs como Protección Online, especializadas en la concienciación contra este tipo de prácticas. “(artículo 197.1 del Código Penal). (Revenge Porn, s.f.)

Esta práctica es ilegal y está castigada por la ley en muchos países, ya que atenta contra la intimidad y la dignidad de la persona. Es importante denunciar estos casos ante las autoridades pertinentes, como la Brigada de Investigación Tecnológica de la Policía Nacional o el Grupo

de Delitos Telemáticos de la Guardia Civil, para que se puedan tomar las medidas necesarias y se pueda perseguir a los responsables.

Además, existen organizaciones y webs especializadas, como Protección Online, que están dedicadas a la concienciación sobre este tipo de prácticas y pueden ofrecer apoyo y asesoramiento a las víctimas. Es fundamental combatir este tipo de violencia y trabajar en la prevención de su ocurrencia.

Conclusiones

En conclusión, es preciso determinar que en el delito de *deepfake* en el Ecuador no se encuentra considerado como un tipo penal ya que se debe tomar en cuenta si un delito el cual no se encuentra tipificado se considera permitido, así generado que las personas vulneren los derechos de los titulares de la información sin el consentimiento de dicha importancia debería estar en la legislación ecuatoriana.

Cada uno de los artículos en los cuales se ha tratado de exponer la falta de determinación que presenta en la sociedad el uso de la inteligencia artificial; sin establecer un límite al momento en que se usa y sin considerar que mediante el cual genera afectaciones en un entorno social ya que solo no es tomado como un delito en la normativa no lo expresa pero en el presente estudio demostramos la falta de tipificación y las consecuencias que este conlleva con un uso inadecuado de la protección de los datos que es la imagen, voz y sonido para esto es de suma importancia considerar que debe existir una figura penal mediante la cual sancione este delito; guiando al uso adecuado de la misma y sobre todo de la información por la cual está siendo expuesta sin considerar si el sujeto cuenta con el consentimiento de la información.

Finalizando así que, existe una omisión del delito de *deepfake* dentro de la legislación Ecuatoriana al momento de no considerar la presencia de la vulneración de los datos del titular de los derechos ya nombrados y sobre todo una falta de regulación en la creación de contenido audiovisual que mediante el uso de la inteligencia artificial no se toma en cuenta un consentimiento expreso o tácito de la persona afectada por lo que, debe existir un reglamento que exprese el uso y su regulación ante el uso de la Inteligencia Artificial para así determinar posibles sanciones correspondientes al delito de *deepfake*.

Recomendaciones

- ➔ Como recomendación es primeramente priorizar que, se considere como un tipo penal el delito de *deepfake*, es importante que se debe estimar una reforma al Código Orgánico Integral Penal cuyo objetivo principal sea proteger los derechos de las personas, por el hecho que, el uso de la inteligencia artificial ha llevado a vulnerar el derecho a la intimidad, honra, carácter sexual, sexual publicación de video y difusión de imagen determinado que dicha información el proporcionada con el mero desconocimiento de la misma.
- ➔ Segunda recomendación; Crear una normativa cual adecue un uso correcto de la inteligencia artificial ya que, como se demuestra en la presente investigación existe la vulneración al usar la inteligencia artificial sin contar con el consentimiento de la persona con el indebido uso de la misma en coordinación entre el poder ejecutivo y legislativo del Estado.
- ➔ Tercera recomendación, en relación a la incentivación ante un uso adecuado de la inteligencia artificial en el ámbito social ya que no se socializa el uso, ventajas y desventajas de la Inteligencia Artificial en relación al tratamiento de los datos personales.
- ➔ Como cuarta recomendación; la creación de políticas públicas en relación al derecho informático para determinar el uso adecuado y tratamiento debido de la información que es proporcionada en las diferentes redes sociales como Facebook, Instagram, X, WhatsApp, como fuentes de difusión de imágenes de mayor uso en un entorno social.

Bibliografía.

I. {urgente}. (20 de 03 de 2024). *urgente24*. Obtenido de urgente24: https://urgente24.com/mundo/giorgia-meloni-exige-una-indemnizacion-los-videos-pornos-fake-su-rostro-n573469

II. {高孟阳}. (s.f.). *Cctv.com*. Obtenido de Cctv.com: http://m.news.cctv.com/2019/12/01/ARTIx8DFkN8HPBhCJoCOPgGA191201.shtml

III. *AECOC*. (16 de 11 de 2020). Obtenido de AECOC: https://www.aecoc.es/innovation-hub-noticias/la-capacidad-de-la-ia-para-crear-deepfakes-cuales-son-los-potenciales-impactos-positivos/

IV. Alumnos, A. (s.f.). *LISA Institute*. Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

V. Alumnos, A. (s.f.). *LISA Institute*. Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

VI. Ansorena, T. R. (Septiembre de 2020). *NUEVA SOCIEDAD*. Obtenido de NUEVA SOCIEDAD: https://nuso.org/articulo/el-fin-de-la-realidad/#:~:text=Los%20deepfakes%20aparecieron%20por%20primera,libre%20acceso%20con%20resultados%20asombrosos.

VII. Carrera, P. (2018). Estratagemas de la posverdad. *Revista latina de comunicación social*, 1469-1481. doi:10.4185/rlcs-2018-1317

VIII. Cloud, G. (s.f.). *Google Cloud*. Obtenido de Google Cloud: https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419

IX. Constituyente, A. (2008). *Constitución de la República del Ecuador.* Montecristi: Registro Oficial.

X. de Derecho, E. P. (s.f.). *Edu.pe*. Obtenido de Edu.pe: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/82458/Rimaicuna_TMF-SD.pdf?sequence=1&isAllowed=y

XI. Del deepfake sexual, L. C. (s.f.). *Ugr.es*. Obtenido de Ugr.es: http://criminet.ugr.es/recpc/26/recpc26-09.pdf

XII. Diéguez, M. G. (25 de 04 de 2024). *ARTÍCULO 14 – Periodismo por la igualdad*. Obtenido de ARTÍCULO 14 – Periodismo por la igualdad: https://www.articulo14.es/internacional/italia-quiere-penar-5-anos-la-difusion-de-contenido-manipulado-con-ia-20240425.html

XIII. Díez, C. C. (09 de 06 de 2021). *Ediciones EL PAÍS S.L*. Obtenido de Ediciones EL PAÍS S.L: https://cincodias.elpais.com/cincodias/2021/06/08/legal/1623163694_649925.html

XIV. Domínguez, A. (25 de 05 de 2021). *Marketing Insider Review*. Obtenido de Marketing Insider Review: https://marketinginsiderreview.com/tecnologia-deepfake-que-es-publicidad/

XV. ENAE. (s.f.). *Enae.es*. Obtenido de Enae.es: https://www.enae.es/blog/la-inteligencia-artificial-en-nuestra-vida-diaria?gad_source=1&gclid=CjwKCAjw88yxBhBWEiwA7cm6pS58TwJ4Lkq6XeBkpZRvn30Y6hV_H-LKmf1WTwcZclS3Lr0174coHBoCIzEQAvD_BwE&_adin=11551547647

XVI. Gil, J. B. (06 de Noviembre de 2024). *¿Quién es Giorgia Meloni?* Obtenido de ¿Quién es Giorgia Meloni?: https://ctxt.es/es/20210701/Politica/36642/giorgia-meloni-ultraderecha-italia-salvini-berlusconi-fratelli-jaime-bordel-gil.htm

XVII. Goncalves, S. (2022). *IROCAMM-International Review Of Communication And Marketing Mix, 5*, 22-38. doi:10.12795/irocamm.2022.v05.i02.02

XVIII. *Gov.cn*. (22 de 11 de 2019). Obtenido de ttps://zwgk.mct.gov.cn/zfxxgkml/zcfg/gfxwj/202012/t20201204_906347.html

XIX. Jiménez-Marín, G. (2022). IROMCAMM. *Los deepfakes como una nueva forma de desinformación*, 14. Obtenido de https://institucional.us.es/revistas/IROCAMM/5_2_2022/IROCAMM_V5-N2-2022_02_gomes-goncalves.pdf

XX. Judicial, D. (31 de 08 de 2018). *Diario Judicial*. Obtenido de Diario Judicial: https://www.diariojudicial.com/news-94362-deepfake-de-aca-a-la-china

XXI. Londoño, P. (06 de 02 de 2023). *Hubspot.es*. Obtenido de Hubspot.es.

XXII. Melguizo, S. (20 de 03 de 2024). *La Razón*. Obtenido de La Razón: Meloni testificará en el juicio por la difusión de vídeos porno «deepfake» en los que aparece

XXIII. Melguizo, S. (20 de 03 de 2024). *La Razón*. Obtenido de La Razón: Meloni testificará en el juicio por la difusión de vídeos porno «deepfake» en los que aparece

XXIV. Moreno, V., Ramírez, M. E., de la Oliva, C., & Moreno y otros, E. (s.f.). *Buscabiografias.com*. Obtenido de Buscabiografias.com: https://www.buscabiografias.com/biografia/verDetalle/11991/Giorgia%20Meloni

XXV. Nacional, A. (2021). *Ley Organica de la Ley de Protección de Datos Personales.* Quito: Registro Oficial. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

XXVI. Nacional, A. (2024). *Código Orgánico Integral Penal.* QuitoRegistro oficial.

XXVII. *NATIONAL GEOGRAPHIC*. (15 de Noviembre de 2023). Obtenido de NATIONAL GEOGRAPHIC: https://www.nationalgeographicla.com/ciencia/2023/11/que-es-un-deepfake

XXVIII. *Pandasecurity.com*. (s.f.). Obtenido de Pandasecurity.com: https://www.pandasecurity.com/es/security-info/revenge-porn/

XXIX. Pila, A. W., & Caiza, A. M. (2022). *Universidad de Otavalo.* Obtenido de Universidad de Otavalo: https://repositorio.uotavalo.edu.ec/bitstream/52000/695/1/PP-DER-CONS-2022-008.pdf

XXX. *REPSOL*. (11 de 09 de 2023). Obtenido de REPSOL: https://www.repsol.com/es/energia-futuro/tecnologia-innovacion/inteligencia-artificial/index.cshtml

XXXI. Resilencia, P. d. (19 de 04 de 2023). *Gob.es*. Obtenido de Gob.es: https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr

XXXII. Rimaicuna Torres, M. F. (2021). *Repositorio Universidad César Vallejo.* Obtenido de Repositorio Universidad César Vallejo: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/82458/Rimaicuna_TMF-SD.pdf?sequence=1&isAllowed=y

XXXIII. Sarmiento, S. (07 de 08 de 2023). *Platzi*. Obtenido de Platzi: https://platzi.com/blog/como-hacer-un-deepfake/

XXXIV. Song}, {., & Dexin, L. (08 de 05 de 2023). *Lexology*. Obtenido de Lexology: https://www.lexology.com/library/detail.aspx?g=6b61d20f-5a8b-4324-9acb-391012ea7b25

Anexo

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Nathaly Lizbeth Arévalo Fernández portador(a) de la cédula de ciudadanía **Nº 0104767090.** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"La omisión del delito de DEEPFAKE en el Código Orgánico Integral Penal en Ecuador"** 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, **04 de julio de 2024**

F: .....

Nathaly Lizbeth Arévalo Fernández

C.I. 0104767090