VNIVERSITAS

Vol. 73
Publicación continua
2024

ISSN: 2011-1711 (En línea) | ISSN: 0041-9060 (Impreso)

Artículos

El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el *deepfake**

The Illicit Use of Artificial Intelligence Techniques and the Need for Regulation: Deepfake

DOI: https://doi.org/10.11144/Javeriana.vj73.uiti

Homero Pracedes Jondec Briones [a]
Universidad César Vallejo, Perú
ORCID: https://orcid.org/0000-0001-9691-2722

María Eugenia Zevallos Loyaga
Universidad César Vallejo, Perú
ORCID: https://orcid.org/0000-0002-2083-3718

Adolfo Yesser Segura Grados
Universidad César Vallejo, Perú
ORCID: https://orcid.org/0000-0001-6348-0855

Erika Milagros Castrejon Vilchez
Universidad César Vallejo, Perú
ORCID: https://orcid.org/0000-0001-7133-6036

Recibido: 04 julio 2024
Aceptado: 30 septiembre 2024
Publicado: 12 diciembre 2024

Resumen:

Este artículo tiene como objetivo principal determinar si es necesario regular el uso ilícito de las técnicas de IA como el *deepfake*; además, por objetivos específicos tiene describir el funcionamiento del *deepfake* como técnica de IA y su uso ilícito; examinar casuísticamente el reciente uso ilícito de *deepfake* y cómo se produce el daño; y, finalmente, identificar los fundamentos para la tipificación del uso ilícito de *deepfake* como técnica de IA. Metodológicamente, se abordó un tipo de investigación básico, con un enfoque de investigación cualitativo y con un diseño no experimental, haciendo uso de entrevistas, y los resultados se obtuvieron mediante un enfoque multidisciplinario, a través de entrevistas con especialistas, análisis documental y estudios relacionados con el *deepfake* y con fuentes de base de datos de confiabilidad. Se concluye que el *deepfake* es un tipo de tecnología emergente que está al alcance de usuarios de todas las edades, que gana adeptos constantemente y que su uso malicioso produce trastornos sociales, siendo fundamental regularlo como delito independiente, estableciéndose figuras legales propias según los contextos, sin depender de otras figuras legales.

Palabras clave: inteligencia artificial, ordenamiento jurídico, delito, tecnología, *deepfake*.

Abstract:

This article has as its main objective to determine whether it is necessary to regulate the illicit use of AI techniques, such as Deepfake. The specific objectives were to describe the functioning of Deepfake as an AI technique and its illicit use, examine recent case studies of illicit Deepfake use and how harm is produced, and, finally, identify the foundations for classifying the illicit use of Deepfake as an AI technique. Methodologically, a basic type of research was undertaken, with a qualitative research focus and a non-experimental design. Interviews were used, and the results were obtained through a multidisciplinary approach, including interviews with specialists, documentary analysis, and study of related materials on Deepfake from reliable databases. The conclusion is that Deepfake is an emerging technology accessible to users of all ages, constantly gaining followers. Its malicious use leads to social disorders, making it essential to regulate it as an independent offense, establishing legal provisions specific to the context, without relying on other legal figures.

Keywords: Artificial Intelligence, Legal System, Crime, Technology, Deepfake.

Notas de autor

[a] Autor de correspondencia. Correo electrónico: hjondecb@hotmail.com

Introducción

El presente artículo aborda el uso progresivo del *deepfake*, que es una técnica de inteligencia artificial que ha ganado terreno en la sociedad. Según un estudio de la empresa Deeptrace, en 2018 se registraron 8000 videos *deepfake*, cifra que ha aumentado a 14678. La mayoría de estos videos eran de contenido pornográfico dirigido exclusivamente a mujeres.

El tema es de vital importancia ya que el *deepfake* representa una amenaza emergente, pues es usado para engañar y dañar la imagen de las personas, representando a individuos haciendo cosas que nunca hicieron, lo que puede causar traumas psicológicos y daños a su reputación. Además, esta tecnología no se limita a personas específicas, afectando tanto a hombres como a mujeres, incluyendo a niños. Ha sido crucial detectar y combatir este contenido malicioso para proteger derechos fundamentales, como la intimidad y la dignidad humana, y evitar la desconfianza y confusión en la sociedad.

Teniendo todo esto en cuenta, surge la siguiente problemática: ¿es necesario regular el uso ilícito de las técnicas de la IA como el *deepfake*?

Esto se justificó desde la perspectiva teórica, profundizando en el fenómeno del *Deepfake* mediante el uso de teorías y conceptos, lo que permitió comprender su funcionamiento, alcance e impacto en la sociedad moderna, ajustándose a nuestra realidad.

En el ámbito de la justificación metodológica, se emplearon instrumentos de investigación, como entrevistas, análisis de documentos y el uso de teorías de confiabilidad, que otorgaron un conocimiento acertado del *deepfake*. Estos métodos no solo otorgan solidez a nuestra investigación, sino que también proporcionan un marco referencial para futuros estudios en este campo emergente. Y, por último, en el ámbito de la justificación práctica, los resultados obtenidos posibilitaron soluciones óptimas a los problemas mencionados, lo que a su vez contribuirá a prevenir y eliminar el uso ilegal de la inteligencia artificial, sobre todo en casos de *deepfake*.

Es necesario reconocer que la inteligencia artificial está empezando a innovar en diferentes áreas de la ciencia y la tecnología, dentro de estas, el uso del *deepfake* es más frecuente. Sin embargo, estos avances tecnológicos acarrean consigo riesgos que deben ser regulados, especialmente cuando se utilizan de manera indebida. Los *deepfakes* como avance tecnológico pueden llegar a convertirse en un tipo de amenaza significativa para las personas, las instituciones y la sociedad en general si llegan a ser manejados de manera inapropiada.

Como objetivo general de la investigación planteamos que es necesario determinar si hay que regular el uso ilícito de las técnicas de IA, como el *deepfake*.

De manera similar, se establecieron los siguientes objetivos específicos: (I) describir el funcionamiento del *deepfake* como técnica de IA y su uso ilícito; (II) examinar casuísticas recientes de uso ilícito de *deepfake* y cómo se produce el daño; (III) identificar los fundamentos para la tipificación del uso ilícito de *deepfake* como técnica de IA.

Breve origen de la inteligencia artificial

Es relevante mencionar el origen de la inteligencia artificial, también conocida como IA. Este se remonta a los tiempos después de la Segunda Guerra Mundial, cuando se desarrolló la "prueba de Turing", título otorgado en honor a su creador, Alan Turing. Posteriormente, fue John McCarthy quien adoptó el término *inteligencia artificial*.

En un principio, se creía que su uso se limitaría exclusivamente al campo de la ciencia, y que se dirigiría a mejorar y simplificar la existencia del ser humano. Sin embargo, con la introducción de nuevas tecnologías

y las conocidas redes de comunicación y de entretenimiento, su uso empezó a ser cada vez más frecuente en las diversas plataformas de entretenimiento.

Vale precisar que la idea central de la aplicación de la IA era que su uso se diera a través de operaciones simples y primitivas, mediante las cuales se pudieran ir construyendo manifestaciones cada vez más profundas; en contraste con esto, se tiene en consideración que su crecimiento exponencial se atribuye a dos factores fundamentales: los avances especializados de *hardware* que maximizan su rendimiento neuronal y el incremento de datos amplios en línea de bajo costo vía *crowdsourcing*, que impulsan su desarrollo.[1]

Perspectivas internacionales sobre la investigación en inteligencia artificial

La IA designa la capacidad de las máquinas para utilizar algoritmos, aprender de los datos y tomar decisiones de manera similar a los seres humanos.[2] Sin embargo, existen diferencias fundamentales entre las máquinas impulsadas por IA y los humanos: los dispositivos basados en IA no requieren de descanso, puesto que no se fatigan, a diferencia de los seres humanos, que sí necesitan periodos de descanso. Por otra parte, la IA tiene la capacidad de analizar grandes cantidades de datos simultáneamente, así como de identificar patrones y predecir resultados para la toma de decisiones. De igual manera, en algunas áreas, estos dispositivos son más eficientes, teniendo un margen de error considerablemente menor al de los seres humanos, aunque no se encuentran exentos de fallos. Por otra parte, se debe considerar que el ser humano ya hace tiempo ha ido conviviendo con máquinas que reemplazan y mejoran sus habilidades, pero en los últimos años la IA ha experimentado un crecimiento innovador en los procesos rutinarios , lo que ha acarreado daños irreversibles cuando es usada de manera inapropiada o maliciosa, por medio de nuevas aplicaciones que están disponibles para cualquier tipo de usuario, lo que genera preocupación.[3] En el caso de los *deepfakes*, se usan algoritmos automáticos, que producen imágenes plausibles acerca de cómo se vería una persona en un entorno, con una iluminación y con poses particulares. Esto se puede realizar de manera rápida o a través de animaciones faciales basadas en la IA.[4]

En este contexto, existen posturas que consideran a la IA como una prioridad mundial, junto con otros riesgos sociales, como las guerras nucleares y las pandemias.[5] La IA genera preocupación y temor, debido a su capacidad para distorsionar de manera errónea e incorrecta la realidad, por lo que es necesario frenar estos actos antes de que adquieran más poder y que provoquen trastornos sociales. Además, la manipulación y los riesgos asociados con la IA también se utilizan para causar daño personal. Uno de los riesgos más graves son los ataques cibernéticos y la ingeniería social, en los que ciertas personas crean perfiles falsos, mediante algoritmos automáticos, utilizando datos reales, y estos perfiles, posteriormente, llegan a ser manipulados para acceder a datos personales y contraseñas de otros usuarios. Por último, existe el riesgo de la manipulación de imágenes, videos o textos, que pueden ser reutilizados y clonados.[6]

Es verdad que los beneficios de la IA son notoriamente útiles en diferentes ámbitos. Sin embargo, existe un gran número de usuarios que suele usarla con fines ilegales, como la desinformación dirigida a diversos sectores de la sociedad. En muchos casos, hay un conocimiento limitado sobre el uso de las nuevas tecnologías, y para el usuario promedio resulta difícil distinguir entre lo verdadero y lo falso.

En ese sentido, es menester mencionar que el Parlamento Europeo, en relación con el creciente uso de *deepfakes* y de la IA, ha señalado que estas herramientas permiten todo tipo de fraude, especialmente aquellos que implican la suplantación de identidad. En la misma línea, dentro de los sectores más vulnerables que llegan a ser víctimas del uso ilegal de la IA, como los *deepfakes*, se encuentran principalmente mujeres, puesto que tienen un mayor riesgo de sufrir difamaciones, intimidación y extorsión, ya que este tipo de tecnologías suelen utilizarse para intercambiar las caras de las víctimas con las de actrices en videos pornográficos.

Es por esto que, a fin de combatir esta amenaza, se han desarrollado sistemas avanzados. Sin embargo, estos sistemas suelen ser de difícil acceso para el usuario promedio, debido a la complejidad de los algoritmos

involucrados, lo cual es un aspecto importante que debe tenerse en consideración. Es por esto que ahora poder diferenciar entre lo real y lo falso es de vital importancia, puesto que actualmente en las redes sociales, con la creación de *deepfakes*, es necesario desarrollar un sistema sólido que identifique los medios falsos, sin la intervención humana, a fin de reducir información falsa.[7]

Perspectivas nacionales sobre la investigación en inteligencia artificial

Según algunos estudios, la globalización ha llevado a la expansión mundial de la IA. Sin embargo, surge la pregunta sobre si su implementación es esencial para nuestro desarrollo como seres humanos o si, por el contrario, podría representar un riesgo, como algunos sugieren.[8] Es por esto que los avances de la IA deben ser analizados con base en sus implicaciones éticas, ya que la IA no puede dirigirse hacia un deterioro de los derechos fundamentales de las personas, tanto naturales como jurídicas. Si la IA llega a causar daño, nuestro ordenamiento jurídico debe estar dirigido en especial al cuidado de la víctima y debe brindarle a esta una solución eficiente, y no debe centrarse en la hermenéutica jurídica, con el fin de hallar un culpable, y de asignarle una responsabilidad objetiva a quien ocasione daños a través del uso de IA.[9] En contraste con esto, algunas investigaciones refieren que la IA es de naturaleza evasiva, debido a la complejidad e imprevisibilidad de los posibles daños que esta puede generar; sobre todo al momento de determinar una responsabilidad, si existiese, ante los riesgos tecnológicos que se identifican de forma creciente,[10] como los delitos cibernéticos, delitos que son el nuevo paradigma del gran cambio revolucionario tecnológico. Es por eso que los procesos de digitalización deberían ir modelando la modernización del Estado, sobre todo en el campo jurídico, ya que es un gran reto legal regular el uso de las nuevas tecnologías.[11] En este sentido, es cierto que existe incertidumbre jurídica ante la posibilidad de que existan fallas en los procedimientos realizados por la IA; sin embargo, resulta innegable que necesitamos una legislación específica en el ámbito de la IA, aunque pueda parecer anticipado en nuestro país plantear normas legales al respecto. Teniendo en cuenta el contexto global, la aplicación del derecho también cambia en cuanto al desarrollo de la IA, es por esto que es necesario contar con normas específicas sobre la materia.[12]

La IA ha ido en aumento en estos últimos años y ha sorprendido por su capacidad para contribuir en diversas actividades, así como por el hecho de que es usada por un público amplio, que abarca desde estudiantes hasta científicos experimentados, lo que recalca que su uso también puede llegar a ser ilícito y malicioso, como en la creación de fotos y videos falsos, conocidos como *deepfakes*, tema que se abordará más adelante.

Inteligencia artificial ilícita

La IA, aparte de ser una ayuda de manera tecnológica y cibernética, con el tiempo puede trabajar con los servicios públicos y privados a través de la tecnología analítica de reconocimientos y datos, las mismas que lucharán contra el fraude. Por ende, deben desarrollarse y usarse con base en ciertos requisitos éticos y legales, ya que pueden afectar a los derechos de la protección personal y de datos y la propia privacidad.[13] El avance progresivo de la IA se asemeja al desarrollo del *deepfake*, que es una tecnología que genera contenidos extremadamente convincentes, pero falsos. Estos contenidos tienen un alto potencial para causar estragos a gran escala, comenzando por la desinformación, la distorsión narrativa, el fraude y las amenazas. La implementación de la IA resulta sumamente útil en diversos campos científicos, ya que sus aportes permiten encontrar soluciones efectivas para problemas complejos, debido al vasto almacenamiento de información que posee. Asimismo, nuestro ordenamiento jurídico promueve el uso de la IA con el objetivo de fomentar el desarrollo económico y social del país, siempre y cuando se garantice un uso adecuado, ético y responsable.

Sin embargo, no aborda de manera exhaustiva la ilicitud de la IA, especialmente en casos como los *deepfakes*, en los cuales su uso malicioso puede atentar contra la intimidad, la privacidad, la dignidad humana, el pudor público, la estafa y la exposición de datos sensibles, causando daños irreparables a las personas, es por esto que es fundamental que el legislador establezca de manera precisa su ilicitud.

El *deepfake* y su ilicitud: modalidades

El *deepfake* es aquella "falsedad profunda" encargada de utilizar el aprendizaje de la IA para poder, de esa manera, engañar fácilmente, utilizando imágenes, videos y audios; estos últimos serán alterados mediante *softwares* de IA que permitirán darles la apariencia de ser reales u originales. Algunos autores consideran que la implementación de la inteligencia artificial es necesaria, porque permite obtener grandes avances tecnológicos, incluso con su implementación del *deepfake* en el entretenimiento o el uso de la sátira (sarcasmo), en diferentes situaciones o sucesos; siempre y cuando exista un límite al derecho de expresión artística, no sería algo negativo, puesto que su uso es el de entretener al internauta y hacerle pasar por un momento de distracción sana, siempre que su uso no deteriore la integridad ética, moral y psicológica de la persona a quien se le realiza.

Los llamados *deepfakes* son contenidos audiovisuales generados mediante algoritmos de IA, con el objetivo de manipular contenido audiovisual. Su implementación ha aumentado considerablemente el uso de aplicaciones de redes sociales. No obstante, en su mayoría, su finalidad ha sido dañar la reputación de algún individuo o ser utilizados para desinformar en todo el mundo. Es innegable que existen avances en la tecnología *deepfake*, que tienen varias aplicaciones beneficiosas, como en los negocios, el entretenimiento e incluso la industria cinematográfica; no obstante, también pueden cumplir objetivos dañinos y contribuir a socavar la confianza en la verdad.[14]

Por otro lado, el *deepfake* es una de las evoluciones progresivas que amenazan a la sociedad, ya que se conoce como un fenómeno tecnológico emergente en el campo audiovisual que se encuentra al alcance de cualquier usuario. Por lo cual, las principales preocupaciones se derivan del ámbito de los medios, de las plataformas digitales, de las redes sociales y otros; entendiendo que estos productos audiovisuales son falsos, pero se hacen pasar por auténticos. Los *deepfakes* representan un avance tecnológico, pero, por otro lado, esto podría conllevar que esta IA mal utilizada se convierta en una amenaza cada vez más grave para las personas, las organizaciones y la sociedad en su conjunto.[15]

Según la empresa Deeptrace, en un estudio realizado recientemente se menciona que en 2018 se registraron 8000 videos *deepfakes*, los cuales han aumentado actualmente a 14678, en los cuales la mayor parte del material era pornográfico y un 96% se encontraba en línea, superando los 100 millones de vistas; por otra parte, también se mencionó que este tipo de videos se dirige exclusivamente a las mujeres.

Pornografía artificial

Los *deepfakes* pueden ser motivo de preocupación cuando se utilizan para crear pornografía falsa o para difamar a alguien en las redes sociales. En consecuencia, es evidente que los *deepfakes* pueden ser sumamente peligrosos si no se detectan adecuadamente.[16]

Manipulación de identidad

Es la alteración o distorsión de información con el objetivo de influir en la opinión de las personas; recientemente, en Twitter, se difundieron mensajes masivos que promovían inversiones falsas, utilizando la

identidad de personajes famosos, como el actor Antonio Resines. Estos mensajes instaban a los usuarios a invertir en criptomonedas, mediante esquemas fraudulentos que prometían ganancias; no obstante, luego, los usuarios se percataron de que eran estafas. Ahora es difícil detectar lo real de lo falso, por otro lado, detectar *deepfakes* sigue siendo un reto significativo. Aunque las personas confían en su habilidad para diferenciar entre imágenes generadas por la IA y las reales, a menudo enfrentan dificultades para hacerlo.[17]

Sátira del *deepfake*

Se presenta en forma de bromas o una acción graciosa de una situación; sin embargo, la sátira del *deepfake* debe ser abordada desde un punto de vista ético y legal, en cual la creatividad se debe encontrar sujeta a la responsabilidad y en la que ambos elementos se deben encontrar presentes de manera equilibrada, respetando los límites de los derechos fundamentales. No obstante, existen personas que suelen usarlo para engañar y dañar a individuos o audiencias masivas de manera ingeniosa; del mismo modo, estos videos muestran a personas haciendo o defendiendo cosas que nunca hicieron, también suelen hacerse para dañar y engañar a individuos o a auditorios masivos; incluso, hay videos que van dirigidos a personalidades del entretenimiento, empresarios y líderes autoritarios.[18]

Casos de deepfakes ilícitos: una perspectiva comparada

Por otro lado, la amenaza emergente del *deepfake* ha causado revuelo en diferentes partes del mundo; por consiguiente, se han precisado casuísticas notorias en diferentes países, lo que demuestra la prontitud con la que este tipo de amenazas deben ser abordadas, con el fin de proteger a las personas de sus daños potenciales y devastadores.

Un caso que, particularmente, ilustra esta problemática se suscitó en septiembre de 2023, cuando se reportaron víctimas de *deepfake* en el municipio de Almendralejo, provincia de Badajoz, en la región autónoma de Extremadura, España. En esta ocasión, los padres de veinte estudiantes adolescentes denunciaron que sus hijas eran víctimas de imágenes generadas por inteligencia artificial, en las que se las mostraba completamente desnudas, y que estas imágenes se estaban distribuyendo en grupos de WhatsApp a un precio de diez euros. Sin embargo, los expertos señalaron que el código penal español no contiene leyes específicas para abordar estos casos de manera efectiva. Por otra parte, el impacto psicológico en las estudiantes fue profundo, ya que esta situación afectó gravemente su bienestar, y este caso reveló una preocupante brecha en la legislación española, ya que el Código Penal español no aborda específicamente este tipo de delitos digitales, lo que deja a las víctimas en una situación de vulnerabilidad ante estas amenazas. De igual forma, los expertos manifestaron sus preocupaciones y la urgente necesidad de reformar las leyes, para enfrentar de manera efectiva los problemas de los *deepfakes* y proteger a las personas de futuros ataques similares.

El Código Penal español de 1995, en su título X, establece lo siguiente en relación con los delitos contra la intimidad:

> El que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.[19]

La legislación penal española aborda el caso de aquel contenido audiovisual producido inicialmente con el consentimiento de una persona, el cual posteriormente es publicado sin su autorización, ya sea en el ámbito privado de su hogar o en un lugar externo, siendo esta una figura típica del delito de pornografía. Sin embargo, en el caso del *deepfake*, la víctima no participa en la creación del contenido; por el contrario, este es generado por algoritmos de IA sin su conocimiento, lo que crea un vacío legal significativo. A pesar de esta diferencia,

el resultado es el mismo: ambos delitos atentan contra la intimidad personal, al divulgar material falso o manipulado. En relación con esto, es importante destacar que la Unión Europea está trabajando en la primera normativa específica sobre IA, enfocada en su uso. En este contexto, sería relevante que nuestro ordenamiento jurídico también adoptara figuras legales relacionadas con la IA. De igual forma, Chile ha presentado un proyecto de ley que pretende incorporar el uso de la IA como un factor agravante en la comisión de delitos dentro de su código penal.

Los *deepfakes* se han convertido en una herramienta de engaño global, que afecta a víctimas a nivel internacional y nacional, las cuales pueden ser desde figuras públicas hasta ciudadanos comunes. Nadie está exento de ser víctima de esta tecnología disruptiva, ya que su impacto trasciende fronteras y contextos sociales.

En el 2021, la famosa escritora británica H. M. fue víctima de un *deepfake* mediante el uso de inteligencia artificial, en el que se crearon imágenes sexuales explícitas de su persona, las cuales se difundieron ampliamente en las redes sociales. Estos eventos provocaron pesadillas, traumas y ansiedad en la afectada. A pesar de intentar emprender acciones legales, la modalidad específica de la que fue víctima no está tipificada en su país.

Una docente de derecho de la Universidad Royal Hollay de Londres, con respecto a este tipo de delitos, mencionó que "tal acción sería típica siempre y cuando la foto o video sea original, privado y sexual". A este respecto, Aislinn O'Connell, en una entrevista reciente con la BBC, hizo alusión al caso de las veinte menores del municipio de Almendralejo, mencionado anteriormente: "El escándalo en un pequeño pueblo de España por las imágenes de decenas de niñas y jóvenes desnudas generadas por IA".[20] Por otro lado, Chile presentó un proyecto de ley que pretende incorporar en el código penal chileno el uso ilícito de la inteligencia artificial como un factor agravante de los delitos. Esta iniciativa refleja una creciente preocupación regional por las repercusiones legales de la tecnología emergente y del uso ilícito de la IA. Paralelamente, en nuestro país, un incidente en un colegio de Chorrillos ilustra la relevancia de esta problemática. En este caso, dos estudiantes de aproximadamente quince años tomaron imágenes de sus compañeras de las redes sociales y utilizaron *deepfakes* para crear y distribuir contenidos con connotación sexual, los cuales eran vendidos clandestinamente a sus pares por montos que oscilaban entre los 15 y 30 soles. Este caso evidencia la necesidad de una respuesta legal y educativa ante estos actos ilícitos.

En contraposición, el exministro del Interior y presidente de la Red Peruana contra la Pornografía Infantil, Dimitri Senmache, manifestó en una entrevista reciente con el diario *La República*, llamada "El peligro de la pornografía *deepfake*", lo siguiente: "En el Congreso habían cuatro proyectos de ley que promovían el uso de la IA en el Perú [...] ninguna de esas iniciativas aborda los nuevos riesgos que trae la IA".[21]

Mientras tanto, nuestro ordenamiento jurídico en relación con los delitos informáticos y el tráfico ilegal de datos, refiere lo siguiente:

> El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.[22]

Del mismo modo, se regula la figura de la suplantación de identidad estableciendo lo siguiente:

> El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.[23]

Dentro de los dos supuestos, se habla sobre las bases de datos, pero se hace un mayor enfoque en la parte informática, económica o de difamación, y no tanto en el contenido de la esfera sexual generada por IA.

De igual forma, el ordenamiento jurídico peruano regula la figura de la manipulación genética, que prescribe que toda persona que haya manipulado genéticamente para clonar a otro ser humano será sancionada. Con respecto a esto, el *deepfake* es una manipulación de la herramienta tecnológica del IA, la

cual no se encuentra aún tipificada en el ordenamiento jurídico para que sea sancionada. He aquí que se visualiza la manipulación tecnológica para poder desvirtuar a la persona a través de plataformas y aplicaciones de internet.[24]

En síntesis, se puede precisar que nuestro código penal peruano aborda la manipulación de seres humanos desde un enfoque científico y no tecnológico. Mientras que la manipulación que realiza el *deepfake* es tecnológica, ya que para usarlo no es necesario de un conocimiento previo de ciencia, sino el empleo de una tecnología. De esta manera, es más accesible para cualquier persona que puede hacer uso de un aparato tecnológico, reduciendo ciertos requisitos en cuanto al agente del delito, puesto que incluso un menor de edad podría cometer tal ilícito penal sin ninguna dificultad.

De igual forma, en el segundo supuesto se encuentra más relacionado con el uso de IA, pero desde un punto de vista ambientado en los prejuicios que tienen consecuencias materiales, por lo que no se hace mención a la parte psicológica o moral que suelen padecer las diversas víctimas de su uso ilegal.

Del mismo modo, después de haber precisado los aportes de la IA y las formas en las que es usada para fines maliciosos o ilícitos, a continuación, se plantearán algunos elementos que pueden ayudar a regular el uso indebido de los *deepfakes*.

Fundamentos para la regulación del *deepfake*

El Dr. Frank Almanza y el Dr. Óscar Peña, reconocidos por su capacidad de explicar la teoría del delito de forma breve y comprensible, afirman que el delito, en su concepción jurídica, es todo acto humano voluntario que se adecua al presupuesto jurídico de una ley penal[25] y que consiste en una conducta humana prohibida por un dispositivo legal que la expresa. Además, el delito adquiere este carácter solo cuando la conducta "se adecue" a esa fórmula legal.[26] Teniendo en cuenta que la teoría del delito aceptada es aquella que dice que el delito es aquella conducta, típica, antijurídica y culpable, esto implica que la conducta de quien comete el delito debe ser tipificada en la ley, por ir en contra de del ordenamiento jurídico y por su consecuencia ser culpable o reprochable penalmente; por otra parte, para que aquella conducta del ser humano sea considerada como penalmente relevante, es necesario que dicho acto se encuentre tipificado dentro de los marcos legales y morales, por ir en contra de leyes existentes y establecidas como delitos. De igual forma, en nuestro código penal se refiere el principio de legalidad, que establece que nadie puede ser sancionado por un acto que no esté antes definido como delito en la ley; del mismo modo, el principio de prohibición del uso de analogías refiere que no se permite el uso de estas para calificar un hecho como delito o definir un estado de peligrosidad. Esto quiere decir que, sin una norma que regule un comportamiento específico, no se puede juzgar a una persona por ese acto, puesto que no se encuentra regulado.

Es por esto que la IA tiene que ser tomada como una prioridad mundial junto a otros riesgos sociales, como las guerras nucleares y la pandemia; ya que esta puede generar preocupación y temor con la difusión desinformada errónea de la realidad, la cual se debe de frenar antes de que tome poder y que provoque un trastorno social.[27] La IA no debe ser usada en contraposición a los derechos fundamentales, ya que, en caso de que esta pueda ocasionar perjuicios, nuestro ordenamiento jurídico debe estar enfocado en la víctima, para proporcionar una solución eficiente y asignarle una responsabilidad objetiva a aquellos que puedan ocasionar daños a través del uso de la IA.

En vista de lo expuesto, nuestro ordenamiento jurídico establece que la IA debe usarse de manera ética, por lo que no debe transgredir la privacidad de las personas y debe actuar de manera segura, para que se pueda lograr un impacto positivo en la sociedad. No obstante, cuando esta herramienta tiene como propósito generar contenido que perjudique la imagen de una persona, afectando su reputación; obtener beneficios económicos por su comercio, o ser utilizado para desinformar, deber ser considerada ilícita, puesto que está transgrediendo la dignidad de la persona, siendo este el fin supremo de nuestra sociedad y del Estado.

En la siguiente sección hablaremos sobre los efectos psicológicos de estos actos, especialmente, sobre la necesidad de una regulación más estricta para prevenir abusos de la IA.

Producción del daño

El incremento de los *deepfakes*, especialmente cuando son malintencionados (pornografía artificial), en las redes sociales y en sitios web maliciosos ha permitido causar en las víctimas daños psicológicos y emocionales, así como angustia y humillación.

En este contexto, la lesión que sufre la persona va directamente dirigida a su honor, su reputación y sus sentimientos; estas y esta es causada por otra persona con la modalidad de culpabilidad o dolosa.[28]

Por ello, en el tipo de violencia que se genera a través de las plataformas de internet y de los mecanismos de la tecnología, las víctimas se ven perjudicadas de manera psicológica, ya que experimentan una violencia invisible no expresada a través de agresiones físicas, pero que sí es susceptible de ser identificada.[29]

Cabe mencionar que las víctimas en su mayoría son de sexo femenino de distintas edades y que son las mismas que después de este maltrato o daño psicológico sufren ciertas repercusiones, como el temor de mirarse al espejo, de salir a las calles, de ir a los centros educativos superiores, de dirigirse a los centros laborales y, al final, pierden todo tipo de comunicación con su entorno social, llegando a reprimirse socialmente y a tener una idea distorsionada de su realidad.

Por lo tanto, al no existir una ley que regule directamente la figura del *deepfake* mediante el uso de IA, se estaría permitiendo el detrimento de la integridad moral de una persona, el perjuicio de su imagen y se afectaría su beneficio económico con su circulación.

Metodología

La metodología se basó en un desarrollo de tipo básico, este tipo de investigación está centrado en la exploración de nuevos conocimientos sin una finalidad práctica inmediata y específica. Su objetivo principal es descubrir principios y leyes científicas, lo que puede eventualmente contribuir a la formulación de una teoría científica.[30] El método de investigación se divide en el planteamiento del problema, la teoría que sustenta el problema y el diseño, en los cuales se incluyen datos, análisis y procedimientos de interpretación para emitir recomendaciones y conclusiones.[31] Del mismo modo, en el proceso de recolección de datos es necesario analizar minuciosamente los datos, que generalmente se obtienen mediante métodos como entrevistas, observaciones y análisis de documentos.[32]

Por lo tanto, el enfoque de la investigación fue cualitativo, ya que se buscaba estudiar los diferentes objetos para poder comprender la vida social y adquirir conocimientos. El enfoque cualitativo se sustenta en evidencias para orientar la descripción profunda del fenómeno que tiene como finalidad comprender y explicar las aplicaciones metodológicas y técnicas derivadas de conceptos y fundamentos epistemológicos.[33]

Correspondiente a ello, el diseño no experimental se caracteriza por no manipular intencionalmente las variables que se estudian. En lugar de esto, observa los fenómenos tal como ocurren en su contexto actual, para luego analizarlos. Para clasificar la investigación no experimental, utilizamos la dimensión temporal, es decir, consideramos el número de momentos o puntos en el tiempo en los cuales se recopilan los datos.[34] Esta metodología es inductiva, ya que busca generar o establecer teorías a partir de datos, comenzando por la pregunta y la recopilación de datos cualitativos, y, posteriormente, se contrastan las teorías existentes con las emergentes.[35] Ante esto, es aquel "método versátil", que se regirá por la recolección de información y de datos para establecer la teoría, el que constituye una recopilación y un análisis por medio de un proceso arduo de investigación.[36]

Además, este método se divide en categorías y subcategorías, las mismas que permitirán definir la investigación. De este modo, estos pasos metodológicos son los que tienden a ordenar los elementos que constituyen analítica e interpretativamente la investigación[37], por lo que se plantearon las siguientes categorías: 1) uso ilícito de la IA, que se detallará con el desarrollo de las subcategorías de I) formas y II) casuística; 2) *deepfake*, que se desarrollará con las subcategorías de I) fundamentación de su tipificación, II) uso ilícito y III) producción del daño.

Nuestro escenario de estudio abarcó las ciudades de Cajamarca y Trujillo. Estos lugares proporcionan un contexto relevante para nuestra investigación, ya que, son las ciudades donde se encuentran los investigadores. En cuanto a los participantes, se tuvo en consideración a los siguientes expertos del derecho, que contribuyeron de manera significativa al estudio: dos fiscales; un asistente en función fiscal; un docente universitario, quien aportó conocimiento teórico práctico, y cuatro abogados litigantes, quienes nos ofrecieron su amplia experiencia en el campo del derecho.

La muestra, conformada por ocho especialistas, se considera adecuada para cumplir con el objetivo de nuestra investigación. No incluimos a otros especialistas de otras ramas del derecho, ya que sus contribuciones podrían no ser significativas en este contexto específico. Dado que nuestro enfoque es cualitativo y no estadístico, esta selección se basó en el criterio del investigador.

Para la recolección de información, la técnica se basó en la búsqueda de información (indexada y científica) en repositorios universitarios y en citas bibliográficas, y se empleó el análisis documental. De tal manera, se realizaron entrevistas, las cuales nos facilitarán la organización de las etapas para la interpretación de la investigación. Esto se hizo teniendo en cuenta que "la técnica es la herramienta que está destinada a la recogida de datos para el enfoque de la investigación con criterio estructural".[38]

El instrumento se adaptó al cuestionario de entrevistas y a la guía de análisis de documentos. Estos elementos se utilizaron para estructurar las unidades de análisis (categorías y subcategorías), así como para interpretar los objetivos del estudio. Además, se consideraron las respuestas proporcionadas por los especialistas entrevistados, y su posterior análisis.

Por lo tanto, el procedimiento de la investigación se llegó a regir desde la realidad problemática, la recolección de información, la misma que emplea la técnica de análisis documental e instrumental de la ficha documental, la cual estará referida a tres casos en específicos, dos internacionales y uno nacional.

Cada guía de análisis documental o ficha documental estuvo compuesta por categorías, subcategorías, análisis e interpretación. Las categorías se han derivado de datos y las subcategorías lo hacen a medida que se continúa la explicación sobre la elaboración de las categorías citadas.

Es de vital importancia mencionar que la compilación de la información se hizo a partir de fuentes documentales bibliográficas, en la biblioteca virtual y otras instituciones nacionales e internacionales, siendo las consultas bibliográficas las encargadas de definir el tema, la búsqueda de los materiales, la recopilación de análisis críticos, la estructura de la investigación y las conclusiones.[39] Así mismo, el procedimiento permite alcanzar el fin con un conocimiento racional sistemático y organizado, ya que el modelo del trabajo es de secuencia lógica y está orientado hacia la investigación.[40]

Por lo tanto, se realizaron entrevistas a ocho expertos en derecho penal mediante un cuestionario y luego se realizó un análisis de cada uno; posteriormente, se crearon tablas, de las cuales se obtuvieron datos cualitativos que luego fueron analizados en la sección de discusión y resultados y objetivos del estudio de investigación. Finalmente, se realizaron recomendaciones y conclusiones útiles para el desarrollo del proyecto de investigación.

El rigor científico es la fase metodológica de la que se obtienen los datos cualitativos válidos y confiables que fueron utilizados en la investigación, ya que incluye la planificación, el desarrollo y el análisis del proyecto y se adhiere a un protocolo de actuación con impacto demostrativo con argumentos basados en evidencia.[41]

En el método de análisis de información se aplicó el procedimiento, la recopilación y el lineamiento, con la finalidad de que se analicen e interpreten los objetos de estudio de las categorías y subcategorías. La información se ampara en el i) método analítico, que permitió el estudio en profundidad de los objetos de estudio separados de las categorías de estudio, para sacar conclusiones fiables más adelante; en el ii) método hermenéutico, con el que se realizó una interpretación reflexiva de la figura del *deepfake* en el derecho peruano y la necesidad de su regulación; por último, iii) en el método inductivo-deductivo, con el que se efectuó la construcción cognitiva sobre el *deepfake* en el derecho, desde lo general a lo particular.

En el aspecto ético, en comparación con los progresos de la ciencia y la investigación, la indagación científica académica nos brinda una visión de las restricciones inherentes a la ciencia y la investigación. Estas limitaciones deben ser tenidas en cuenta al momento llevar a cabo cualquier estudio.[42] Asimismo, se respetaron los derechos de autor y la correcta estructura de citación, el cual cautela los derechos de autor de los expertos citados.

De tal manera que, para nuestro proyecto de investigación, se cumplió con los objetivos expuestos durante la recolección de resultados obtenidos mediante la utilización de fundamentos en revistas científicas, libros, tesis y artículos de repositorios de diversas universidades a nivel nacional e internacional, respetando las normas de la American Psychological Association (APA). Es importante señalar de manera precisa y concisa que en el proyecto se han citado a los diversos autores de manera adecuada, respetando su derecho de autor y teniendo en cuenta que el trabajo de investigación no debe exceder el 20% de plagio, con el fin de respetar las investigaciones previas.

Resultados

Para desarrollar los resultados de nuestra investigación, creamos figuras y tablas que facilitaron la visualización y el análisis de la información recopilada, así como las perspectivas y opiniones proporcionadas por los entrevistados. A continuación, presentamos los resultados organizados según los tres objetivos específicos que nos planteamos.

Objetivo específico 1

En el marco del objetivo específico 1 (Figura 1), se realizaron las siguientes preguntas: ¿tiene información sobre el *deepfake*? Desde su experiencia como profesional, ¿cuáles son las razones para que el uso ilícito de las técnicas de la IA, como el *deepfake*, se incremente en el futuro? ¿El *deepfake* ilícito va en contra la dignidad de la persona? ¿Por qué el *deepfake*, incluido su uso ilegal, es accesible para todas las edades, incluidos los menores?

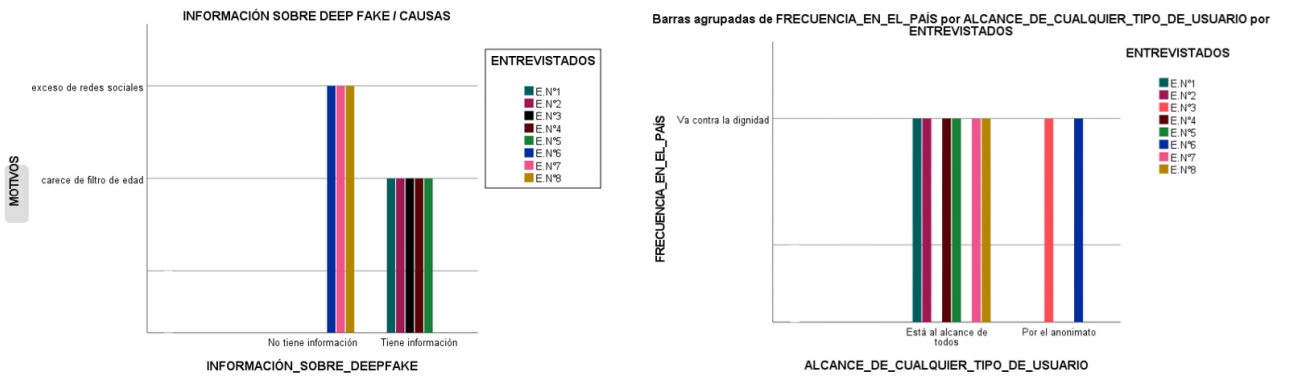

FIGURA 1.
Conocimiento previo de especialistas sobre *deepfake* y sus causas
Fuente: elaboración propia.

Interpretación

De los resultados obtenidos, se aprecia que el 62,5% de los entrevistados tenía conocimiento previo acerca del *deepfake* y considera que es una tecnología emergente con propósitos legítimos; sin embargo, lamentaba su uso incorrecto. No obstante, el 37,5% de los entrevistados encontraron el *deepfake* como un tema nuevo o reciente, y lo describieron como intrigante e interesante, afirmando que es vital comprenderlo a profundidad. De igual forma, el 100% de entrevistados coincidió en que el uso ilegal de *deepfakes* afecta la dignidad de las personas, asociando este acceso al uso excesivo de redes sociales (sobre todo por parte de menores), en las que se comparte información indebida. Por otro lado, el 25% de los entrevistados cree que el acceso a *deepfakes* se lleva a cabo de manera anónima y que dichas aplicaciones electrónicas carecen de mecanismos o filtros de control de edad efectivos o de mecanismos de verificación adecuados.

Objetivo específico 2

Para la elaboración del objetivo específico 2, se realizó la siguiente tabla sobre casuística reciente (Tabla 1).

TABLA 1.
Análisis documental de casuística relevante

País	Año	Hechos	Daño producido
Reino Unido	2021	Helen Mort fue víctima de un *deepfake* elaborado a través de la IA, en el que se crearon y se difundieron de forma masiva imágenes sexuales explícitas falsas de ella en redes sociales. Esto le causó pesadillas, traumas y ansiedad.	• Pesadillas • Depresión • Ansiedad • Traumas • La imagen • La reputación
Estados Unidos	2024	Taylor Swift fue objeto de un *deepfake* generado por una IA, en el que se crearon imágenes suyas de manera explícita y se difundieron en las redes sociales.	
Estados Unidos	2024	Scarlett Johansson también fue objeto de un *deepfake* en el que se usó su rostro para generar películas para adultos a través de la IA.	
Italia	2024	Giorgia Meloni, primera ministra de Italia, fue víctima de un *deepfake* para simular videos para adultos, el cual fue difundido en internet.	
España	2023	Alumnas menores de edad fueron víctimas de *deepfakes* generados por la IA, en los que se las mostraba completamente desnudas. Dichas imágenes se distribuyeron por grupos de WhatsApp a un precio de diez euros.	
Perú	2023	En un colegio del distrito de Chorrillos, se descubrió que dos estudiantes adolescentes de quince años comercializaban fotos alteradas con connotación sexual de compañeras del mismo centro de estudio, las cuales fueron elaboradas mediante el uso de un *deepfake* (IA). Estas imágenes fueron vendidas entre sus compañeros a un precio de entre quince y treinta soles.	

Fuente: elaboración propia.

Interpretación

En los casos más recientes de *deepfakes* en países como Reino Unido, Estados Unidos, Italia, España y Perú, se evidencia que la mayoría de las víctimas son personas famosas en campos como el arte, la música o la actuación. Además, también se ven afectados personajes políticos, como la primera ministra de Italia. Sin embargo,

lo más preocupante es la presencia significativa de menores, que sufren daños psicológicos debido a estas prácticas malintencionadas. En todos los casos, las personas afectadas experimentaron pesadillas, depresión, ansiedad y traumas, además de ver afectada su imagen y su reputación.

Objetivo específico 3

Para la elaboración del objetivo específico 3 se realizaron las siguientes preguntas: según su experiencia profesional, ¿cree que las repercusiones sociales, morales y económicas del uso ilícito de *deepfake* justifican su inclusión como delito en el código penal?, ¿debería considerarse el uso ilícito de *deepfake* como un delito independiente en el código penal o, tratarse como un agravante dentro de los delitos existentes?, ¿es imprescindible incorporar el uso ilícito de *deepfake* como una figura penal específica en nuestro ordenamiento jurídico? (Figura 2).

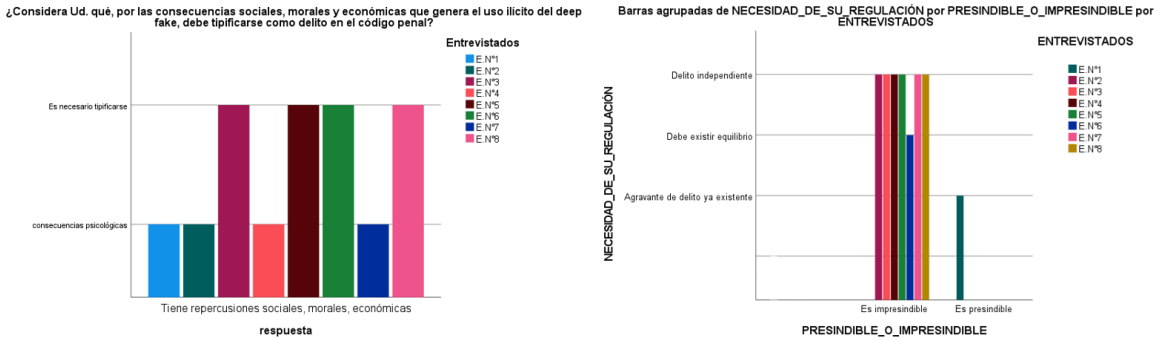

FIGURA 2.
Consecuencias en el ámbito social, moral y económico del uso ilícito del ***deepfake*** y su tipificación
Fuente: elaboración propia con base en las entrevistas aplicadas a los especialistas.

Interpretación

De los resultados obtenidos, se obtuvo que el 100% de los entrevistados coincidieron en que el uso ilícito del *deepfake* ocasiona repercusiones sociales, morales y económicas, estando así justificado para que sea incluido como un delito en nuestro ordenamiento jurídico. Del mismo modo, el 75% de los entrevistados consideró que es imprescindible que el *deepfake* sea regulado como un delito independiente, puesto que presenta desafíos únicos que merecen leyes específicas, ya que eso permitiría aplicaciones efectivas y proporcionales según la gravedad de los contextos, sin depender de otras disposiciones legales; no obstante, el 12,5% de los entrevistados discrepó de esta opinión, porque consideró que existen delitos similares, siendo la opción más práctica el adecuarlos, por lo que considera que no es prescindible tipificarlo como un delito independiente.

Discusión

Después de obtener los resultados observados, es factible iniciar la fase de discusión, sin perder de vista el objetivo general: describir el funcionamiento de los *deepfakes* como una técnica de inteligencia artificial, así como su uso ilícito. Además, contextualizamos este análisis en un marco más amplio. Esto se abordó a través de entrevistas a especialistas (Figura 1), mediante las cuales se mostró que la mayor parte de los entrevistados coincidieron en que el *deepfake* es un tipo de tecnología emergente que tiene como finalidad crear archivos totalmente falsos, con las identidades de las personas, aunque tiene un propósito legítimo cuando se aplica en el campo del cine y de la creatividad. Sin embargo, lamentan que sea usado de manera inapropiada o ilícita para

difamar, dañar la imagen personal y acosar a personas, mediante la creación de videos falsos que las muestran realizando acciones inadecuadas. De igual forma, consideraron que en un futuro el uso ilícito del *deepfake* como técnica de la IA será más frecuente en nuestro país y que se podría volver en algo habitual, dado que la IA está en evolución y es una tendencia que está obteniendo cada día más adeptos; paralelamente, advierten que esta herramienta está al alcance de usuarios de todas las edades, incluidos los menores de edad, los cuales usan las redes sociales frecuentemente y no siempre se encuentran supervisados por un adulto responsable.

La situación mencionada está respaldada por una investigación que se encuentra previamente citada, la cual aborda el tema de los *deepfakes*, y refiere que estos son contenidos audiovisuales generados mediante algoritmos de IA que tienen como objetivo manipular contenido audiovisual y que en su mayoría tienen como finalidad dañar la reputación de algún individuo o desinformar en todo el mundo. Así mismo, concluye que, aunque los avances en la tecnología del *deepfake* tiene varias aplicaciones beneficiosas para campos como el de los negocios, del entretenimiento o, incluso, de la industria cinematográfica, también pueden cumplir objetivos dañinos y contribuir a la falta de credibilidad en la verdad.[43] De forma análoga, se ha señalado que la IA ha experimentado un incremento de manera innovadora en los procesos rutinarios, pero que también ha causado daños irreversibles, debido a su mala utilización, ya que, a través de aplicaciones nuevas dirigidas y disponibles al alcance de cualquier usuario, es usada de manera inapropiada o maliciosa, y puede causar daños irreversibles, lo que genera preocupación.[44]

De manera similar, se ha señalado que los *deepfakes* representan evoluciones progresivas, que amenazan a la sociedad, ya que se conocen como un fenómeno tecnológico emergente en el campo audiovisual que se encuentra al alcance de cualquier usuario. Por este motivo, las principales preocupaciones se derivan del ámbito de los medios, de las plataformas digitales, de las redes sociales, entre otros, en los que los *deepfakes* generalmente son entendidos como productos falsos, que se hacen pasar por auténticos. Si bien *deepfakes* representan un avance tecnológico, su uso indebido podría llevar a que se conviertan en una amenaza cada vez más grave para las personas, las organizaciones y la sociedad en su conjunto.[45]

En relación con objetivo específico 2, que estuvo enfocado en examinar casuísticas recientes sobre el uso ilícito de *deepfakes* y el tipo de daño que producen (Tabla 1). A partir del análisis documental de la casuística, se obtuvo que los *deepfakes* en países como Reino Unido, Estados Unidos, Italia, España y Perú dan como resultado que la mayoría de las víctimas son personas famosas que trabajan en campos como el arte, la música o la actuación. Además, también se vieron afectados personajes políticos, como la primera ministra de Italia. Sin embargo, lo más preocupante es la presencia significativa de menores que sufren daños psicológicos debido a estas prácticas malintencionadas. En todos los casos, se experimentaron pesadillas, depresión, ansiedad y traumas, además de que las personas implicadas vieron afectada su imagen y su reputación.

En consecuencia, lo expuesto previamente está relacionado con la investigación realizada en 2024, en la que se menciona que la difusión de un *deepfake* sexual puede causar daños psicológicos en la víctimas, las cuales pueden requerir tratamiento médico, en especial cuando se trata de menores.[46] De manera similar, se ha señalado que los *deepfakes* pueden ser motivo de preocupación cuando son usados para crear pornografía falsa o para difamar a alguien en redes sociales y que son sumamente peligrosos cuando no son detectados adecuadamente. En este orden de ideas, la empresa Deeptrace mencionó que la mayor parte del *deepfakes* está compuesta por material pornográfico, que de este un 96% se encuentra en línea y que este tipo de videos se dirigen exclusivamente a las mujeres.[47]

En esa misma línea, se ha afirmado que la lesión que suele sufrir una persona va directamente contra su honor, su reputación, sus sentimientos. Estas son las mismas lesiones que son causadas por otra persona con la modalidad de culpabilidad o dolo.[48]

En cuanto a los objetivos específicos 3 y 4, se logró identificar los fundamentos para la tipificación del uso ilícito del *deepfake* como técnica de la IA. A través de entrevistas realizadas a especialistas, se pudo evidenciar que la mayor parte de entrevistados coincidieron en que el uso ilícito del *deepfake* produce repercusiones

sociales, morales y económicas, y que es de imperiosa necesidad que se tipifique como un delito, ya que causa daños psicológicos muy graves, haciendo que las víctimas experimenten sentimientos profundos de ansiedad. También es necesario que sea evaluado cuidadosamente desde el punto de vista legal, para encontrar un equilibrio entre la libertad de expresión y la protección de los derechos fundamentales. Por otra parte, la mayor parte de los entrevistados consideraron que el *deepfake* debería ser regulado como un delito independiente, debido a que presenta desafíos únicos que merecen leyes específicas. Estas últimas permitirían llevar a cabo aplicaciones efectivas y proporcionales de acuerdo con la gravedad de los contextos analizados, garantizando medidas de protección y reparación adecuadas para las víctimas, sin que estas dependan de otros apartados legales, pero estableciendo un equilibrio que permita una aplicación efectiva y proporcional en función de los distintos escenarios que se presenten. Finalmente, los especialistas coincidieron en su mayoría en que es imprescindible tipificar el uso ilícito del *deepfake* como un delito independiente, ya que eso permitiría implementar una protección más efectiva de los derechos fundamentales, teniendo en cuenta que es una amenaza emergente que se encuentra en evolución y que no debería existir debate sobre su aplicación.

En este sentido, los avances de la IA no pueden dirigirse hacia el deterioramiento de los derechos fundamentales de las personas, ya que si la IA llega a causar daño, nuestro ordenamiento jurídico debe proteger la víctima y brindarle una solución eficiente, y asignar una responsabilidad objetiva a quien ocasione daños a través del uso de la IA.[49] Por otro lado, indubitablemente existe la necesidad de contar con la legislación específica en IA, y, aunque pareciese anticipado en nuestro país plantear normas legales a este respecto, teniendo en cuenta el contexto global, la aplicación del derecho también cambia en cuanto al desarrollo de la IA, y es por esto que es necesario contar con normas específicas que la aborden.[50]

Por otra parte, la IA debe ser tomada como una prioridad mundial junto con otros riesgos sociales, ya que algunos de sus usos pueden llegar a generar preocupación, por lo que estos deben ser frenados antes de que tomen poder y provoquen trastornos sociales.[51]

Conclusiones

Es necesario regular el uso ilícito de las técnicas de IA como el *deepfake*, debido a que existe un uso excesivo de las redes sociales, en las que generalmente se comparte información generada por *deepfakes*. Por tal motivo, es crucial implementar un sistema legal que incluya requisitos éticos y legales específicos que regulen su uso, puesto que, si estos materiales no son tratados adecuadamente, pueden llegar a amenazar organizaciones, personajes públicos o, incluso, a la sociedad en general, incluidos los menores de edad, por lo que este es un asunto de prioridad mundial.

El funcionamiento del *deepfake* como técnica de IA y su uso ilícito consiste en aquella "falsedad profunda" que, a través de redes neuronales, algoritmos o *softwares*, utiliza el aprendizaje de la IA para crear contenido audiovisual falso con las identidades de las personas. Sin embargo, su uso es lícito en los campos del cine y de la creatividad, pero se convierte en ilícito cuando es implementado para engañar y dañar a individuos o a audiencias masivas, así como para difundir información falsa o crear pornografía artificial comercializada.

El fenómeno del *deepfake* afecta no solo a artistas famosos, escritores y políticos, sino también a menores de edad. Estos últimos, tras verse involucrados en situaciones de *deepfake*, experimentaron daños psicológicos, pesadillas, ansiedad y traumas, lo que afectó significativamente su imagen y su reputación.

Finalmente, los fundamentos para la tipificación del *deepfake* que se identificaron en este artículo son que estos acarrean consecuencias a nivel social, moral y económico, por lo que es fundamental regularlo como un delito independiente en el código penal, mediante el establecimiento de figuras legales propias que se adapten a la gravedad de los contextos, sin depender de otras figuras legales, para garantizar un equilibrio entre la libertad de expresión y la protección de los derechos fundamentales.

Referencias

Adrián Enrique Hernández Muñoz, Miguel Ángel Alexandro Rangel Alvarado, Lenin Torres García, Gustavo Hernández Martínez, Pierre Kalid Castillo Ixta, Leticia Lizzet Olivares Moreno y Andrea Guadalupe Sánchez Morales, *Proceso para la realización de una revisión bibliográfica en investigaciones clínicas*, Digital Ciencia UAGRO (julio de 2022), https://revistas.uaq.mx/index.php/ciencia/article/view/686

Alejandro Morales Cáceres, *El impacto de la inteligencia artificial en el derecho*, Advocatus (marzo de 2021), https://doi.org/10.26439/advocatus2021.n39.5117

Andrés Abeliuk y Claudio Gutiérrez, *Historia y evolución de la inteligencia artificial*, Revista Bits de Ciencia 14 (2021), https://revistasdex.uchile.cl/index.php/bits/article/view/2767

Ángeles Jareño Leal, *El derecho a la imagen íntima y el Código penal: la calificación de los casos de elaboración y difusión del* deepfake *sexual*, Revista Electrónica de Ciencia Penal y Criminología, Revista Electrónica de Ciencia Penal y Criminología (abril de 2024), https://dialnet.unirioja.es/servlet/articulo?codigo=9537441

Antonio Rodríguez Rosado, *Rigor científico, pertinencia y relevancia en los artículos científicos*, Revista Prisma Social (julio de 2024). https://revistaprismasocial.es/

Aurelio Recuenco y William Reyes, *Inteligencia artificial: camino a un nuevo esquema del mundo*, 23 SCIÉNDO 299 (2020), https://doi.org/10.17268/sciendo.2020.036

Carlos Sabino, *El proceso de investigación* (Ed. Panapo, 1992).

Carmelo Hernández Ramos, Vicente Magro Servet y J. Pablo Cuéllar Otón, *El maltrato psicológico. Causas, consecuencias y criterios jurisprudenciales. El problema probatorio* (Instituto de Capacitación Judicial del Supremo Tribunal de Justicia de Sinaloa, 2014), http://hdl.handle.net/10045/46929

Casiano Highton, *Los daños derivados de la inteligencia artificial y del impacto de las nuevas tecnologías* (Pontificia Universidad Católica Argentina, 2020).

Christian Dennis Valero Quispe, *Derecho e inteligencia artificial en el mundo de hoy: escenarios internacionales y los desafíos que representan para el Perú*, 79 Themis. Revista de Derecho 311 (2021), https://doi.org/10.18800/themis.202101.017

Código Penal Español [CPE]. Ley Orgánica 10/1995. 23 de noviembre 1995 (España).

Código Penal Peruano [CPP]. Decreto Legislativo 1545 de 2023. Art. 324. 22 de noviembre de 2023 (Perú).

Cristina Romero Chaves, *La categorización un aspecto crucial en la investigación cualitativa*, Revista de Investigaciones Cesmag 113 (junio de 2005), https://biblioteca.unicesmag.edu.co/digital/revinv/0123-1340v11n11pp113.pdf

Manuel E. Cortés Cortés y Miriam Iglesias León, *Generalidades sobre metodología de la investigación* (Ed. Universidad Autónoma del Carmen, Colección Material Didáctico, 2004), https://www.unacar.mx/contenido/gaceta/ediciones/metodologia_investigacion.pdf

Eryn J. Newman y Norbert Schwarz, *Misinformed by images: How images influence perceptions of truth and what can be done about it*, 56 Curr Opin Psychol 101778 (2024), https://doi.org/10.1016/j.copsyc.2023.101778

Fabio Anselmo Sánchez Flores, *Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos*, 13 Revista Digital de Investigación en Docencia Universitaria 101 (enero de 2019), http://dx.doi.org/10.19083/ridu.2019.644

Frank Almanza Altamirano y Óscar Peña Gonzales, *Teoría del delito: manual práctico para su aplicación en la teoría del caso* (Ed. Asociación Peruana de Ciencias Jurídicas y Conciliación [APECC], 2010).

Gülselin Güler y Sedef Gündüz, *Deep learning based fake news detection on social media*, 12 IJISS (2023), https://doi.org/10.55859/ijiss.1231423

Guy Hedgecoe, *El escándalo en un pequeño pueblo de España por las imágenes de decenas de niñas y jóvenes desnudas generadas por IA*, BBC News Mundo (25 de septiembre de 2023), https://www.bbc.com/mundo/articles/cz9r6792k13o

Hugo Bernal Huayhua Quispe, *Los retos legales del Perú en la era de la revolución tecnológica e inteligencia artificial* (Red de Repositorios Latinoamericanos, 2022).

Hugo Sánchez Carlessi, Carlos Reyes Romero y Katia Mejía Sáenz, *Manual de términos en investigación científica, tecnológica y humanística* (Ed. Universidad Ricardo Palma, 2018).

Jacob Bañuelos Capistrán, *Deepfake: la imagen en tiempos de la posverdad*, 2 Revista Panamericana de Comunicación 51 (2020), https://doi.org/10.21555/rpc.v0i1.2315

Joshua Glick, *Deepfake Satire and the Possibilities of Synthetic Media*, 50 Afterimage 81 (2023), https://doi.org/10.1525/aft.2023.50.3.81

Juana Ojeda de López, Johana Quintero y Ineida Machado, *La ética en la investigación*, 9 Telos 345 (mayo de 2007), http://www.redalyc.org/articulo.oa?id=99318750010

Kevin Roose, *Los líderes del sector advierten sobre el "riesgo de extinción" de la inteligencia artificial* (NYT, 2023).

Lasse Rouhiainen, *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro* 15-32 (Alienta Editorial, 2018).

Ley 30096 de 2013. Ley de delitos informáticos. 22 de octubre de 2013. D. O. No. 505484.

Ley 30096 de 2013. Ley de delitos informáticos. 22 de octubre de 2013. D. O. No. 505484.

Luz Marina Carmona Rave y Laura Valencia Ruiz, *Valoración del daño psicológico en el contexto jurídico colombiano*, 7 Revista de Psicología Universidad de Antioquia 147 (julio de 2015), https://doi.org/10.17533/udea.rp.325210

Mario Gonzáles Arencibia y Dagmaris Martínez Cardero, *Soluciones educativas frente a los dilemas éticos del uso de la tecnología Deep Fake*, 1 Revista Internacional de filosofía teoría y práctica 99 (mayo de 2024), https://doi.org/10.51660/riftp.v1i1.22

Mike Seymour, Lingyao Yuan, Alan Dennis y Kai Riemer, *Facing the Artificial: Understanding Affinity, Trustworthiness, and Preference for More Realistic Digital Humans*, Hamilton Library, 4673 (2020), https://hdl.handle.net/10125/64316

Mizanur Rahman, Harold Jan Terano, Nafizur Rahman, Aidin Salamzadeh y Saidur Rahaman, *ChatGPT and Academic Research: A Review and Recommendations Based on Practical Examples*, SSRN (2023).

Narcisa Dolores Piza Burgos, Francisco Alejandro Amaiquema Márquez y Gina Esmeralda Beltrán Baquerizo, *Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias*, 15 Conrado 455 (diciembre de 2019), http://conrado.ucf.edu.cu/index.php/conrado

Nicolás Pascual de la Parte, *Ciberseguridad europea con sabor español*, Revista SIC Ciberseguridad, Seguridad de la Información y Privacidad (2023).

Óscar Miranda, *El peligro de la pornografía deepfake*, La República (3 de septiembre de 2023), https://larepublica.pe/domingo/2023/09/03/el-peligro-de-la-pornografia-deepfake-porno-chorrillos-inteligencia-artificial-111374

Óscar Alejandro Palacios Rodríguez, *La teoría fundamentada: origen, supuestos y perspectivas*, Intersticios Sociales 47 (2021), https://www.redalyc.org/journal/4217/421769000003/

Paulina Iveth Vizcaíno Zúñiga, Ricardo Javier Cedeño Cedeño y Israel Alejandro Maldonado Palacios, *Metodología de la investigación científica: guía práctica*, 7 Ciencia Latina 9723 (septiembre de 2023), https://doi.org/10.37811/cl_rcm.v7i4.7658

Pedro Morales Corrales y Alejandro Morales Cáceres, *El impacto de las nuevas tecnologías en las relaciones laborales*, IUS et Praxis 39 (2021), https://doi.org/10.26439/iusetpraxis2021.n052.5072

Percy Jesús Sánchez Loayza y Miguel Ángel Zúñiga Marino, *Necesidad de regulación de la inteligencia artificial en la responsabilidad civil extracontractual en el Perú, 2021*, (Universidad Tecnológica del Perú, 2022).

Ricardo De La Espriella Guerrero y Carlos Gómez Restrepo, *Teoría fundamentada*, 49 Revista Colombiana de Psiquiatría 126 (2020), https://www.elsevier.es/es-revista-revista-colombiana-psiquiatria-379-articulo-teoria-fundamentada-S0034745018300891

Ricardo Nieves, *Teoría del delito y práctica penal* (Ed. Editora Centenario S.A, 2010).

Rimsha Rafique, Rahma Gantassi, Rashid Amin, Jaroslav Frnda, Aida Mustapha y Asma Hassan Alshehri, *Deep fake detection and classification using error-level analysis and deep learning*, 13 Scientific reports (2023), https://doi.org/10.1038/s41598-023-34629-3

Sebastián Ríos, *Los riesgos de la inteligencia artificial*, 72 Mensaje 40 (2023).

Victor Lahoud S., *Metodología de la investigación científica* 1 Odontología Sanmarquina 51 (2001), https://sisbib.unmsm.edu.pe/bvrevistas/odontologia/2001_n8/pdf/metologia_investigacion_cientifica.pdf

Notas

* Artículo de revisión científica.

1 Andrés Abeliuk y Claudio Gutiérrez, *Historia y evolución de la inteligencia artificial*, Revista Bits de Ciencia 14 (2021).

2 Lasse Rouhiainen, *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro* 15-32 (Alienta Editorial, 2018).

3 Casiano Highton, *Los daños derivados de la inteligencia artificial y del impacto de las nuevas tecnologías* (2020).

4 Mike Seymour, Lingyao Yuan, Alan Dennis y Kai Riemer, *Facing the Artificial: Understanding Affinity, Trustworthiness, and Preference for More Realistic Digital Humans* 4673 (Hamilton Library, 2020).

5 Kevin Roose, *Los líderes del sector advierten sobre el "riesgo de extinción" de la inteligencia artificial* (NYT, 2023).

6 Sebastián Ríos, *Los riesgos de la inteligencia artificial* 40 (Universidad Alberto Hurtado, 2023).

7 Gülselin Güler y Sedef Gündüz, *Deep learning based fake news detection on social media* (IJISS, 2023).

8 Aurelio Recuenco y William Reyes, *Inteligencia artificial: camino a un nuevo esquema del mundo* 299 (SCIÉNDO, 2020).

9 Pedro Morales Corrales y Alejandro Morales Cáceres, *El impacto de las nuevas tecnologías en las relaciones laborales* 39 (Advocatus, 2021).

10 Percy Jesús Sánchez Loayza y Miguel Ángel Zúñiga Marino, *Necesidad de regulación de la inteligencia artificial en la responsabilidad civil extracontractual en el Perú, 2021* (Universidad Tecnológica del Perú, 2022).

11 Hugo Bernal Huayhua Quispe, *Los retos legales del Perú en la era de la revolución tecnológica e inteligencia artificial* (Red de Repositorios Latinoamericanos, 2022).

12 Christian Dennis Valero Quispe, *Derecho e inteligencia artificial en el mundo de hoy: escenarios internacionales y los desafíos que representan para el Perú,* Themis Revista De Derecho 311 (2021).

13 Nicolas Pascual de la Parte, *Ciberseguridad europea con sabor español*, Revista SIC Ciberseguridad, Seguridad de la Información y Privacidad 5 (2023).

14 Rimsha Rafique, Rahma Gantassi, Rashid Amin, Jaroslav Frnda, Aida Mustapha y Asma Hassan Alshehri, *Deep fake detection and classification using error-level analysis and deep learning, Scientific reports* (2023).

15 Jacob Bañuelos Capistrán, *Deepfake: la imagen en tiempos de la posverdad*, Revista Panamericana de Comunicación 51 (2020).

16 Mizanur Rahman, Harold Jan Terano, Nafizur Rahman, Aidin Salamzadeh y Saidur Rahaman, *ChatGPT and Academic Research: A Review and Recommendations Based on Practical Examples*, SSRN, 1 (2023).

17 Eryn J. Newman y Norbert Schwarz, *Misinformed by images: How images influence perceptions of truth and what can be done about it* 101778 (Elsevier BV, 2024).

18 Joshua Glick, *Deepfake Satire and the Possibilities of Synthetic Media* 81 (Afterimage, 2023).

19 Código Penal Español [CPE], Ley Orgánica 10/1995, 23 de noviembre de 1995 (España).

20 Guy Hedgecoe, *El escándalo en un pequeño pueblo de España por las imágenes de decenas de niñas y jóvenes desnudas generadas por IA*, BBC News Mundo (25 de septiembre de 2023).

21 Oscar Miranda, *El peligro de la pornografía deepfake,* La República (3 de septiembre de 2023).

22 Ley 30096 de 2013. Ley de delitos informáticos. 22 de octubre de 2013. D. O. No. 505484.

23 Ley 30096 de 2013. Ley de delitos informáticos. 22 de octubre de 2013. D. O. No. 505484.

24 Código Penal Peruano [CPP], Decreto Legislativo 1545 de 2023, art. 324, 22 de noviembre de 2023 (Perú).

25 Frank Almanza Altamirano y Óscar Peña Gonzales, *Teoría del delito: manual práctico para su aplicación en la teoría del caso* 62 (Ed. Asociación Peruana de Ciencias Jurídicas y Conciliación [APECC], 2010).

26 Ricardo Nieves, *Teoría del delito y práctica penal* 39 (Ed. Editora Centenario S.A., 2010).

27 Roose, supra nota 6.

28 Luz Marina Carmona Rave y Laura Valencia Ruiz, *Valoración del daño psicológico en el contexto jurídico colombiano*, Revista de Psicología Universidad de Antioquia 147 (julio de 2015).

29 Carmelo Hernández Ramos, Vicente Magro Servet y J. Pablo Cuéllar Otón, *El maltrato psicológico. Causas, consecuencias y criterios jurisprudenciales. El problema probatorio* 27 (Instituto de Capacitación Judicial del Supremo Tribunal de Justicia de Sinaloa, 2014).

30 Hugo Sánchez Carlessi, Carlos Reyes Romero y Katia Mejía Sáenz, *Manual de términos en investigación científica, tecnológica y humanística* 79 (Ed. Universidad Ricardo Palma, 2018).

31 Victor Lahoud S., *Metodología de la investigación científica* 41 (Odontología Sanmarquina, 2001).

32 Paulina Iveth Vizcaíno Zúñiga, Ricardo Javier Cedeño Cedeño y Israel Alejandro Maldonado Palacios, *Metodología de la investigación científica: guía práctica*, Ciencia Latina 9723 (septiembre de 2023).
33 Fabio Anselmo Sánchez Flores, *Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos*, Revista Digital de Investigación en Docencia Universitaria 101 (enero de 2019).
34 Manuel E. Cortés Cortés y Miriam Iglesias León, *Generalidades sobre metodología de la investigación* 10, 27 (Ed. Universidad Autónoma del Carmen, Colección Material Didáctico, 2004).
35 Óscar Alejandro Palacios Rodríguez, *La teoría fundamentada: origen, supuestos y perspectivas*, Intersticios Sociales.
36 Ricardo De La Espriella Guerrero y Carlos Gomez Restrepo, *Teoría fundamentada,* Revista Colombiana de Psiquiatría 126 (2020).
37 Cristina Romero Chaves, *La categorización un aspecto crucial en la investigación cualitativa*, Revista de Investigaciones Cesmag 113 (junio de 2005).
38 Narcisa Dolores Piza Burgos, Francisco Alejandro Amaiquema Marquez y Gina Esmeralda Beltrán Baquerizo, *Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias,* Conrado 455 (diciembre de 2019).
39 Adrián Enrique Hernández Muñoz, Miguel Ángel Alexandro Rangel Alvarado, Lenin Torres García, Gustavo Hernández Martínez, Pierre Kalid Castillo Ixta, Leticia Lizzet Olivares Moreno y Andrea Guadalupe Sánchez Morales, *Proceso para la realización de una revisión bibliográfica en investigaciones clínicas,* Digital Ciencia UAGRO 50 (julio de 2022).
40 Carlos Sabino, *El proceso de investigación* 25 (Ed. Panapo, 1992).
41 Antonio Rodríguez Rosado, *Rigor científico, pertinencia y relevancia en los artículos científicos,* Revista Prisma Social (julio de 2024).
42 Juana Ojeda de López, Johana Quintero y Ineida Machado, *La ética en la investigación,* Telos 345 (mayo de 2007).
43 Rafique, Gantassi, Amin, Frnda, Mustapha y Hassan Alshehri, *supra* nota 15.
44 Highton, *supra* nota 4.
45 Bañuelos Capistrán, *supra* nota 16, pág. 51.
46 Ángeles Jareño Leal, *El derecho a la imagen íntima y el código penal: la calificación de los casos de elaboración y difusión del deepfake sexual*, Revista Electrónica de Ciencia Penal y Criminología, Revista Electrónica de Ciencia Penal y Criminología 1 (abril de 2024).
47 Rahman, Jan Terano, Rahman, Salamzadeh y Rahaman, *supra* nota 17, pág. 1.
48 Carmona Rave y Valencia Ruiz, *supra* nota 29, pág. 147.
49 Alejandro Morales Cáceres, *El impacto de la inteligencia artificial en el derecho*, Advocatus 39 (marzo de 2021).
50 Valero Quispe, *supra* nota 13, pág. 311.
51 Roose, *supra* nota 6.

Cómo citar: Homero Pracedes Jondec Briones, María Eugenia, Zevallos Loyaga, Adolfo Yesser Segura Grados y Erika Milagros Castrejon Vilchez, *El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el* deepfake, 73 Vniversitas (2024). https://doi.org//10.11144/Javeriana.vj73.uiti