



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
ESCUELA PROFESIONAL DE DERECHO



TESIS

**Los deepfakes como nueva modalidad delictiva de
suplantación de identidad con el uso de inteligencia
artificial**

Autor:

Bach. Ayasta Gonzales, Edwin Joel

Asesor:

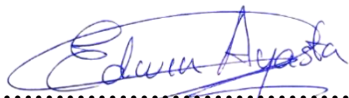
Dr. Vargas Rodríguez, César

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

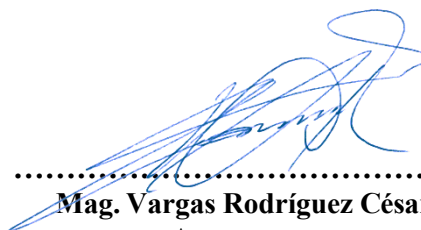
Fecha de Sustentación: 06 de Julio del 2026

LAMBAYEQUE, 2026

Tesis denominada “Los deepfakes como nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial” presentada para optar El TITULO PROFESIONAL DE ABOGADO, por:



.....
Bach. Ayasta Gonzales Edwin Joel
Autor

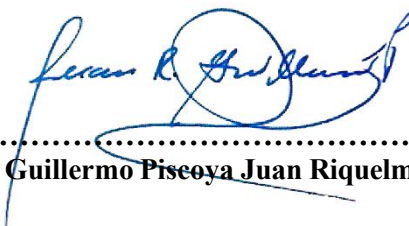


.....
Mag. Vargas Rodríguez César
Asesor

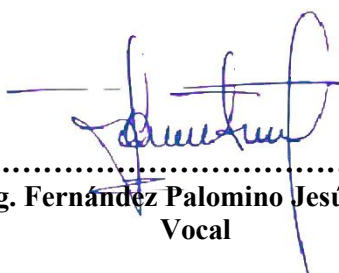
APROBADO POR:



.....
Dr. Chavarry Correa Ezequiel Baudelio
Presidente



.....
Dr. Guillermo Piscoya Juan Riquelme
Secretario



.....
Mag. Fernández Palomino Jesús Alicia
Vocal

DEDICATORIA

La presente investigación
está dedicada a mis padres Eulogio
y Lucía, que, con mucho esfuerzo
y dedicación, siempre buscaron la
forma de apoyarme en todo mi
camino para lograr ser un
profesional. Ambos son mi fuente
de inspiración y motivación, pues
de ustedes aprendí que con
perseverancia y trabajo duro se
pueden alcanzar las metas.

AGRADECIMIENTO

Agradezco a Dios por haberme dado la salud, sabiduría y la fuerza de voluntad necesaria, para llegar hasta este último escalón de mi etapa de pregrado.

De la misma forma le doy gracias a mis hermanos, que me enseñaron a ser fuerte y a no rendirme nunca, gracias por confiar en mí y brindarme su apoyo incondicional en cada paso de mi camino académico.



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE DERECHO Y CIENCIA POLITICA
UNIDAD DE INVESTIGACION



ACTA DE SUSTENTACIÓN

A C T A DE SUSTENTACIÓN PRESENCIAL N° 75 – 2026 -UI-FDCP

Sustentación para optar el Título de profesional de ABOGADO de: **Edwin Joel Ayasta Gonzales**.

Siendo las 7:00 p.m. del día lunes 06 de julio del 2026 se reunieron en el Sala de simulación de audiencias de la Facultad de Derecho y Ciencia Política de la Universidad Nacional “Pedro Ruiz Gallo”, los miembros del jurado evaluador de la tesis titulada: “**LOS DEEPFAKES COMO NUEVA MODALIDAD DELICTIVA DE SUPLANTACIÓN DE IDENTIDAD CON EL USO DE INTELIGENCIA ARTIFICIAL**”, designados por Resolución N° 006-2024-FDCP-VIRTUAL de fecha 05 de enero del 2024, con la finalidad Evaluar y Calificar la sustentación de la tesis antes mencionada, por parte de los Señores Catedráticos:

PRESIDENTE : Dr. EZEQUIEL BAUDELIO CHAVARRY CORREA.

SECRETARIO : Dr. JUAN RIQUELME GUILLERMO PISCOYA.

VOCAL : Mag. JESÚS ALICIA FERNÁNDEZ PALOMINO

La tesis fue asesorada por Mag. CESAR VARGAS RODRIGUEZ, nombrado por Resolución N° 006-2024-FDCP-VIRTUAL de fecha 05 de enero del 2024.

El acto de sustentación fue autorizado por Resolución 457-2026-FDCP-VIRTUAL de fecha 06 de julio del 2026.

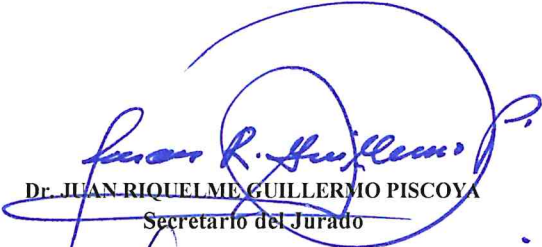
La tesis fue presentada y sustentada por el bachiller **Edwin Joel Ayasta Gonzales** y tuvo una duración de 30 minutos. Después de la sustentación y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva, obteniendo el siguiente resultado: **APROBADO** con la nota de **17 (diecisiete)** en la escala vigesimal, mención de **BUENO**.

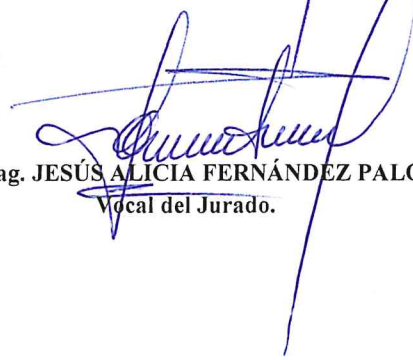
Por lo que queda **APTO** para obtener el Título Profesional de ABOGADO, de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Derecho y Ciencia Política, y la Universidad Nacional Pedro Ruiz Gallo.

Siendo las **08:15 p.m.**, del mismo día, se da por concluido el acto académico tomando la juramentación respectiva y suscribiendo el Acta los miembros del jurado.

Lambayeque, lunes 06 de julio del 2026


Dr. EZEQUIEL BAUDELIO CHAVARRY CORREA
Presidente del Jurado


Dr. JUAN RIQUELME GUILLERMO PISCOYA
Secretario del Jurado


Mag. JESÚS ALICIA FERNÁNDEZ PALOMINO
Vocal del Jurado.

CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD

Yo, CESAR VARGAS RODRIGUEZ usuario revisor de:

Tesis ☒

Trabajo de Suficiencia Profesional ☐

Trabajo Académico ☐

Titulado: “LOS DEEPFAKES COMO UNA NUEVA MODALIDAD DELICTIVA DE SUPLANTACIÓN DE IDENTIDAD CON EL USO DE INTELIGENCIA ARTIFICIAL”

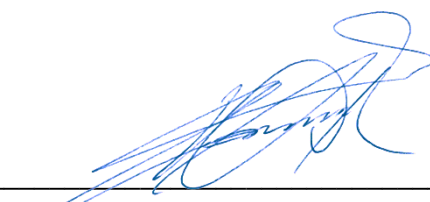
Cuyo(s) autor(es) es(son):

EDWIN JOEL AYASTA GONZÁLES DNI N° 76780906, declaro que la evaluación realizada por el Programa informático, ha arrojado un porcentaje de similitud 16%, verificables en el Resumen del Reporte Automatizado de similitudes que se acompaña.

El (La/Los/Las) suscrito(a/s/as) analizó y concluyó que cada una de las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio y que el documento cumple con la integridad científica y con las normas para el uso de citas y referencias establecidas en los protocolos respectivos.

Se cumple con adjuntar el Recibo Digital a efectos de la trazabilidad respectiva del proceso.

Lambayeque, 08 de julio del 2026.



Nombres y Apellidos: César Vargas Rodríguez
DNI N° 16484422
ASESOR

Defina la modalidad con (x)

Adjuntar

- *Reporte Automatizado de similitudes*
- *Recibo Digital*

Los deepfakes como nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial

INFORME DE ORIGINALIDAD

16%	15%	3%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unprg.edu.pe	4%
	Fuente de Internet	
2	rpc.up.edu.mx	2%
	Fuente de Internet	
3	cuti.org.uy	1%
	Fuente de Internet	
4	dspace.uib.es	1%
	Fuente de Internet	
5	1library.co	<1%
	Fuente de Internet	
6	hdl.handle.net	<1%
	Fuente de Internet	
7	seon.io	<1%
	Fuente de Internet	
8	www.lisanews.org	<1%
	Fuente de Internet	
9	core.ac.uk	
	Fuente de Internet	


Abog. CESAR VARGAS RODRIGUEZ
DNI: 16484422
ASESOR



Recibo digital

Este recibo confirma que su trabajo ha sido recibido por **Turnitin**. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega: Edwin Joel Ayasta Gonzales
Título del ejercicio: Quick Submit
Título de la entrega: Los deepfakes como nueva modalidad delictiva de suplantac...
Nombre del archivo: INFORME_FINAL_EDWIN_JOEL_AYASTA_GONZALES.docx
Tamaño del archivo: 349.72K
Total páginas: 77
Total de palabras: 14,724
Total de caracteres: 82,847
Fecha de entrega: 27-nov.-2024 01:10p. m. (UTC-0500)
Identificador de la entrega... 2534119124



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO



TESIS

Los deepfakes como nueva modalidad delictiva de
suplantación de identidad con el uso de inteligencia
artificial

Autor:
Bach. Ayasta Gonzales, Edwin Joel

Asesor:
Dr. Vargas Rodriguez, César

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGA

Fecha de sustentación
LAMBAYEQUE, 2024



Abog. CESAR VARGAS RODRIGUEZ
DNI: 16484422
ASESOR

ÍNDICE

DEDICATORIA	3
AGRADECIMIENTO	4
RESUMEN	7
ABSTRACT.....	8
INTRODUCCIÓN	9
CAPITULO I: ASPECTOS METOLOGICOS	11
1. REALIDAD PROBLEMÁTICA.....	11
1.1. Planteamiento del problema.....	11
1.2. Formulación del problema	14
1.3. Justificación e importancia del estudio	14
1.3.1. Justificación.....	15
1.3.2. Importancia.....	15
1.4. Objetivos.....	16
1.4.1. Objetivo General	17
1.4.2. Objetivos Específicos	17
1.5. Hipótesis	17
1.6. Variables	18
1.6.1. Variable independiente.....	18
1.6.2. Variable dependiente	18
1.7. Métodos, técnicas e instrumentos de recolección de datos	18
1.7.1. Métodos.....	18
1.7.1.1. Métodos generales.....	19
1.7.1.2. Métodos específicos	20
1.7.2. Técnicas.....	21
1.7.3. Instrumentos	22

CAPITULO II: MARCO CONCEPTUAL	23
PARTE I: ANTECEDENTES DEL PROBLEMA	23
PARTE II: BASES TEÓRICAS DE LOS DELITOS INFORMATICOS	26
Delitos informáticos.....	26
Sujeto pasivo	32
CAPITULO III: ANÁLISIS DE RESULTADOS	53
3.1. Resultados en tablas y figuras.....	53
CAPITULO IV: CONTRASTACIÓN DE LA HIPÓTESIS	64
4.1. Discusión de los resultados	64
II. CONCLUSIONES.....	71
III. RECOMENDACIONES.....	72
REFERENCIAS.....	73

Resumen

El estudio conlleva como título “Los deepfakes como nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial” con el propósito de demostrar como en la realidad peruana el deepfakes viene siendo utilizado como una nueva modalidad de actos delictivos, pues el mal uso de la inteligencia artificial (IA) puede tener consecuencias negativas en diversos ámbitos, incluyendo la privacidad, la seguridad y la ética. El uso incorrecto de la IA podría dar lugar a la comisión de un delito, que variará según los hechos supuestamente cometidos. Por ejemplo, el uso de la IA para la generación de contenido visual sin la debida atribución o autorización puede constituir un delito de plagio o infracción de derechos de autor. Es por ello que se propuso como objetivo general, Describir de qué manera el uso de los deepfakes pueden ser utilizados como una nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial. Cabe mencionar que todo ello fue posible porque se utilizó como estructura metodológica a los Método Inductivo, Método Deductivo y Método Histórico. Logrando de esta manera concluir que, los deepfakes representan una evolución preocupante en la suplantación de identidad, utilizando la inteligencia artificial para crear engaños casi indetectables que pueden ser utilizados para fines delictivos.

Palabras Claves: Deepfakes, Inteligencia, Artificial, Delito, Identidad

Abstract

The study is titled “Deepfakes as a new criminal modality of identity theft with the use of artificial intelligence” with the purpose of demonstrating how in the Peruvian reality deepfakes are being used as a new modality of criminal acts, since misuse . of artificial intelligence (AI) can have negative consequences in various areas, including privacy, security and ethics. Incorrect use of AI could lead to the commission of a crime, which will vary depending on the acts allegedly committed. For example, the use of AI to generate visual content without proper attribution or authorization may constitute the crime of plagiarism or copyright infringement. That is why the general objective was proposed to describe how the use of deepfakes can be used as a new criminal modality of identity theft with the use of artificial intelligence. It is worth mentioning that all of this was possible because the Inductive Method, Deductive Method and Historical Method were used as a methodological structure. In this way, we conclude that deepfakes represent a worrying evolution in identity theft, using artificial intelligence to create almost undetectable deceptions that can be used for criminal purposes.

Keywords: Deepfakes, Intelligence, Artificial, Crime, Identity

INTRODUCCIÓN

Los avances tecnológicos han evolucionado constantemente a lo largo de los años. Esta evolución tiene como propósito principal innovar la tecnología y proporcionar distintos beneficios a los ciudadanos. No obstante, aunque se obtienen numerosos beneficios, también han surgido circunstancias en las que la tecnología se ha utilizado para llevar a cabo acciones delictivas, como el cibercrimen, los fraudes en línea y los delitos financieros, entre otros. Un ejemplo de esto es el caso de los deepfakes, que representan una nueva modalidad delictiva de suplantación de identidad mediante el uso de inteligencia artificial.

En la actualidad, la inteligencia artificial, como avance tecnológico de la ciencia informática que ofrece respuestas inmediatas, ha llevado a que algunas personas utilicen esta herramienta para cometer nuevas acciones delictivas. Un ejemplo de esto es la suplantación de identidad mediante deepfakes, una modalidad que requiere ser sancionada y regulada de manera eficiente para que de esta manera se pueda prevenir la vulneración de los derechos fundamentales de los ciudadanos, que vienen siendo los más afectados.

Tomando en cuenta lo mencionado previamente en los párrafos anteriores, fue necesario que la investigación se encuentre constituida en su primer capítulo, todo lo relacionado a los aspectos metodológicos, esto incluye la realidad problemática, la misma formulación del problema, los cuales originaron la redacción de justificación e importancia del estudio, de terminación tanto del objetivo principal como los específicos, la misma hipótesis, las variables de estudios y por ultimo todo los métodos generales y específicos que formaron parte del estudio.

Con respecto al segundo capítulo, se puede confirmar que estuvo constituido por el marco conceptual, el cual tiene como base a los antecedentes de estudio, las distintas bases teóricas que se encuentra totalmente relacionado tanto con la variable independiente: Los deepfakes como nueva modalidad delictiva, y por otro lado la variable dependiente, el cual hace mención a la Suplantación de identidad, cabe precisar que en este apartado investigativo, se tuvo en consideración distintas bases doctrinales, como jurisprudencia y legislación.

Seguidamente, se desarrolló el tercer capítulo investigativo, en el cual se tuvo en consideración tanto el análisis e interpretación de todas las respuestas que fueron posible obtener a través de la encuesta aplicada a los expertos que fueron seleccionados, cabe precisar que estos resultados fueron detallados tanto en tablas y gráficos que permitieron su mejor entendimiento.

Con respecto al cuarto capítulo investigativo, se procedió a realizar la respectiva discusión de los resultados, en el cual se tuvo en cuenta tanto a los objetivos, resultados y distintas investigaciones, que permitieron triangular las ideas y datos obtenidos para demostrar la viabilidad investigativa.

Como penúltimo punto desarrollado, se tuvo en cuenta la redacción de las conclusiones, las cuales estuvieron totalmente relacionados a los objetivos investigativo, para que de esta forma se puede corroborar la importancia y viabilidad del estudio.

Por último, se redactaron las respectivas recomendaciones, con el único objetivo de poder establecer mecanismos nuevos que permitan subsanar la problemática que ha sido estudiada.

CAPITULO I: ASPECTOS METOLOGICOS

1. REALIDAD PROBLEMÁTICA.

1.1. Planteamiento del problema

El mal uso de la inteligencia artificial (IA) puede tener consecuencias negativas en diversos ámbitos, incluyendo la privacidad, la seguridad y la ética. Su uso incorrecto podría dar lugar a la comisión de un delito, que variará según los hechos supuestamente cometidos. Por ejemplo, el uso de esta inteligencia para la generación de contenido visual sin la debida atribución o autorización puede constituir un delito de plagio o infracción de derechos de autor.

Además, el uso de la IA para la toma de decisiones automatizadas puede generar discriminación y sesgos, lo que puede tener consecuencias negativas para las personas afectadas. Es importante considerar las implicaciones éticas, legales y sociales de su uso y garantizar que su desarrollo y aplicación se realicen de manera responsable y sostenible. En este sentido, se han establecido marcos éticos y legales para guiar su correcto uso, como los principios de ética de la IA de la Unión Europea y la Ley de Protección de Datos Personales como por ejemplo lo hace Brasil.

Un informe de 2020 del Centro de IA y Robótica del Instituto Interregional de Investigación de Justicia y Delincuencia de las Naciones Unidas señaló que en foros clandestinos se estaban observando tendencias relacionadas con el abuso de la inteligencia artificial y el aprendizaje automático (machine learning), que podrían intensificarse en un futuro próximo. Entre

estas tendencias se encontraba la imitación de comportamiento humano en las redes sociales. Hoy en día, esas predicciones ya se han concretado y, en muchos casos, han superado lo que se había anticipado.

El uso de la tecnología y de la información ha sido beneficioso en nuestro país gracias al desarrollo de la era digital. Sin embargo, con el tiempo se han adoptado nuevas formas de cometer delitos, como la Suplantación de Identidad, el cual se encuentra regulado en el artículo 9 de la Ley 30096 de Delitos Informáticos.

El avance tecnológico cada vez es más fácil con el acceso a internet pues esto permite que diversas personas obtengan información relevante para realizar informes, del mismo modo alterar información, suplantar identidad y entre otras formas que permitan evadir determinados parámetros y derechos de una persona, sin embargo, existen tanto profesionales como estudiantes que de forma fácil realizan estas acciones sin darse cuenta el daño que generan literariamente a la persona suplantando su identidad, y todo ello por el hecho de no acarrear una sanción efectiva que permita proteger a las víctimas (Soto, 2012).

Cabe mencionar que se ha utilizado la tecnología de la información para implementar una nueva técnica llamada "Deepfake"(son todos aquellos videos, foto o audios, generados por una técnica de inteligencia artificial) , que amenaza la identidad y la seguridad de los cibernautas en el mundo digital. Al acceder a fotos y audios de una persona, se pueden crear videos hiperrealistas manipulando tanto su rostro como su voz, lo que crea una

percepción de realidad que daña la imagen, el audio y la identidad de la persona. (Rimaicuna, 2021)

El término "aprendizaje profundo" y "fake" (falsificación), se fusionaron para formar el término "deepfake". Se refiere a una técnica sofisticada impulsada por Inteligencia artificial, que permite la creación de contenido multimedia que parece real, pero en realidad es ficticio. Cabe mencionar que los deepfakes pueden alterar el discurso de una persona en un audio, superponer caras en videos e incluso crear imágenes realistas de personas que nunca existieron utilizando algoritmos de aprendizaje profundo. (Rimaicuna, 2021)

Cabe mencionar que, durante estos primeros casos, la tecnología deepfake, los cuales son una manifestación avanzada de la tecnología digital que combina IA con medios manipulados, creando un desafío tanto técnico como ético en la era actual. ha crecido rápidamente y se ha extendido ampliamente en los últimos años, lo que incluso ha llamado la atención del FBI (Organismo internacional de investigaciones de los EE.UU). Es importante reconocer que la agencia estadounidense emitió una alerta a principios de 2023 después de notar un aumento en las denuncias de falsos videos para adultos que "protagonizan" las víctimas a partir de imágenes o videos que los delincuentes obtenían de sus redes sociales.

La evolución tecnológica en los últimos años ha puesto en peligro la autenticidad de las imágenes, los audios y los videos. Por lo tanto, reforzar la atención en las formas en que nos comunicamos a distancia, a través de cualquier modalidad, es crucial. Como se ha demostrado, el objetivo

principal de la ingeniería social son las personas. Por lo tanto, la principal medida de seguridad para evitar ser víctimas de estos ataques debería centrarse en las acciones del usuario.

Como se ha venido desarrollando la investigación, se puede asegurar que en la legislación peruana no existen adecuado mecanismo que permitan asegurar o proteger el bienestar de los ciudadanos ante estas nuevas actividades ilícitas de los deepfakes que afectan directamente la identidad de una persona, y de forma general trasgrede sus derechos fundamentales que se encuentran respaldados y protegidos por la constitución.

1.2. Formulación del problema.

¿De qué manera los Deepfakes podrán ser configurados como una nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial?

1.3. Justificación e importancia del estudio.

1.3.1. Justificación.

La investigación se justificó desde una técnica teórica, debido a que la suplantación de identidad es uno de los actos delictivos que está establecido por dos vertientes, por una parte, la afectación y vulneración de los derechos de la víctima y por otro lado el beneficio ilícito obtenido por el sujeto activo.

Desde una técnica espacial, la problemática de estudio está dirigida a la falta de sanción a las nuevas modalidades de suplantar la identidad

como es hoy en día el deepfakes, que es una nueva modalidad de inteligencia artificial que permite suplantar tanto el rostro, voz y entre otros aspectos de una persona para hacerlo pasar como si fuera dicha persona, sin embargo ante estos avances tecnológicos se puede demostrar que no existen adecuado mecanismos que permitan sancionar y a la vez combatir esta problemática, es por ello que el estudio está dirigido a establecer parámetros para su respectiva sanción.

Desde una técnica jurídica, totalmente justificable por el tan solo hecho, que esta dirigido a delimitar penalmente la nueva figura jurídica de los Deepfakea como acto delictivo de suplantación de identidad con el uso de inteligencia artificial, y de este modo reducir los actos delictivos que se vienen dando a causa de la falta de delimitación normativa en relación a los delitos informáticos.

Desde una técnica operacional, la investigación aplicara método de análisis de datos, así como la revisión adecuada de bibliografía y elementos que ayuden a evidenciar y buscar una solución al problema.

1.3.2.Importancia

La investigación es de gran importancia, ya que a través de ello se logrará establecer nuevas alternativas que permita asegurar y proteger la identidad de una persona y de esta manera las nuevas modalidades de suplantación de identidad a causa de la deepfakes de

la inteligencia artificial.

La regulación de los deepfakes es imperativa no solo para proteger derechos individuales, sino también para salvaguardar la integridad social y política en un entorno digital. La creación de un marco legal específico, acompañado por tecnología avanzada para su detección y una mayor concienciación pública, son pasos necesarios para abordar los desafíos que presenta esta innovadora pero potencialmente peligrosa tecnología.

1.4. Objetivos.

Los objetivos investigativos son enunciados claros y específicos que definen lo que se pretende lograr con un estudio, sirviendo como guía para el diseño y desarrollo de la investigación. Estos objetivos pueden clasificarse en generales y específicos, donde el objetivo general establece la meta principal y los objetivos específicos detallan los pasos concretos necesarios para alcanzarla. La importancia de los objetivos radica en que proporcionan un enfoque estructurado y coherente, permitiendo a los investigadores concentrar sus esfuerzos y recursos de manera efectiva. Además, facilitan la evaluación del progreso y los resultados de la investigación, asegurando que se aborden las preguntas planteadas y se logre una comprensión más profunda del fenómeno estudiado. En resumen, los objetivos investigativos son fundamentales para orientar el proceso de investigación y asegurar su relevancia y aplicabilidad.

1.4.1. Objetivo General.

Describir de qué manera el uso de los deepfakes pueden ser utilizados como una nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial.

1.4.2. Objetivos Específicos.

1. Comparar el uso de los deepfakes a nivel nacional e internacional
2. Acreditar en qué circunstancias se genera la suplantación de identidad de una persona
3. Identificar qué casos relevantes han existido como consecuencia del uso de deepfakes
4. Demostrar como la inteligencia artificial ha influido en el aumento de casos de deepfakes en el Perú

1.5. Hipótesis

Una hipótesis investigativa es una suposición o proposición que se formula como respuesta preliminar a una pregunta de investigación, la cual puede ser probada a través de la recolección y análisis de datos. La importancia de una hipótesis radica en que guía el diseño del estudio, estableciendo un enfoque claro para la investigación y permitiendo a los investigadores dirigir sus esfuerzos hacia la búsqueda de evidencia que confirme o refute la suposición planteada. Al formular hipótesis, los investigadores pueden

identificar variables clave, establecer relaciones entre ellas y estructurar su análisis de manera más efectiva. En resumen, una hipótesis es fundamental para orientar la investigación, aportar claridad al proceso y contribuir al desarrollo del conocimiento en un área específica.

Si se configura los deepfakes con el uso de la inteligencia artificial como una nueva modalidad delictiva se podrá sancionar eficientemente el delito de suplantación de identidad

1.6. Variables.

1.6.1. Variable independiente.

Los deepfakes como nueva modalidad delictiva

1.6.2. Variable dependiente.

Suplantación de identidad

1.7. Métodos, técnicas e instrumentos de recolección de datos.

1.7.1. Métodos.

Los métodos investigativos son enfoques sistemáticos y estructurados utilizados para recolectar, analizar e interpretar datos con el fin de responder preguntas específicas y resolver problemas en diversas disciplinas. Su importancia radica en que proporcionan un marco riguroso que garantiza la validez y fiabilidad de los resultados obtenidos, permitiendo así una comprensión más

profunda de los fenómenos estudiados. Estos métodos facilitan la toma de decisiones informadas, contribuyen al avance del conocimiento y promueven el desarrollo de habilidades críticas y analíticas. En resumen, los métodos investigativos son fundamentales para asegurar que las investigaciones se realicen de manera efectiva y que sus hallazgos sean relevantes y aplicables en contextos prácticos.

1.7.1.1. Métodos generales.

- El Método Inductivo consiste en validar una creencia o afirmación mediante la aplicación de la lógica deductiva, basándose en creencias o afirmaciones previamente aceptadas. Este enfoque se utiliza en varias áreas del conocimiento, como la ciencia y la filosofía, donde se requiere una argumentación rigurosa y consistente.
- El Método Deductivo se basa en justificar una creencia o proposición mediante la lógica deductiva, partiendo de otras creencias o proposiciones que ya se han aceptado. Este enfoque se emplea en múltiples disciplinas, como la ciencia y la filosofía, donde se requiere una argumentación rigurosa y coherente.
- El Método Histórico sostiene que todos los fenómenos sociales se desarrollan dentro de un contexto particular de tiempo y lugar, y que están condicionados por su pasado y presente, con efectos que se proyectan hacia el futuro.

- **Método Lógico:** El método lógico es un enfoque sistemático y ordenado para el análisis y la resolución de problemas que se basa en principios de razonamiento claro y coherente. Este método se centra en el uso de la lógica formal para derivar conclusiones a partir de premisas, asegurando que el proceso de pensamiento sea riguroso y estructurado. A menudo se utiliza en disciplinas como la matemática, la filosofía, la ciencia y la lógica misma, donde es fundamental establecer relaciones precisas entre conceptos y proposiciones.

1.7.1.2. Métodos específicos.

- **El Método Estadístico** se enfoca en el análisis numérico de los datos utilizando técnicas estadísticas. Este enfoque implica la recolección de datos mediante la selección de muestras representativas de una población, seguida de su análisis estadístico. Mediante cálculos y pruebas estadísticas, se pueden obtener resultados relevantes y aplicables a la población estudiada.
- **Métodos Dialectico:** El método dialéctico es fundamental en diversas disciplinas, incluyendo la filosofía, la sociología, la historia y la teoría política, ya que proporciona un marco para analizar problemas complejos y entender la dinámica de los cambios sociales y culturales. Su enfoque en las contradicciones y el desarrollo permite a los investigadores y pensadores abordar la realidad de manera más profunda y crítica, facilitando así un entendimiento más completo de los fenómenos en cuestión.

- **Método Hermenéutico:** El método hermenéutico es un enfoque interpretativo utilizado para comprender y analizar textos, discursos y fenómenos culturales. Originado en el estudio de la interpretación de textos sagrados y literarios, la hermenéutica ha evolucionado para abarcar diversas disciplinas, incluyendo la filosofía, la sociología, la psicología y la teoría del derecho. Este método se centra en la búsqueda de significados, contextos y relaciones que van más allá de la mera literalidad de las palabras.
- **Método exegético:** El método exegético es fundamental para la interpretación precisa de textos complejos, especialmente en el ámbito religioso y filosófico. Permite a los investigadores y estudiosos profundizar en el significado de las obras y comprender su impacto en el pensamiento y la cultura a lo largo del tiempo.

1.7.2. Técnicas.

Las técnicas investigativas son procedimientos utilizados para recolectar, analizar e interpretar datos con el fin de responder a preguntas específicas y resolver problemas dentro de un área de estudio. Estas técnicas pueden variar según la disciplina y el enfoque de la investigación, y pueden incluir métodos cuantitativos, cualitativos o mixtos.

Encuesta: Se realizará una encuesta dirigida a una muestra específica para obtener conocimiento y opiniones sobre el proceso deepfakes como nueva modalidad delictiva de suplantación de identidad con el

uso de inteligencia artificial. El objetivo es encontrar una solución para la problemática planteada en la investigación, y se utilizará la escala de Likert.

1.7.3. Instrumentos.

Los instrumentos investigativos son herramientas diseñadas para facilitar la recolección, medición y análisis de datos en un estudio. Estos instrumentos pueden adoptar diversas formas, como cuestionarios, encuestas, guías de entrevistas, escalas de evaluación, registros de observación y más. Su principal función es ayudar a los investigadores a obtener información relevante y precisa sobre el fenómeno que están estudiando.

Cuestionario: Se diseñará un cuestionario de 10 preguntas para ser aplicado virtualmente a la muestra seleccionada. El objetivo es conocer la opinión de los encuestados sobre el tema a investigar y validar la hipótesis y solución propuestas.

Con respecto a la población investigativa, se tuvo en consideración a expertos como jueces, fiscales y abogados que tengan conocimiento relacionados a los deepfakes como nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial. Cabe mencionar que se tuvo en consideración como muestra investigativa a 35 expertos de distrito judicial de Lambayeque.

CAPITULO II: MARCO CONCEPTUAL

PARTE I: ANTECEDENTES DEL PROBLEMA

Maldonado & Ovalles (2022) en su artículo titulado “Repercusiones éticas sobre el uso indebido del deepfake en el ámbito de las TIC mediante un análisis cualitativo documental” en el cual concluyó que: “Gracias al estudio de los casos documentados del uso del Deepfake por sus principales exponentes, se puede evidenciar y recolectar información pertinente para combatir el uso indebido de este, advirtiéndolo en la comunidad perteneciente a las TIC las principales repercusiones éticas que afectan a individuos inocentes y sus principales consecuencias sociales y legales que influyen en el bienestar social; gracias al análisis de las consecuencias del Deepfake, se brindan estrategias que pueden servir de guía para crear mejores software de detección y pautas éticas en la comunidad de las TIC”.

Bañuelos (2020) en su artículo titulado “Deepfake: la imagen en tiempos de la posverdad” en el cual concluyó que: “El escenario socio-mediático del deepfake es amplio, progresivo y cambiante, se construye sobre el territorio fértil de la posverdad, que propicia la propagación de contenidos falsos mezclando hechos y emociones con fines propagandísticos o maliciosos. El deepfake es un elemento más de la arquitectura mediática, política, moral, ética y cultural que alberga la creación y propagación de la falsedad como producción de realidad. La teoría crítica de la posverdad ve una posibilidad de generar discursos que cuestionen las verdades detentadas por poderes conservadores y dominantes. Sin embargo, la

valoración ética y legal de los discursos de la posverdad, entre ellos los deepfakes, se tendrán que valorar desde su lectura y daños en un contexto moral, ético, legal y cultural específico”.

Zea (2018) en su tesis titulada “Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala” en el cual concluyó que: “En Guatemala se encuentran tipificados los delitos relativos a la destrucción de registros informáticos que componen varias modalidades de crimen como el robo de identidad mediante dispositivos electrónicos y que, en su mayoría, derivan en la clonación de tarjetas de crédito o débito para obtener un beneficio económico. Esta tipificación es suficiente para que, en un proceso penal, se compruebe la comisión de dichos delitos. Sin embargo, el Estado estará ausente respecto de la violación a la intimidad, de la acción de apropiación indebida de fondos monetarios ajenos, pues no se especifica en ninguna parte del Código Penal, aun así se logran penas de prisión”.

Vidal (2018) en su artículo titulado “La falta de regulación frente a la suplantación y usurpación de identidad en Internet” concluyó que: “Tal y como se ha expuesto a lo largo del trabajo, los ciberdelitos o delitos cometidos en la red, son cada día más frecuentes en la actual realidad sociocultural, y ello supone un peligro frente a la ciberseguridad, ya que los delitos en la red evolucionan a un ritmo constante y mucho más rápido que la legislación en este ámbito. Más concretamente, la usurpación de identidad en internet en sus diversas modalidades y los delitos que se derivan de ésta suponen un peligro para el bien jurídico protegido de la fe

pública en la identidad de los ciudadanos, además de otros bienes jurídicos protegidos como el derecho al honor, a la intimidad personal y familiar o a la propia imagen, así como el patrimonio entre otros, por lo que su tipificación en el Código Penal es de vital importancia”.

Hernández (2019) en su tesis titulada “La suplantación de identidad cibernética en el Ecuador” concluyó que: “Mediante la investigación realizada se puede determinar que el objetivo uno se ha podido identificar de manera clara ya que el Ecuador es un país subdesarrollado, motivo por el cual su población no cuenta con la educación y cultura necesarias para acceder a los beneficios que brinda la internet, volviéndonos un grupo sumamente vulnerable para sufrir las consecuencias de los delitos informáticos. Los gobernantes de turno no se han preocupado de forma apta y adecuada para que la población de toda índole social se capacite de manera adecuada y de esta forma la alfabetizar a la población para de esta manera disminuir los riesgos que se encuentran dentro del ciberespacio”.

Rimaicuna (2021) en su tesis titulada “Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096” en cual concluyó que: “El uso de tecnología deepfake trae como consecuencias la generación de un detrimento en la imagen, el honor, contribuye a fomentar o ejercer violencia material o psicológica sobre una persona, coadyuva a la desinformación y crea manipulación respecto a un contenido informativo que la población está dispuesto a validar, atentando contra la identidad y seguridad de los cibernautas”.

Carrillo & Montenergo (2018), en su tesis titulada, “La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos” concluyó que “Con el uso de la tecnología han surgido diferentes modalidades delictivas, las cuales no están muy bien reguladas por el ordenamiento jurídico peruano, es por ello que el Estado en el año 2013 promulga la Ley 30096 – Ley de Delitos Informáticos, sin embargo esta no regula de manera precisa el delito de atentado a la integridad de sistemas informáticos, por lo que se debe modificar el artículo 4 de dicha ley, incorporando no solo a los medios tecnológicos de información y comunicación sino también a los medios tradicionales como medios comisivos de este delito; con el objetivo de salvaguardar los intereses de las personas, de sus sistemas informáticos”.

PARTE II: BASES TEÓRICAS DE LOS DELITOS INFORMATICOS

Delitos informáticos

La globalización ha traído consigo diversas mejoras en el acceso a los recursos tecnológicos que permiten optimizar el intercambio comercial y tecnológico; sin embargo, con estos avances también han aparecido nuevas conductas delictivas que se han convertido en un problema mundial creciente. El Perú no es ajeno a ello, pues estas conductas se presentan en la cotidianeidad, desde una transacción comercial multinacional hasta un pago a través de las ya conocidas billeteras digitales. En este contexto, numerosos países y organizaciones a nivel global están trabajando para

detener a los delincuentes cibernéticos y mejorar la seguridad de los sistemas y datos informáticos.

Según UNIR (2022), los delitos informáticos implican la realización de acciones que van en contra de las leyes penales, haciendo uso de medios electrónicos e internet, ya sea a través de redes públicas o privadas. Este tipo de acciones tienen como objetivo causar daño o destruir sistemas y equipos informáticos, así como también afectar la identidad, intimidad, propiedad y seguridad de individuos o entidades legales.

Bajo esta premisa, el Consejo de Europa junto a otros Estados presentaron el Convenio de Budapest que se firmó en el 2001 y entró en vigor internacionalmente en el 2004, convencidos de la urgencia de implementar una política penal común, con el fin de salvaguardar a la sociedad de la ciberdelincuencia, especialmente a través de la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional.

Tomando como base dicho convenio, en el 2013 se publicó en nuestro país la Ley N.º 30096 (Ley de Delitos Informáticos), que sufrió modificaciones, como la que se dio mediante la Ley N.º 30171, publicada el 2014, su objetivo principal es la prevención y sanción de conductas ilícitas que afectan a los sistemas y datos informáticos, así como a otros bienes jurídicos relevantes desde el punto de vista penal, cuando se cometen mediante el uso de tecnologías de la información y comunicación. Esto tiene como fin una lucha efectiva contra la ciberdelincuencia.

En ese sentido, dicha ley presenta un catálogo de delitos que tutelan los datos y sistemas informáticos, la indemnidad y libertad sexual, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública; en ese contexto, en la tipificación de dichas conductas se tomó como base las normas de carácter internacional; sin embargo, el legislador nacional consideró necesario tipificar el delito de suplantación de identidad, previsto en el art. 9 de la Ley N.º 30096. Bajo esta premisa brindaremos algunos alcances respecto a la estructura típica del mencionado delito, además de algunas respuestas a algunas interrogantes que se presentan al momento de desarrollar la estructura típica del mismo.

Suplantar la identidad

El *Diccionario de lengua española* define al verbo “suplantar” como “ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba”. En ese sentido, Puelles (2022) considera que se debe entender al verbo “suplantar” como el ocupar el lugar de alguien más. Al respecto, debemos precisar que el suplantar implica, dentro de su propia naturaleza, el que se haga respecto de una persona, quien ha sufrido una afectación a su derecho a la identidad, misma que ha sido disfrutada o viene siendo disfrutada por un tercero. Del mismo modo, Galán (2010) indica que la conducta punible recae sobre la obtención o apoderamiento de datos, informaciones o documentos de un sujeto tercero para utilizarlos con la finalidad de hacerse pasar por otro en los diversos ámbitos de la vida cotidiana.

En ese sentido, para efectos del presente delito, la acción de suplantar debe contar con la idoneidad suficiente para ocupar el lugar de otro a través de las TIC, es decir, no tratarse de suplantaciones burdas; en caso no se cuente con dicha idoneidad, la acción decaerá en atípica para el delito de suplantación de identidad. Para mejor comprensión, un ejemplo es crear una página web con similares características a la de una reconocida empresa multinacional y a la del *brochure* con la que esta cuenta en sus sitios oficiales, mediante la cual se ofrezca puestos de trabajo, suplantación que cumpliría con la idoneidad para transgredir la confianza del sujeto pasivo; situación diferente es cuando se suplanta la identidad de la misma empresa pero a través de una publicación en un grupo jurídico de Facebook, donde se ofrezca puestos de trabajo, pero estos tengan errores ortográficos, discordancia en el imago tipo, isotipo, entre otros, de la empresa a quien se pretenda suplantar su identidad.

Bien jurídico protegido

La aparición de la cibercriminalidad atenta contra varios bienes jurídicos, siendo que cada uno de los delitos que se encuentran dentro de este grupo presenta una afectación plural a bienes jurídicos. En ese sentido, consideramos que, al igual de los demás delitos tipificados en la Ley N.º 30096, el delito materia de análisis es uno que pertenece a la categoría de delitos pluriofensivos.

Pérez (2019) sostiene que esta figura delictiva vendría a proteger punitivamente el “principio de veracidad”; en ese sentido, el bien jurídico protegido por el delito de suplantación de identidad sería la fe pública, es

decir, el derecho a la verdad, precisando además que este supuesto del injusto de falsedad personal penaliza aquellas suplantaciones de identidad idóneas para afectar el bien jurídico tutelado, esto es, la fe pública, en cuanto a la veracidad que deben manifestar los participantes en el tráfico jurídico a través de las tecnologías de la información o de la comunicación. Detallado este punto, no se ahondará más en él, en vista de la extensa literatura y jurisprudencia que existe en la actualidad respecto al concepto de dicho bien jurídico. El objetivo del presente artículo es más bien brindar mayores detalles de las nuevas modalidades delictivas ante el poco conocimiento que se tiene sobre ellas.

En ese sentido, diferimos de lo expuesto por el referido autor respecto a que la fe pública es el único bien que se pretende proteger en el delito materia de análisis. Consideramos que, si la intención del legislador era el solo resguardar dicho bien jurídico, existían ya dentro del catálogo previsto en el Código Penal dispositivos legales que bien pudieran haber tutelado lo sancionado en el tipo penal materia de investigación, como lo es el delito de falsedad genérica, tipificado en el art. 438 del CP, que dentro de su naturaleza de delito residual y sus supuestos de aplicación sanciona el usurpar la identidad de una persona.

En ese sentido, coincidimos con Elías (2022), quien propone a la *interacción social en entornos digitales* como el bien jurídico protegido del delito de suplantación de identidad, postura a la que nos allanamos en razón de que las nuevas formas de interacción social que se vienen desarrollando a través de entornos digitales (WhatsApp, Facebook

Messenger, Instagram, Twitter, Telegram, entre otros) han sustituido a las formas de comunicación presencial con los que se contaba; comunicación en la red que permite crear espacios en los que engloban todos los aspectos de la vida diaria, esto es, trabajo, entretenimiento, educación, cultura, entre otros, por lo que merece ser cautelada. En ese sentido, creemos que la intención del legislador al castigar los atentados que se propicien necesariamente en entornos de comunicación digitales es, además de cautelar la fe pública, resguardar la interacción social en entornos digitales.

Sujeto activo

Las personas que cometen los delitos informáticos son aquellas que poseen características particulares relacionadas con el conocimiento del uso de la informática, que es el elemento diferenciador con los delincuentes convencionales, vale decir que son características que no presenta el denominador común de los delincuentes tradicionales.

Jiménez (2017) refiere que los sujetos activos en este tipo de delitos tienen habilidades para el manejo de los sistemas informáticos.

Así también, Pérez (2019) señala que puede ser cualquier persona; el citado dispositivo legal no hace referencia a una cualidad especial del autor del delito o que este tenga conocimientos específicos en informática. Bajo este supuesto, como bien se precisa, el sujeto activo puede ser cualquier persona que ha de tener conocimientos básicos en el manejo de las tecnologías de la información o comunicación.

Sujeto pasivo

El legislador introduce una novedad al especificar que la víctima puede ser tanto una persona física como una entidad jurídica. Según Gutiérrez (1991), la principal víctima de los delitos informáticos es la persona jurídica, debido a su participación en el tráfico económico y las actividades que realizan. Por esta razón, los sectores más afectados por la criminalidad informática incluyen la banca, las instituciones públicas y la industria manufacturera, entre otros.

Habiendo precisado que el sujeto pasivo puede ser cualquier persona, conviene resaltar que esta calidad no solo puede atribuírsele a la persona a quien se suplantó su identidad mediante los medios señalados en la norma, esto por cuanto puede considerarse como tal a cualquier persona que resultó afectada producto de la suplantación de identidad. Al respecto, el art. 94 del CPP señala que se considera agraviado a todo aquel que resulte directamente ofendido por el delito o perjudicado por sus consecuencias; así también, Elías (2022) precisa que el perjuicio debe ser ocasionado, entre otros, a su titular, pero el delito de suplantación de identidad no lo exige, por lo que el perjuicio podrá ser invocado por terceros; asimismo, en la Cas. N.º 596-2021 Junín, de 11 de marzo del 2022, se indica que “debe diferenciarse en clave procesal entre el ofendido por el delito y el perjudicado por el delito. El primero es el titular del bien jurídico lesionado o puesto en peligro; y el segundo es quien resulta afectado o dañado como consecuencia de la conducta delictiva del agente delictivo” (f. j. n.º 3).

Tipo subjetivo

El delito de suplantación de identidad es un delito estrictamente doloso, no cabe culpa en ninguna de sus manifestaciones, en vista de que el sujeto debe tener conocimiento y voluntad de la suplantación efectuada y el perjuicio a ocasionarse producto de la misma. Como bien lo señala Faraldo (2019), dicha conducta podría ser objeto de un error de hecho en los supuestos en que el sujeto activo utilice el nombre o filiación desconociendo que en realidad le pertenecen a otra persona, lo cual lo excluiría del dolo directo.

Consumación

La suplantación de identidad es un delito de resultado, en vista de que es necesario que el sujeto activo cause un perjuicio al sujeto pasivo. La mera acción de suplantación no es suficiente para sostener la consumación del referido delito. Así también, corresponde precisar que el delito de suplantación de identidad puede desenvolverse en el grado de tentativa, esto cuando no se haya logrado efectivizar el perjuicio en desmedro del sujeto pasivo del delito.

PARTE III: TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

El medio para la realización del acto de suplantación debe ser necesariamente las TIC. En caso la acción de suplantar no se realice por medio de estas ya no tan nuevas y cambiantes tecnologías, implicaría la atipicidad de los hechos respecto al delito materia de análisis, por lo que

estos deberían ser reconducidos al delito de falsedad genérica, tipo penal residual previsto en el art. 438 del CP.

Actualmente, se han propuesto diversas definiciones para las TIC. En este sentido, resulta adecuado el concepto ofrecido por la Universidad Latina de Costa Rica, que define las tecnologías de la información y la comunicación como los recursos y herramientas empleadas en el proceso, gestión y distribución de información mediante dispositivos tecnológicos como computadoras, teléfonos, televisores, entre otros. En ese contexto, para los fines del presente artículo, podemos llegar a concluir que las TIC son todos aquellos recursos (Internet, WhatsApp, correos electrónicos, equipos celulares, entre otros) que permiten manipular diversa información digital, siendo que su utilización para la comisión del presente delito implica que estas tengan la capacidad de sociabilización digital.

Perjuicio moral o material

El *Diccionario de lengua española* define al “perjuicio” como la acción de ocasionar daño o menoscabo material o moral. En ese sentido, podemos sostener que el delito materia de análisis requiere necesariamente que la conducta cause un daño material o moral; de no cumplirse tal condición, la conducta solo habría quedado en un grado de tentativa.

Así también, corresponde mencionar que el delito de suplantación de identidad no tutela el patrimonio o el honor del sujeto pasivo, pues el objeto de tutela penal en dicho ilícito es la interacción social en entornos digitales y la fe pública conforme ya se detalló anteriormente, y si bien la

comisión de este injusto penal podría generar un perjuicio, no es ese el objeto de protección de la norma penal. Sobre este punto, el legislador, al redactar el tipo penal, no ha previsto la confusión que pudiese generar al momento de estudiar la estructura del tipo penal; asimismo, los términos “moral” y “material” son generales y ambiguos, sobre los cuales resultaba suficiente, al igual que en otros delitos que atentan a la fe pública, prever la existencia solo de un perjuicio.

De otro lado, el art. 11 de la Ley N.º 30096, Ley de Delitos Informáticos, prescribe sus circunstancias agravantes. En ese sentido, el num. 3 precisa como agravante cuando el agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia; en ese sentido, podemos sostener que, al ya prever la presencia de un perjuicio en la realización de la conducta típica, el obtener un beneficio económico está implícitamente recogida en dicho tipo penal.

PARTE IV: MODALIDAD DELICTIVA DE LOS DEEPFAKES

Deepfakes

Los deepfakes son videos, imágenes o audios generados que imitan la apariencia y el sonido de una persona utilizando inteligencia artificial. Esta tecnología, también conocida como "medios sintéticos", es tan convincente que puede engañar tanto a las personas como a los algoritmos. Los deepfakes son generados por la IA en directo y sus formas más comunes de aplicación son en videos o como filtros de realidad aumentada. El término "deepfake" proviene de la combinación de las palabras "deep

learning" y "fake", para representar algo falso que es resultado de la tecnología de aprendizaje profundo. Aunque existen aplicaciones de consumo que utilizan la tecnología deepfake para el entretenimiento, su uso malicioso ha generado preocupaciones, ya que puede ser utilizado para difundir noticias falsas, suplantar identidades, realizar estafas, entre otros. Los deepfakes son extremadamente realistas y difíciles de distinguir, lo que plantea desafíos en términos de detección y prevención de su uso malicioso.

Los deepfakes, que son videos, fotos o grabaciones de audio manipulados con inteligencia artificial para que parezcan reales, han sido identificados como una herramienta cada vez más utilizada para facilitar diversos actos delictivos. Según un informe de LISA News, los actores de amenazas harán un uso creciente de la tecnología deepfake para cometer delitos como extorsión, fraude, manipulación de la opinión pública, apoyo a narrativas extremistas o de grupos terroristas, y pornografía infantil, entre otros. Europol también ha alertado sobre el potencial de los deepfakes para convertirse en una herramienta básica del crimen organizado. Aunque los deepfakes tienen aplicaciones legítimas, como el entretenimiento, su uso para cometer delitos es motivo de preocupación debido a su capacidad para influir en la opinión pública, desencadenar disturbios civiles y cometer fraudes. A pesar de que los deepfakes son en su mayoría legales, pueden considerarse ilegales si violan leyes existentes, como las relacionadas con la pornografía infantil, difamación o discurso de odio.

Un acto delictivo se refiere a cualquier acción que viole la ley y que esté sujeta a sanciones legales. En el contexto de los deepfakes, se ha

identificado que esta tecnología puede facilitar diversas actividades delictivas, como la extorsión, el fraude, la manipulación de la opinión pública, el apoyo a narrativas extremistas o de grupos terroristas, y la pornografía infantil, entre otros. Los deepfakes, al ser capaces de crear contenido falso altamente convincente, representan un desafío significativo en términos de detección y prevención de su uso malicioso. Aunque la mayoría de las aplicaciones de deepfakes son legales y tienen usos legítimos, su potencial para ser utilizados en actividades delictivas ha generado preocupaciones y ha llevado a un mayor escrutinio en términos de regulación y prevención.

Los deepfakes, al ser capaces de crear contenido falso altamente convincente, pueden ser utilizados para cometer diversos delitos, entre ellos:

1. Extorsión: Los deepfakes pueden ser utilizados para crear videos o audios falsos con el fin de extorsionar a personas, empresas o instituciones.
2. Fraude: La creación y difusión de deepfakes con el propósito de engañar a personas o influir en decisiones financieras puede constituir un delito de fraude.
3. Violación de la intimidad sexual: La utilización de deepfakes para crear contenido pornográfico falso sin el consentimiento de la persona afectada puede constituir un delito de violación de la intimidad sexual.

4. Difamación: La creación y difusión de deepfakes con el propósito de dañar la reputación de una persona puede constituir un delito de difamación.

5. Violación de derechos de autor: La utilización de imágenes o audios protegidos por derechos de autor para la creación de deepfakes sin la autorización correspondiente puede constituir un delito de violación de derechos de autor.

En respuesta a la creciente preocupación por el uso malicioso de los deepfakes, se han propuesto iniciativas legislativas en varios países para penalizar su creación y difusión sin consentimiento y con intención maliciosa. Estas iniciativas buscan establecer sanciones proporcionales a los delitos que puedan cometerse a través de los deepfakes, con el fin de prevenir su uso indebido y proteger los derechos de las personas afectadas.

Legislación e impacto del deepfake

El creciente impacto de los deepfakes en la vida cotidiana, ha llevado a una respuesta legislativa por parte de los Estados Unidos, pertinente para poder luchar contra las prácticas maliciosas de este medio. La legislación relativa a los deepfakes se ha incorporado en la Ley de Autorización de Defensa Nacional para el Año Fiscal 2020 en los Estados Unidos. Entre las medidas contempladas se incluye la obligación de informar sobre el uso de deepfakes como armas extranjeras, notificar al Congreso sobre actividades de desinformación mediante deepfakes en las elecciones de dicho país, y establecer un concurso de "Deepfakes Prize" para fomentar

la investigación o comercialización de tecnologías de detección de deepfakes.

Durante el año 2020, en los estados de Virginia y California se aprobó una legislación que sanciona la distribución de pornografía no consensuada generada mediante deepfakes. De igual forma, en Texas se penaliza la difusión de deepfakes que puedan dañar a un candidato durante el período electoral.

Es crucial reconocer la necesidad de una regulación más amplia a nivel internacional para abordar de manera integral el problema de los deepfakes. Dada la naturaleza transnacional de Internet y las tecnologías digitales, una respuesta eficaz requiere la colaboración entre múltiples países y jurisdicciones. La ausencia de una regulación coherente y global puede facilitar la propagación de los deepfakes a través de fronteras y evitar la acción legal en diferentes contextos. (Chipman et al., 2019)

Además, debemos reconocer el impacto significativo que los deepfakes han tenido en los últimos años, siendo objeto de crítica por parte de diversos medios de comunicación a nivel mundial. Un ejemplo notable es la iniciativa del diario The Wall Street Journal de implementar un programa de directrices para la detección de deepfakes. Así como otros medios de información, lucha contra la proliferación de videos falsos en las noticias, estableciendo pautas para sus periodistas, que incluyen la verificación de la fuente, la búsqueda de versiones anteriores de las imágenes, y el examen minucioso de las imágenes con técnicas como la visualización en cámara lenta y con zoom para identificar posibles

inconsistencias como saltos, borrosidades, cambios de iluminación, alteraciones del fondo, alteraciones climáticas, y voz artificial, entre otros. (Marconi & Daldrup, 2018)

Deepfake pornográfico

El surgimiento del deepfake pornográfico ha generado una creciente preocupación y debate en la sociedad de hoy en día. Esta tecnología, que utiliza algoritmos “Deep learning” para superponer rostros de personas reales en contenido pornográfico, plantea serios riesgos y desafíos éticos en términos de privacidad, consentimiento y manipulación de la imagen. Su capacidad para crear vídeos falsos de manera realista y convincente ha llevado a una serie de consecuencias preocupantes, incluida la difamación, el acoso y la vulneración de los derechos de las personas afectadas. Ante este panorama, es crucial explorar en profundidad el impacto y las implicaciones de esta práctica emergente.

Según Deeptrace, en el año 2019 se registró un aumento considerable en la cantidad de deepfakes encontrados en Internet, duplicándose con respecto a años anteriores. De un total de 14 678 deepfakes identificados, el 96% corresponden a contenido pornográfico, con un total de 134 millones de visualizaciones. Nueve sitios web están exclusivamente dedicados a la difusión de deepfakes pornográficos, mientras que ocho de cada diez sitios pornográficos alojan este tipo de contenido.

Los ataques utilizando deepfakes pornográficos se enfocan principalmente en mujeres, músicos y actores, siendo común que estos personajes sean de

nacionalidades británicas, surcoreanas, norteamericanas e israelíes. Estos deepfakes no solo afectan a celebridades conocidas como Scarlett Johansson, Gal Gadot, Taylor Swift, Maisie Williams y Jessica Alba, sino que también se utilizan contra personas privadas con fines de extorsión. La expansión de avatares y deepfakes pornográficos podría fomentar una industria personalizada de este tipo y aumentar los riesgos de acoso y chantaje en los próximos años.

La aplicación DeepNude ejemplifica el avance de las tecnologías del deepfake al permitir la "desnudez" de una mujer a partir de un retrato. Esta aplicación analiza una imagen y, utilizando una base de datos de 10 000 fotos de mujeres desnudas obtenidas de forma bastante sencilla y rápida en Internet, agrega un cuerpo desnudo al rostro de la imagen original. Cuando se confrontó al desarrollador de la aplicación mencionada, este argumentó que, incluso si él no la creaba, alguien más lo haría. Esta aplicación ha generado advertencias legales y preocupaciones éticas debido a sus implicaciones.

En efecto, se afirma que el uso generalizado de deepfakes pornográficos contribuye a la cosificación de la mujer. La totalidad de los sitios web dedicados a este tipo de contenido atacan y dañan la reputación de mujeres al utilizar sus imágenes para crear material pornográfico sin su consentimiento. Esta práctica reduce a las mujeres a meros objetos sexuales y perpetúa estereotipos de género, exacerbando la violencia y la discriminación contra ellas. La difusión de deepfakes pornográficos representa una violación de los derechos humanos y refuerza la necesidad

de una regulación más estricta para proteger la dignidad y la integridad de las personas, especialmente de las mujeres, en línea. (Ajder, 2019)

Circunstancias y contextos en el uso de los Deepfakes

La disponibilidad de herramientas de IA que facilitan la creación de deepfakes ha aumentado significativamente. Estas herramientas, que anteriormente requerían conocimientos técnicos avanzados, ahora son accesibles para el público en general. Esto ha permitido que individuos sin experiencia técnica puedan generar contenido manipulado, lo que ha contribuido al incremento de casos de deepfakes en el país.

Casos de Uso Indebido

Uno de los ejemplos más preocupantes en Perú es el caso de estudiantes en Chorrillos que utilizaron deepfakes para crear y distribuir contenido pornográfico no consensuado de sus compañeras. Este incidente resalta cómo la tecnología puede ser utilizada para humillar y acosar, especialmente a mujeres jóvenes, y cómo la falta de regulación adecuada permite que tales actos queden impunes.

Desconocimiento y Vulnerabilidad

Un factor crítico que ha contribuido al aumento de deepfakes en Perú es el alto nivel de desconocimiento sobre esta tecnología entre la población. Según estudios, alrededor del 75% de los peruanos no saben qué es un deepfake, lo que los hace más susceptibles a ser víctimas de fraudes y manipulaciones. Este desconocimiento se ve agravado por la falta de

educación sobre ciberseguridad y el uso responsable de las tecnologías digitales.

PARTE V: CASOS RELEVANTES DEL DEEPPFAKE

La legislación en Perú aún no ha avanzado al ritmo de la tecnología, lo que ha permitido que los deepfakes se utilicen con poca o ninguna consecuencia legal. Aunque hay iniciativas en otros países que buscan regular el uso de la IA y los deepfakes, en Perú, los proyectos de ley relacionados no abordan específicamente los riesgos asociados con esta tecnología, dejando un vacío que los delincuentes pueden explotar.

Implicaciones Sociales

La proliferación de deepfakes en Perú también tiene implicaciones sociales más amplias, como la normalización de la violencia de género y el acoso en línea. La facilidad con la que se pueden crear y compartir estos contenidos puede contribuir a un entorno en el que se minimizan las agresiones digitales, afectando la dignidad y la seguridad de las personas, especialmente de las mujeres.

Casos Relevantes de Deepfakes

Tom Cruise en TikTok: Un usuario creó una serie de vídeos deepfake que mostraban a Tom Cruise realizando trucos de magia y otras actividades cotidianas. Estos vídeos se volvieron virales y generaron un amplio debate sobre la autenticidad de los contenidos en redes sociales y

la facilidad con la que se pueden crear representaciones engañosas de figuras públicas.

Mark Zuckerberg: En un vídeo deepfake, se mostró a Zuckerberg hablando sobre el control de datos y la manipulación de la información. Este caso se utilizó como una crítica a la forma en que las plataformas digitales manejan la privacidad y la información personal, resaltando el potencial de los deepfakes para distorsionar la realidad y difundir desinformación.

Emma Watson: La actriz fue víctima de un caso de deepfake que la involucró en la creación de contenido pornográfico no consensuado. Este caso subrayó los peligros de la tecnología, especialmente en lo que respecta a la privacidad y el consentimiento, y cómo puede ser utilizada para dañar la reputación de las personas.

Deepfakes en Campañas Políticas: Se han reportado casos donde los deepfakes se utilizan para crear vídeos falsos de líderes políticos haciendo declaraciones comprometedoras. Esto no solo afecta la percepción pública de los individuos involucrados, sino que también puede influir en procesos electorales y generar desconfianza en la información política

Implicaciones de Estos Casos

Estos ejemplos destacan cómo los deepfakes pueden ser utilizados para:

Manipulación de la Opinión Pública: Al crear contenido que parece auténtico, los deepfakes pueden influir en la percepción de eventos y

figuras públicas, lo que puede tener repercusiones en la política y la sociedad.

Violaciones a la Privacidad: La creación de deepfakes no consensuados, especialmente en el contexto de contenido sexual, plantea serias preocupaciones sobre el consentimiento y el derecho a la privacidad.

Desconfianza en los Medios: La proliferación de deepfakes puede llevar a un escepticismo generalizado hacia los medios de comunicación, dificultando la identificación de información veraz.

PARTE VI: APLICABILIDAD DE LA INTELIGENCIA ARTIFICIAL

Inteligencia Artificial

Al ser un tema de amplio bagaje hoy en día, es pertinente delimitar su definición a fin de evitar ambigüedades, para beneficio de esta investigación. La Real Academia Española (2024) la define como la “Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico”. Con esto, nos quiere decir que la inteligencia artificial (en adelante IA), se centra en el desarrollo de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Del mismo modo, según la Comisión Europea (2020), las IA son sistemas de software y hardware diseñados por humanos, que se desempeñan en el ámbito físico o digital para frente a objetivos complejos. Asimismo, tienen la capacidad de percibir su entorno mediante la

adquisición e interpretación de datos estructurados o no estructurados, así como de razonar sobre el conocimiento derivado de estos datos y tomar decisiones óptimas para lograr el objetivo establecido. Además, pueden emplear reglas simbólicas o aprender a partir de modelos numéricos, y también tienen la capacidad de adaptar su comportamiento al analizar cómo el entorno se ve afectado por sus acciones previas.

Pimentel (2020), considera que la característica fundamental que ostenta la inteligencia artificial, radica en su motor de funcionamiento, el renombrado “algoritmo“. En palabras del autor, " Un algoritmo de aprendizaje automático es un proceso de prueba y error, pero lo interesante de este es que cada prueba consecutiva es al menos tan buena como la anterior". Ello implica que, con cada ciclo de prueba y error, el algoritmo mejora progresivamente hasta alcanzar un nivel óptimo para su implementación y uso práctico. Asimismo también es importante destacar que llegar a este nivel de perfección requiere que la máquina y sus algoritmos pasen por numerosas pruebas y errores, lo que resulta en una reducción gradual de la frecuencia de errores en cada repetición.

A continuación, es importante resaltar lo que Arend Hintze señala sobre las IAs, pues afirma que existen tipos de IAs, los cuales merecen ser señalados para poder comprender mejor lo que abarcan este tipo de tecnología. Menciona cuatro tipos: Las máquinas reactivas, las de memoria limitada, aquellas que poseen una “Teoría de la mente”, y las de autoconciencia. En cuanto a la primera, se dice que son las más básicas, son incapaces de recordar o aprender de experiencias pasadas. Por otro

lado, el segundo tipo (sistemas de memoria limitada) sí son capaces de retener información de experiencias pasadas, como los vehículos autónomos, aunque su memoria sea temporal y no pueda aplicarse a situaciones futuras. El tercer tipo son las llamadas máquinas con una “Teoría de la mente”, con una amplia capacidad para formar representaciones sobre el mundo y otros agentes con los que mantienen interacción. Se caracterizan por poseer un nivel de comprensión más avanzado, fundamental para una interacción efectiva entre los sistemas de IA y su entorno, lo cual les permite comprender que las personas tienen pensamientos y emociones que influyen en su comportamiento. Por último, se presentan a las llamadas autoconciencias, las cuales van más allá de la “Teoría de la mente”, son una especie de extensión de esta, permitiendo ahora a los sistemas crear representaciones de sí mismos; sin embargo, alcanzarlas aún es un desafío que requiere más avances en el campo de la IA. (Hintze, 2016)

Por otro lado, Russel & Norvig (2022), distinguen una manera distinta de clasificar a las IA, estableciendo también cuatro tipos de sistemas. En primer lugar, tenemos a aquellos que piensan como humanos, los cuales se centran en replicar tanto el comportamiento como el proceso de pensamiento humano. Luego, están los sistemas que actúan como humanos, enfocados en replicar cómo se comportan y actúan los humanos en situaciones diversas. En tercer lugar, están aquellos sistemas que piensan racionalmente, enfocados en resolver problemas de manera lógica y eficiente, sin necesariamente imitar el comportamiento humano. Por

último, están los que actúan racionalmente, centrados en tomar decisiones óptimas basadas en la información disponible y en maximizar la efectividad de sus acciones en el mundo real.

Machine Learning

El Machine Learning es definido como una modalidad de inteligencia artificial que capacita a un sistema para aprender a partir de los datos mediante una programación explícita. Este proceso implica proporcionar datos al algoritmo para su entrenamiento, lo que resulta en la creación de modelos precisos que están relacionados con los datos utilizados en el proceso de aprendizaje. (IBM, 2020)

Por otro lado, la postura de Amazon (2018) indica que el Machine Learning o Aprendizaje Automático se define como un conjunto de algoritmos capaces de aprender de datos recopilados y hacer predicciones basadas en ellos, así como optimizar una función de utilidad específica, descubrir patrones ocultos en los datos y organizarlos en resúmenes concisos. En esencia, el Machine Learning implica la habilidad de una computadora para aprender, tomar decisiones y hacer predicciones utilizando una gran cantidad de datos, conocidos como Big Data. Aunque esta capacidad otorga a las máquinas ciertas habilidades humanas notables, todavía no alcanzan el mismo nivel de inteligencia. Además, es importante destacar que la efectividad del Machine Learning depende en gran medida de la calidad y cantidad de los datos con los que se alimenta. Asimismo, el objetivo del Machine Learning es desarrollar un algoritmo que una máquina pueda utilizar para llevar a cabo tareas específicas, como

encontrar un modelo de aprendizaje que se ajuste de manera óptima a los datos proporcionados. A diferencia de la programación tradicional, donde el programador brinda instrucciones explícitas a la máquina, en el Machine Learning, el enfoque radica en permitir que la máquina aprenda por sí misma a partir de los datos, sin que se le indique directamente cómo encontrar el modelo óptimo para trabajar con ellos. (Pimentel, 2020)

Deep Learning

Por otro lado, el deep learning se considera una subcategoría del aprendizaje automático, ya que su objetivo es crear modelos complejos a partir de conceptos simples. El concepto implica el uso de redes neuronales con múltiples capas para aprender de los datos de manera iterativa, especialmente eficaz para identificar patrones en datos no estructurados y abordar problemas abstractos. Se aplica en diversas áreas, como reconocimiento de voz, imágenes y visión por computadora, donde su capacidad para manejar abstracciones y problemas ambiguos es especialmente relevante (Casas et al., 2019).

PARTE VII: DEFINICIÓN DE TÉRMINOS.

Delitos

El delito es un acto u omisión que infringe una norma penal establecida por el ordenamiento jurídico de un país, y que es considerado como una conducta reprochable y perjudicial para la sociedad. Los delitos pueden clasificarse en diversas categorías, como delitos contra la persona, la propiedad, la libertad y el estado, y varían en gravedad, desde faltas

menores hasta crímenes graves. La tipificación de un comportamiento como delito conlleva consecuencias legales, que pueden incluir sanciones penales como multas, prisión o medidas de rehabilitación. En esencia, el delito no solo afecta a la víctima directa, sino que también compromete la seguridad y el bienestar colectivo, justificando la intervención del Estado para mantener el orden social y proteger los derechos de los ciudadanos.

Deepfakes

Los deepfakes son manipulaciones de apariencia facial a través de métodos generativos profundos. Estas tecnologías pueden reemplazar rostros, manipular expresiones faciales, sintetizar rostros y sintetizar voz para crear videos, fotos o grabaciones de audio que parecen reales pero han sido alterados con inteligencia artificial. Aunque los deepfakes tienen aplicaciones benignas y legítimas en áreas como el entretenimiento y el comercio, también se utilizan comúnmente con fines de explotación, como la creación de contenido pornográfico falso. Existe preocupación sobre el potencial crecimiento del uso de deepfakes para desinformación, influencia en elecciones, incitación a disturbios civiles y guerra psicológica. Aunque los deepfakes son generalmente legales, pueden ser ilegales si violan leyes existentes, como las relacionadas con la pornografía infantil, difamación o discurso de odio. Por ejemplo, un deepfake que muestre a una persona diciendo palabras que en realidad no dijo podría considerarse ilegal. Las plataformas de redes sociales, como Facebook, han tomado medidas para abordar el problema de los deepfakes, incluida la prohibición de videos que puedan engañar a los espectadores.

Suplantación de identidad

La suplantación de identidad, también conocida como robo de identidad, consiste en el uso no autorizado y malintencionado de los datos personales de un individuo por parte de otra persona, con el fin de actuar en su nombre. Esta práctica puede ocurrir en diversos contextos, como en el ámbito digital, donde se utilizan datos personales para cometer fraudes, o en el mundo real, donde se usurpa la identidad de alguien para realizar actividades ilegales. La suplantación de identidad es un delito que puede causar perjuicios significativos a la víctima, tanto en términos financieros como en su reputación y bienestar emocional. Es importante tomar medidas para prevenir y detectar este tipo de delitos, así como para denunciarlo en caso de ser víctima de suplantación de identidad.

Inteligencia artificial

La inteligencia artificial (IA) se refiere a la habilidad de las máquinas para emular la inteligencia humana y llevar a cabo tareas que normalmente necesitarían intervención humana. Este campo incluye una amplia gama de aplicaciones, que van desde el reconocimiento de voz y la visión por computadora hasta el aprendizaje automático y el procesamiento del lenguaje natural. La IA ha tenido un impacto significativo en diversos sectores, incluyendo la salud, las finanzas, el transporte y la educación, y se espera que continúe siendo una fuerza impulsora en la innovación tecnológica. A medida que las capacidades de la IA evolucionan, también lo hacen las consideraciones éticas y regulatorias en torno a su uso.

Modalidad delictiva

Las modalidades delictivas se refieren a las diferentes formas en que se cometen los delitos. Estas modalidades pueden variar según el tipo de delito y las circunstancias específicas de su comisión. Por ejemplo, en el ámbito de la seguridad ciudadana, se pueden identificar modalidades delictivas como el hurto a celulares, la estafa, el robo a mano armada, entre otros. El estudio de las modalidades delictivas es importante para comprender mejor la naturaleza de los delitos y desarrollar estrategias efectivas de prevención y combate a la delincuencia.

CAPITULO III: ANÁLISIS DE RESULTADOS

3.1. Resultados en tablas y figuras

Las tablas y figuras son herramientas esenciales en la presentación de datos en investigaciones cuantitativas. Su uso adecuado no solo mejora la claridad de los resultados, sino que también facilita la comprensión del contenido por parte del lector.

Además, as tablas y figuras son elementos cruciales en las investigaciones cuantitativas que mejoran la presentación de datos. Su uso efectivo requiere atención al detalle en su diseño y organización, asegurando que sirvan como herramientas claras y útiles para la comunicación científica.

Técnica utilizada: Encuesta

Población: Jueces, fiscales y abogados de Lima y Lambayeque

Cantidad de personas encuestadas: 35

Tabla 1.

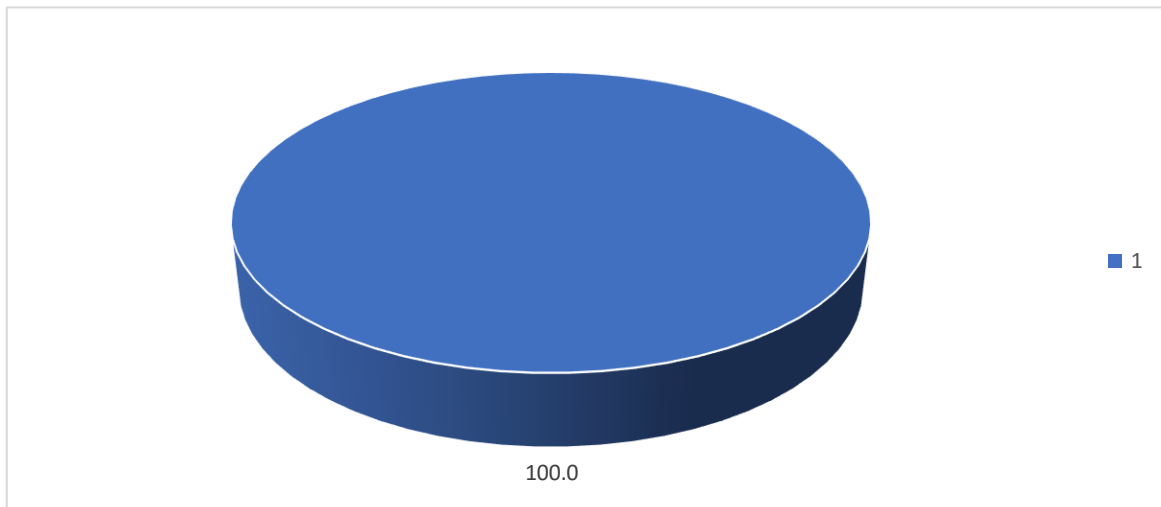
Modalidad delictiva de suplantar identidad.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 1.

Modalidad delictiva de suplantar identidad.



Nota. Resultados del cuestionario aplicada a través de la encuesta a jueces, fiscales y abogados

Con respecto a los datos que se han podido recopilar a través de la encuesta aplicada, se puede asegurar que el 100% de los expertos están a favor de considerar los deepfakes como una nueva modalidad delictiva de suplantación de identidad. Queda confirmado que los deepfakes son una herramienta tecnológica utilizada por personas inescrupulosas para obtener beneficios propios de forma ilícita, afectando a diferentes ciudadanos debido a las insuficiencias políticas por parte del estado para combatir esta problemática.

Tabla 2

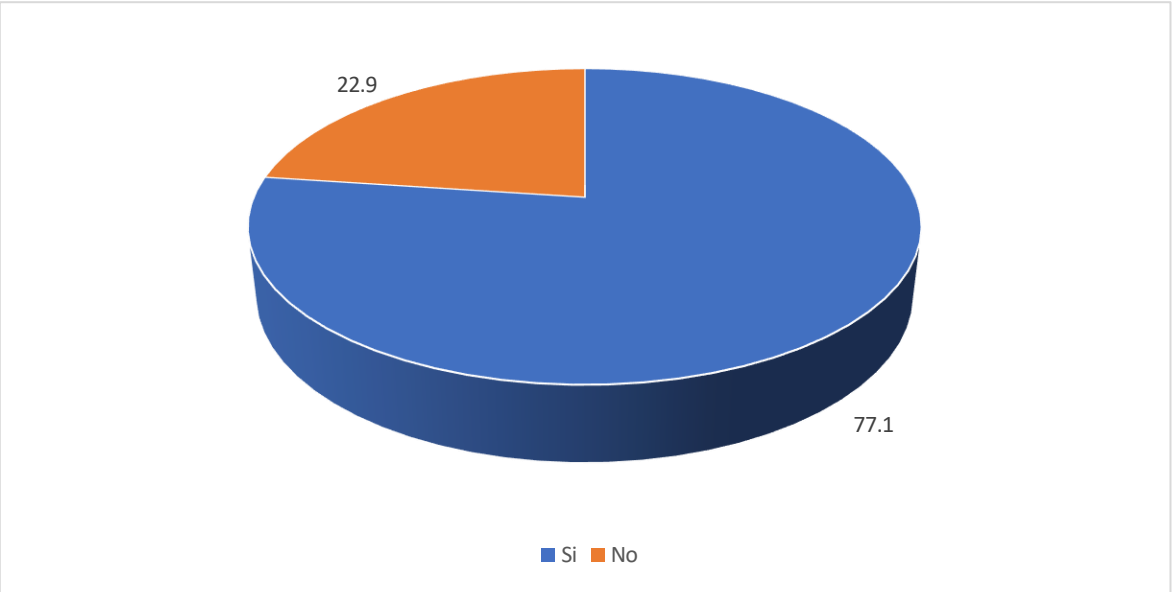
Inteligencia artificial y deepfakes.

Descripción	Frecuencia	Porcentaje
Si	27	77.1
No	8	22.9
Total	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 2.

Inteligencia artificial y deepfakes.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

En relación a los datos obtenidos por la segunda interrogante, se puede asegurar que el 77.1% de los expertos, manifiestan estar si estar a favor en que la sociedad peruana no cuenta con mecanismos para afrontar la inteligencia artificial y deepfakes, sin embargo, existe un 22.9% de los conocedores del derecho, que aseguran no estar a favor de la pregunta establecida. Los datos obtenidos permiten aseguran que la sociedad peruana carece totalmente de mecanismos para afrontar el mal uso de la inteligencia artificial y deepfakes.

Tabla 3

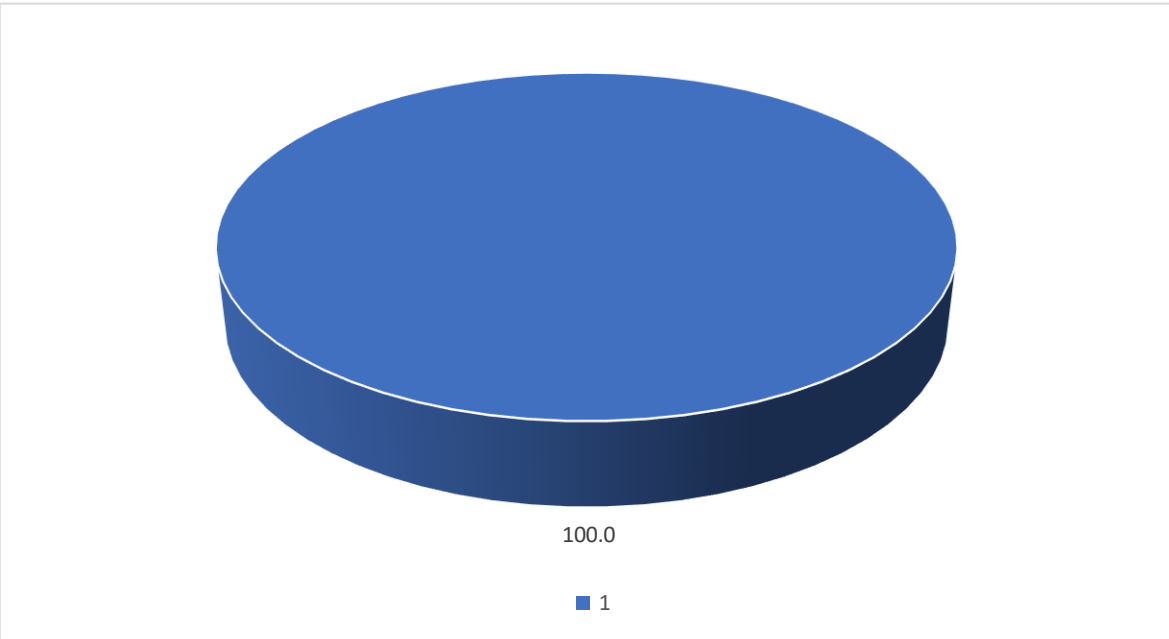
Suplantar identidad.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 3.

Suplantar identidad.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

Teniendo en consideración lo manifestado por los distintos participantes, se puede asegurar que el 100% de los encuestados aseguran si estar a favor en que se deba describir cómo los deepfakes viene siendo utilizados para suplantar identidad. Conforme a estos datos que han sido posible obtener, se puede corroborar que todos los expertos aseguran que en la sociedad peruana es necesario que se describa el mal uso de los deepfakes.

Tabla 4

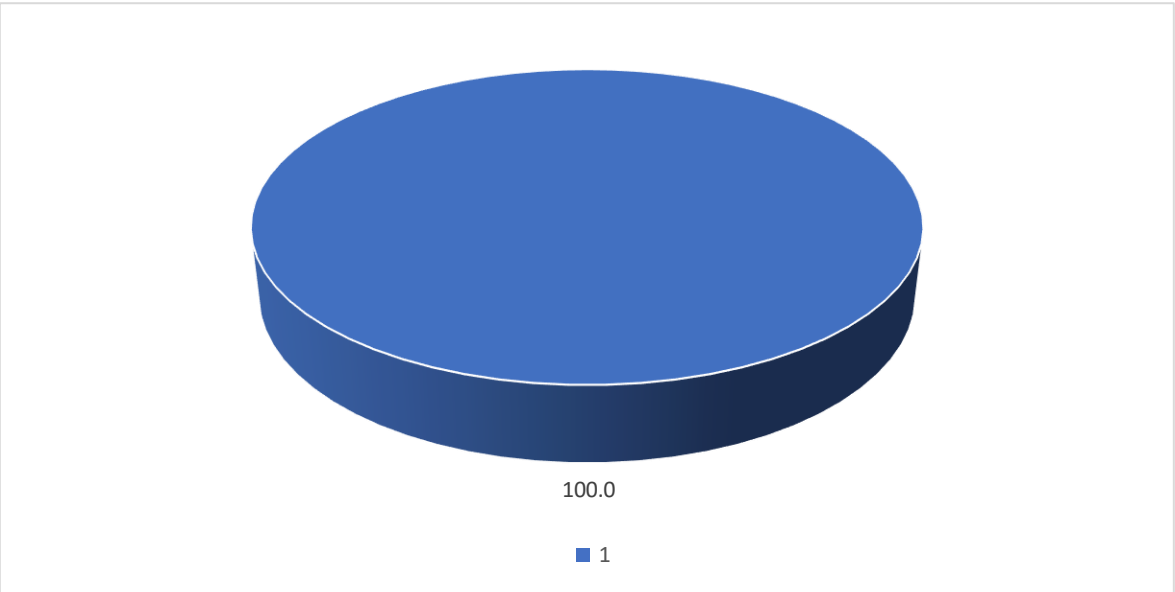
Deepfakes a nivel nacional e internacional.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 4.

Deepfakes a nivel nacional e internacional.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

En relación a la cuarta interrogante, se puede asegurar que el 100% de los expertos que han formado parte de la encuesta aplicada, aseguran si estar a favor en que es necesario que analice el uso de los deepfakes a nivel nacional e internacional, para que de esta manera se pueda identificar las formas como se viene utilizando dicha herramienta tecnológica y de esta manera obtener una perspectiva efectiva para combatirla de manera adecuada y eficiente.

Tabla 5

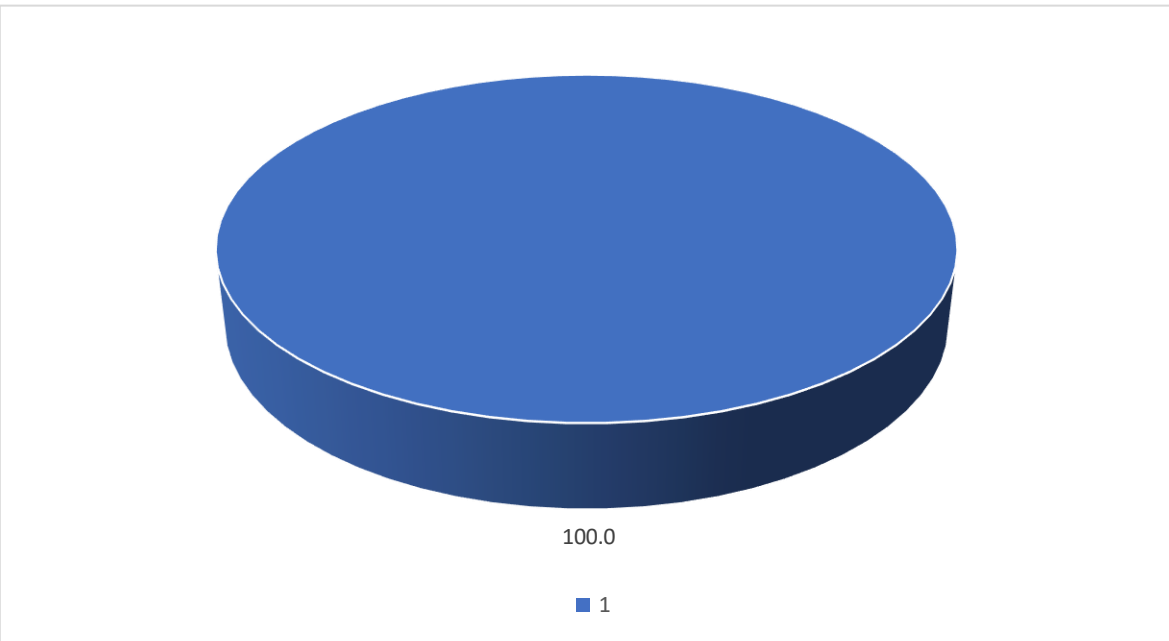
Suplantación de identidad de una persona.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 5.

Suplantación de identidad de una persona.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

Con respecto a la quinta pregunta, se puede confirmar que el 100% de los encuestados están a favor de describir en qué circunstancias se genera la suplantación de identidad de una persona. De esta manera, se podría identificar en qué se está fallando al afrontar o combatir esta situación, la cual está aumentando exponencialmente debido a la falta de mecanismos o estrategias para enfrentar este problema.

Tabla 6

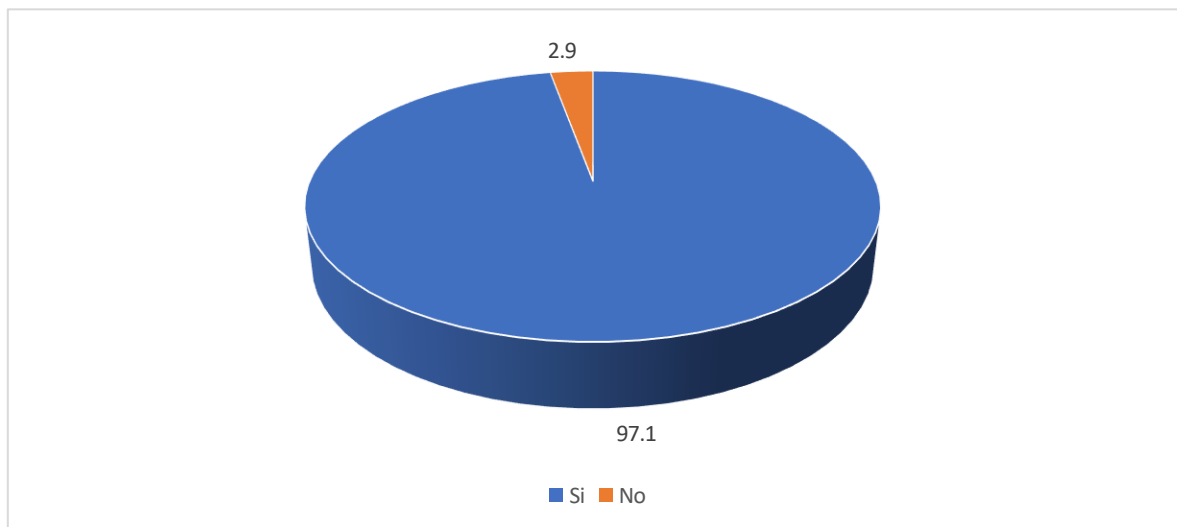
Consecuencia del uso de deepfakes.

Descripción	Frecuencia	Porcentaje
Si	34	97.1
No	1	2.9
Total	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 6.

Consecuencia del uso de deepfakes.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

Teniendo en consideración a la sexta interrogante, se puede asegurar que el 97.1% de los expertos aseguran si estar a favor en que se deba identificar qué casos relevantes han existido como consecuencia del uso de deepfakes, sin embargo, existe un 2.9% de los encuestados que aseguran no estar conforme con la pregunta establecida, pues consideran que no es necesario y solo se debe combatir eficientemente.

Tabla 7

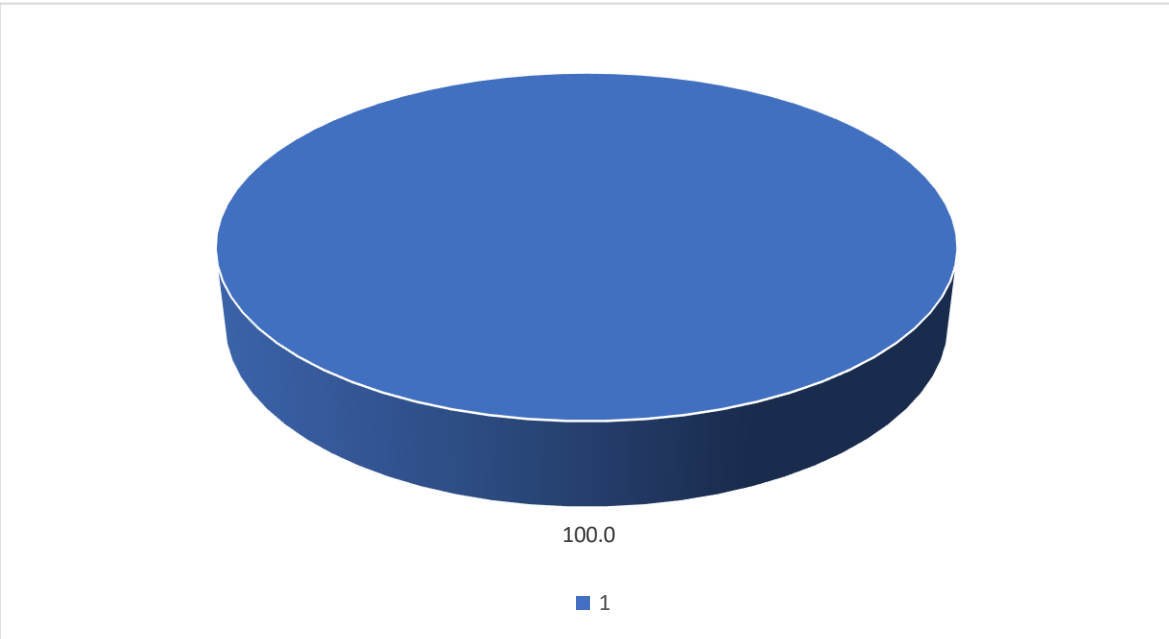
Inteligencia artificial.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 7.

Inteligencia artificial.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

En relación a la séptima interrogante, se puede asegurar que el 100% de los encuestados, manifiestan si estar a favor en que, se deba describir como la inteligencia artificial ha influido en el aumento de casos de deepfakes en el Perú. Con respecto a este resultado, se puede asegurar la inteligencia artificial al ser una herramienta que ofrece información de todo tipo y de forma inmediata, ha ocasionado que se incremente el uso delictivo de los deepfakes en el Perú

Tabla 8

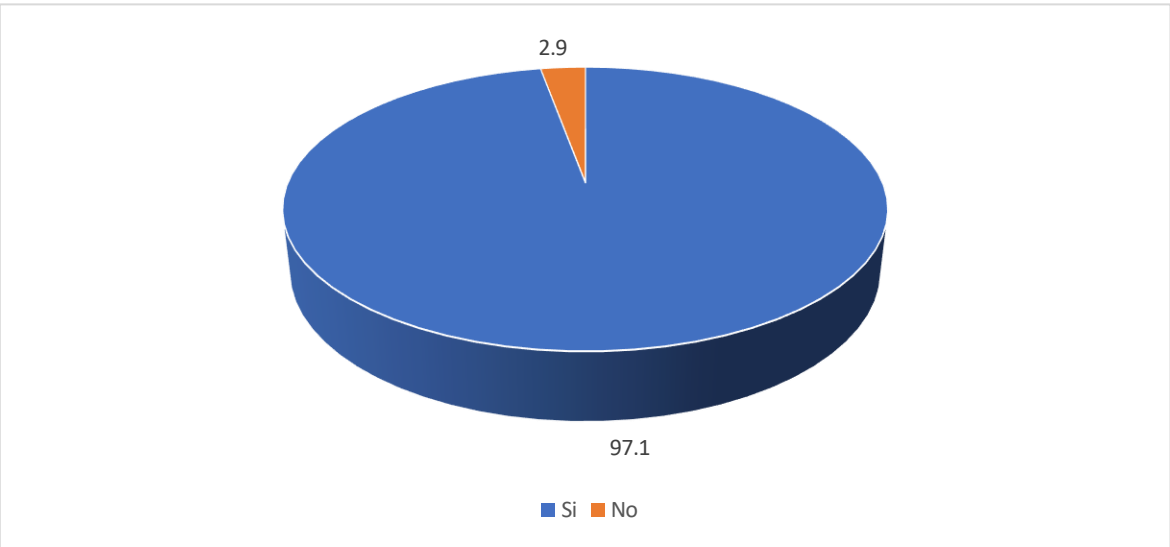
Instituciones especializadas.

Descripción	Frecuencia	Porcentaje
Si	34	97.1
No	1	2.9
Total	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 8.

Instituciones especializadas.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

En relación a la octava interrogante, se puede asegurar que el 97.1% de los expertos, manifiestan si estar a favor en que es necesario que se incorporen instituciones especializadas para poder afrontar eficientemente el deepfake y la inteligencia artificial mal utilizada, sin embargo, existe un 2.9% de los participantes, que manifiestan no estar a favor de la interrogante establecida. Es importante mencionar que, al incorporar nuevas instituciones especializadas en el tema, se podrá contribuir eficientemente en la reducción de estos actos delictivos

Tabla 9

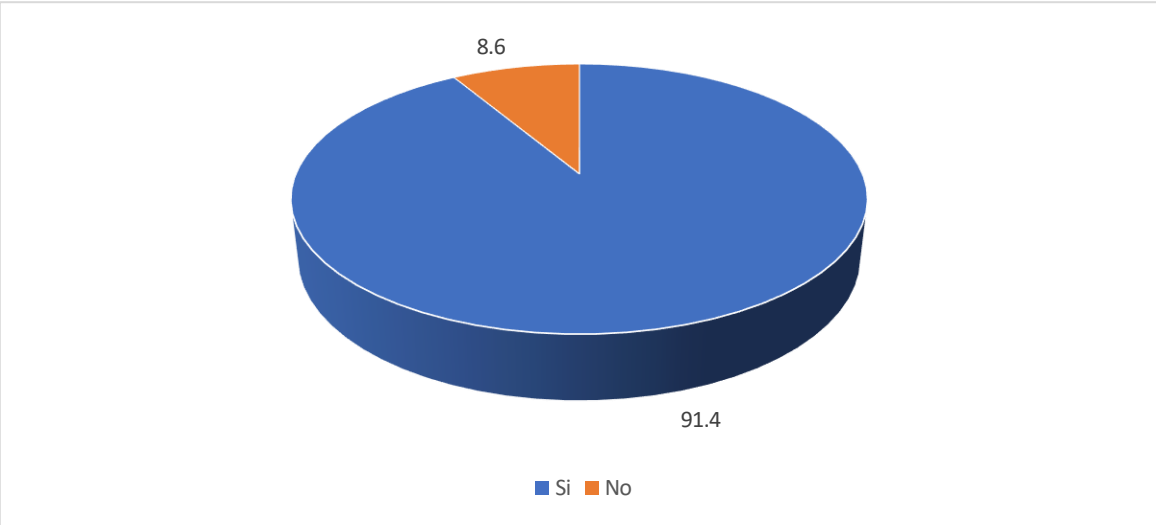
Ineficiencia de los mecanismos actuales.

Descripción	Frecuencia	Porcentaje
Si	32	91.4
No	3	8.6
Total	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 9.

Ineficiencia de los mecanismos actuales.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

Con respecto a lo manifestado por el 91.4% de los conocedores del derecho, se puede asegurar que, si están a favor en que los mecanismos actuales que presenta el estado peruano, son ineficientes ante la inteligencia artificial y deepfake, sin embargo, el 8.6% restante de participantes, manifiestan no estar conforme con la pregunta establecida, pues mencionar que si existen mecanismos para afrontar estas nuevas actividades ilícitas que han sido originadas por la inteligencia artificial.

Tabla 10

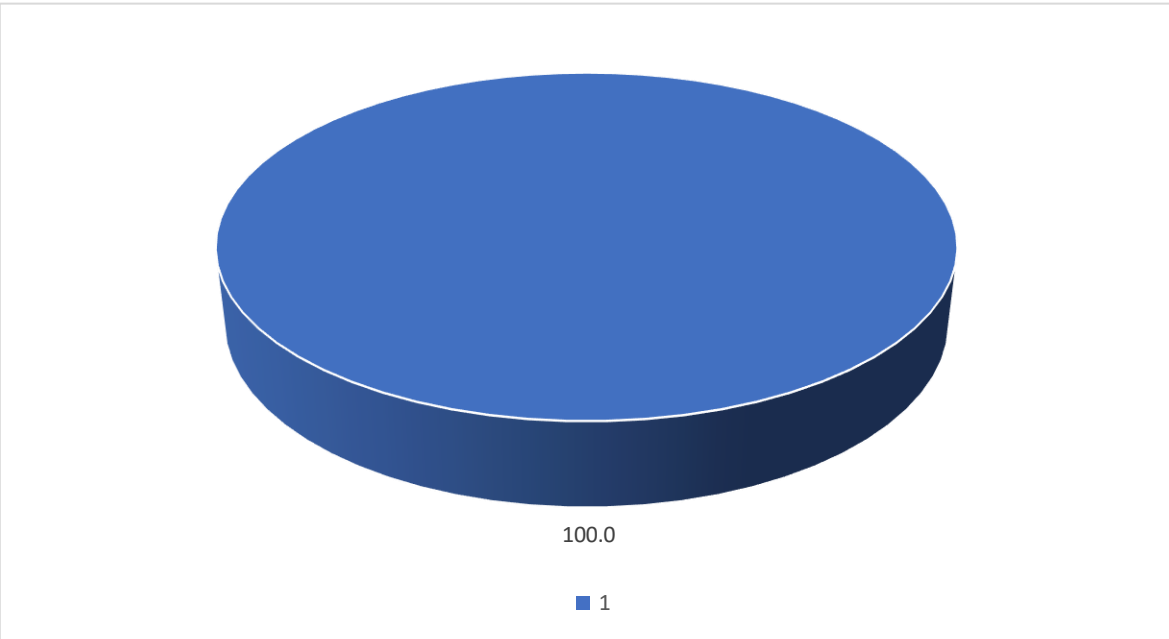
Sanción penal.

Descripción	Frecuencia	Porcentaje
Si	35	100.0

Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados.

Figura 10.

Sanción penal.



Nota. Resultados del cuestionario aplicad a través de la encuesta a jueces, fiscales y abogados

Para culminación del apartado de interpretación de los resultados, se puede asegurar que el 100% de las personas que formaron parte de la encuesta aplicada, aseguran si estar a favor en que se deba establecer una sanción penal eficiente para afrontar la problemática de deepfake y la inteligencia artificial mal utilizada. Conforme a estos resultados, se puede asegurar que el Estado peruano requiere de nuevas estrategias e instituciones para afrontar eficientemente esta situación que en la actualidad por el fácil acceso a la tecnológica se ha convertido en una problemática muy constante.

CAPITULO IV: CONTRASTACIÓN DE LA HIPÓTESIS

4.1. Discusión de los resultados

En este apartado investigativo, se detallaron de manera precisa los resultados que más se asemejan a los objetivos investigativo, los cuales fueron contrastados con diferentes estudios investigativo que permitieron confirmar la viabilidad del estudio, es por ello que se tuvo en cuenta al objetivo general, el cual buscó describir de qué manera el uso de los deepfakes pueden ser utilizados como una nueva modalidad delictiva de suplantación de identidad con el uso de inteligencia artificial, para este objetivo se tuvo en cuenta a lo obtenido en la Tabla N°3 donde se puede asegurar que el 100% de los encuestados aseguran si estar a favor en que se deba describir cómo los deepfakes viene siendo utilizados para suplantar identidad. Conforme a estos datos que han sido posible obtener, se puede corroborar que todos los expertos aseguran que en la sociedad peruana es necesario que se describa el mal uso de los deepfakes. Es importante reconocer que, en la actualidad, la sociedad peruana enfrenta diversas dificultades para abordar la problemática de los delitos cometidos por los ciudadanos. Sin embargo, esta situación empeora día a día, ya que el Estado no cuenta con herramientas ni mecanismos eficaces para enfrentar el uso indebido e ilícito de la inteligencia artificial, como es el caso de los deepfakes. Así mismo, este resultado puede ser contrastado con lo sustentado por Vidal (2018) que ha llegado a detallar a lo largo del trabajo, los ciberdelitos, o delitos cometidos en la red, se están volviendo cada vez más comunes en la realidad sociocultural actual. Esto representa una amenaza significativa para la ciberseguridad, dado que estos delitos

evolucionan a un ritmo mucho más rápido que la legislación en este ámbito. En particular, la usurpación de identidad en internet y los delitos asociados a ella constituyen una amenaza para la protección de la fe pública en la identidad de los ciudadanos. Además, afectan otros bienes jurídicos protegidos, como el derecho al honor, a la intimidad personal y familiar, y a la propia imagen, así como al patrimonio, lo que subraya la importancia de su inclusión en el Código Penal. Es importante señalar que, frente a la problemática de los deepfakes a nivel nacional, la sociedad peruana no dispone de mecanismos adecuados para enfrentar esta situación. Esto resulta en una afectación directa a la población, especialmente a las personas más desprotegidas ante este problema, y pone en cuestión la eficiencia del Estado peruano como protector de los ciudadanos para abordar este fenómeno en constante emergencia.

Con respecto al primer objetivo específico, Analizar el uso de los deepfakes a nivel nacional e internacional, se tuvo como respaldo a lo obtenido en la Tabla N°4 donde se puede asegurar que el 100% de los expertos que han formado parte de la encuesta aplicada, aseguran si estar a favor en que es necesario que analice el uso de los deepfakes a nivel nacional e internacional, para que de esta manera se pueda identificar las formas como se viene utilizando dicha herramienta tecnológica y de esta manera obtener una perspectiva efectiva para combatirla de manera adecuada y eficiente. La problemática del inadecuado uso del deepfakes tanto a nivel nacional como internacional, es situación que viene aumentando constantemente en diferentes Estados, sin embargo, es

importante reconocer que diferentes Estados reconocidos como países desarrollados, enfrenta esta situación con sanciones penales más eficientes y del mismo modo con herramientas tecnológicas para poder identificar el mal uso de los avances tecnológicos. Con respecto a este resultado, se puede asegurar que se asemeja con lo sustentado por Carrillo y Montenergo (2018) quienes concluyeron que el avance de la tecnología ha dado lugar a nuevas modalidades delictivas que no están adecuadamente reguladas por la legislación peruana. Por ello, en 2013, el Estado promulgó la Ley 30096 – Ley de Delitos Informáticos. Sin embargo, esta ley no regula de manera precisa el delito relacionado con la integridad de los sistemas informáticos. Es necesario modificar el artículo 4 de la ley para incluir no solo los medios tecnológicos de información y comunicación, sino también los métodos tradicionales utilizados para cometer este tipo de delitos, con el fin de proteger mejor los intereses y sistemas informáticos de las personas. En relación con los resultados obtenidos y los estudios realizados por los autores citados anteriormente, se puede afirmar que los avances tecnológicos continuarán evolucionando constantemente con el objetivo de beneficiar a la sociedad. Sin embargo, esta evolución no cuenta con herramientas adecuadas para detener o contrarrestar el uso ilícito de la tecnología, como ocurre con la inteligencia artificial y los deepfakes, que actualmente se utilizan para obtener beneficios personales de forma ilícita. En relación al segundo objetivo específico, Describir en qué circunstancias se genera la suplantación de identidad de una persona, ante este objetivo se tuvo como respaldo a lo obtenido en la Tabla N°5 el cual permitió confirmar que el 100% de los encuestados están a favor de describir en qué

circunstancias se genera la suplantación de identidad de una persona. De esta manera, se podría identificar en qué se está fallando al afrontar o combatir esta situación, la cual está aumentando exponencialmente debido a la falta de mecanismos o estrategias para enfrentar este problema. Es necesario reconocer que, para afrontar de manera eficiente una problemática que se viene suscitando en una sociedad, es necesario primero identificar el problema principal, para que de esta forma incorporar o formular estrategias efectivas que permitan subsanar problemas que se vienen dando en la sociedad como es el caso de la inteligencia artificial y los deepfakes, el cual se ha convertido en un problema que los ciudadanos tienen miedo ser afectado, pues esta herramienta tecnológica puede atacar a cualquier persona sin excepción alguna. Así mismo este puede ser contrastado con lo sustentado por Rimaicuna (2021) determinó que el uso de la tecnología deepfake resulta en varios efectos negativos, como la deterioración de la imagen y el honor de las personas, la promoción o la práctica de violencia tanto material como psicológica, la facilitación de la desinformación y la manipulación de información que el público tiende a aceptar. Todo esto pone en riesgo la identidad y la seguridad de los usuarios en línea. Tomando como referencia el resultado previamente detallado y lo sustentado por el autor, se puede asegurar que la suplantación de identidad mediante deepfakes ocurre cuando la tecnología de inteligencia artificial es utilizada para crear imágenes o videos falsos que imitan de manera convincente la apariencia y el comportamiento de una persona. Estas circunstancias suelen involucrar la utilización de datos audiovisuales recolectados de redes

sociales, videos públicos o imágenes personales sin el consentimiento del individuo.

Con respecto al tercer objetivo específico, Identificar qué casos relevantes han existido como consecuencia del uso de deepfakes, se tuvo como base estadística de respaldo a lo obtenido en la Tabla N° 6 donde se puede asegurar que el 97.1% de los expertos aseguran si estar a favor en que se deba identificar qué casos relevantes han existido como consecuencia del uso de deepfakes, sin embargo, existe un 2.9% de los encuestados que aseguran no estar conforme con la pregunta establecida, pues consideran que no es necesario y solo se debe combatir eficientemente. Es importante precisar que en la actualidad los deepfakes viene siendo generados con el único objetivo de poder engañar a otros, ya sea para difundir desinformación, cometer fraudes, o dañar la reputación de una persona. La facilidad para manipular estos contenidos y la dificultad para detectar la falsedad contribuyen a que esta forma de suplantación de identidad sea especialmente peligrosa, afectando gravemente la privacidad y seguridad de las personas. Desde una perspectiva similar, se tiene a lo sustentado por Hernández (2019) concluyó que, a través de la investigación realizada, se ha podido identificar claramente que, dado que Ecuador es un país en desarrollo, su población carece de la educación y cultura necesarias para aprovechar plenamente los beneficios de internet. Esto hace que el país sea extremadamente vulnerable a las consecuencias de los delitos informáticos. Además, los líderes actuales no han tomado medidas adecuadas para asegurar que la población de todos los sectores sociales reciba la capacitación necesaria, lo cual es crucial para alfabetizar

digitalmente a la gente y reducir los riesgos asociados con el ciberespacio. Conforme a los avances tecnológicos que se han venido originando con el transcurrir de los años, se han venido demostrando diferentes casos donde personas reconocidas internacionalmente como artistas del cine, han sido perjudicado por el uso ilícito de su imagen, pues han sido involucrado en actos publicitarios ilícitos, lo que ha conllevado a ser investigado como fue la situación de Tom Cruise, Volodímir Zelenski, entre otros famosos.

Para finalizar, se tuvo en cuenta al cuarto objetivo específico, el cual buscó describir como la inteligencia artificial ha influido en el aumento de casos de deepfakes en el Perú, para este propósito se tuvo como respaldo a lo obtenido en la Tabla N°7 en el cual se puede confirmar que el 100% de los encuestados, manifiestan si estar a favor en que, se deba describir como la inteligencia artificial ha influido en el aumento de casos de deepfakes en el Perú. Con respecto a este resultado, se puede afirmar que la inteligencia artificial, al ser una herramienta que proporciona información de todo tipo de manera inmediata, ha llevado a un incremento en el uso delictivo de los deepfakes en Perú. En relación con este último hallazgo, se puede concluir que la inteligencia artificial, al ofrecer información de forma rápida y accesible, se ha convertido en la principal herramienta utilizada por personas inescrupulosas para cometer actos ilícitos, ya sea a través de deepfakes u otras formas de delitos tecnológicos. Por último, este resultado es contrastado con lo sustentado por Bañuelos (2020) concluyó que el entorno socio-mediático del deepfake es extenso, en constante evolución y adaptable, y se desarrolla en el contexto de la posverdad, la cual facilita la difusión de información falsa al combinar hechos y emociones con fines

propagandísticos o maliciosos. El deepfake es un componente dentro de la estructura mediática, política, moral, ética y cultural que fomenta la creación y distribución de falsedades como si fueran realidades. La teoría crítica de la posverdad ofrece la oportunidad de generar discursos que cuestionen las verdades establecidas por poderes conservadores y dominantes. Sin embargo, la evaluación ética y legal de estos discursos, incluidos los deepfakes, debe realizarse teniendo en cuenta su impacto y daños en un contexto moral, ético, legal y cultural particular. Para culminar este apartado investigativo, es necesario reconocer que la influencia de la inteligencia artificial en el aumento de casos de deepfakes en el Perú es notable y significativa. La capacidad de esta tecnología para generar contenido visual y auditivo altamente convincente y realista ha facilitado la proliferación de deepfakes, exacerbando los problemas relacionados con la desinformación y la suplantación de identidad. En un país donde la infraestructura tecnológica y la educación digital aún están en desarrollo, el fácil acceso a herramientas de inteligencia artificial ha permitido que personas malintencionadas utilicen estas tecnologías para engañar y perjudicar a otros. Esto subraya la necesidad urgente de fortalecer las medidas de ciberseguridad, así como de implementar políticas y estrategias educativas que capaciten a la población en la identificación y manejo de estos riesgos emergentes.

II. CONCLUSIONES

CONCLUSIÓN GENERAL

En conclusión, los deepfakes representan una evolución preocupante en la suplantación de identidad, utilizando la inteligencia artificial para crear engaños casi indetectables que pueden ser utilizados para fines delictivos.

CONCLUSIONES ESPECÍFICAS

1. El uso de deepfakes plantea un dilema complejo que abarca desde la innovación tecnológica hasta la ética y la seguridad. Si bien esta tecnología tiene aplicaciones potencialmente positivas, como en el arte o la medicina, su uso malintencionado puede tener consecuencias devastadoras a nivel personal y social.
2. La suplantación de identidad surge cuando los datos personales caen en manos equivocadas y se utilizan con fines delictivos, causando graves perjuicios a las víctimas.
3. El uso de deepfakes ha dado lugar a varios casos relevantes que han captado la atención pública y han generado preocupaciones sobre la manipulación de la identidad y la desinformación.
4. La influencia de la inteligencia artificial en el aumento de casos de deepfakes en Perú se debe a la accesibilidad de la tecnología, el desconocimiento generalizado, la falta de regulación y las implicaciones sociales que surgen de su uso indebido. Estos factores combinados crean un entorno propicio para la proliferación de deepfakes y sus consecuencias negativas.

III. RECOMENDACIONES

1. La sociedad y las instituciones deben adaptarse rápidamente para mitigar estos riesgos y proteger la integridad de la identidad personal en el entorno digital.
2. La respuesta a estos desafíos requiere un enfoque colaborativo que incluya legislación, desarrollo de tecnologías de detección y educación pública para mitigar los riesgos asociados con los deepfakes.
3. Es crucial tomar medidas para proteger nuestra información y denunciar cualquier incidente sospechoso.
4. La necesidad urgente de desarrollar tecnologías de detección efectivas y de establecer marcos legales que aborden los desafíos éticos y legales que plantea el uso de deepfakes.
5. La combinación de educación, regulación, tecnología y apoyo a las víctimas es esencial para abordar este fenómeno de manera efectiva.

REFERENCIAS

- Ajder, H. (2019). The State of Deepfakes: Landscape, Threats, and Impact. Amsterdam: Deeptrace. Medium: <https://medium.com/sensity/mapping-the-deepfake-landscape-27cb809e98bc>
- Amazon. (2018). Lenovo Brazil improves supply and demand balance with DataRobot,. AWS: <https://aws.amazon.com/es/partners/success/lenovo-datarobot/>
- Bañuelos, J. (2020). Deepfake: la imagen en tiempos de la posverdad. <https://revistas.up.edu.mx/rpc/article/download/2315/1890/6321>
- Carrillo, C.F., Montenergo, A.N. (2018). La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. <https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4514/Carrillo%20Diaz%20%26%20Montenegro%20Davila.pdf?sequence=1&isAllowed=y>
- Casas, J., Bosch, A., & Lozano , T. (2019). Deep learning: principios y fundamentos. Editorial UOC.
- Chipman, J., Ferraro, M., & Preston, S. (2019). First Federal Legislation on Deepfakes Signed Into Law. JdSupra: <https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/>
- Elías, R. (2022). Suplantación de identidad en el Perú: análisis del artículo 9 de la Ley de Delitos Informáticos. Derecho Global.

- Faraldo, P. (2019). Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. *Revista de Derecho Penal y Criminología*.
- Galán, A. (2010). El robo de identidad: aproximación a una nueva y difusa conducta delictiva. En I. Alamillo. (Ed.), *Robo de identidad y protección de datos* (pp. 169-198). Aranzadi.
- Gutiérrez, M. (1991). *Fraude informático y estafa*. Ministerio de Justicia.
- Hernández, D.A. (2019). La suplantación de identidad cibernética en el ecuador. <https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content>
- Hintze, A. (2016). Understanding the four types of AI, from reactive robots to self-aware beings. *The Conversation*: <https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>
- IBM. (2020). ¿Qué es Machine Learning? IBM: https://www.ibm.com/ar-es/analytics/machine-learning?p1=Search&p4=43700052827921639&p5=b&cm_mmc=Search_Google_-_1S_1S_-_LA_ISA_-_%2Bmachine
- Jiménez, J. (2017). *Manual de derecho penal informático*. Jurista Editores.
- Maldonado, M. & Ovalles, F. (2022). Repercusiones éticas sobre el uso indebido del deepfake en el ámbito de las TIC mediante un análisis cualitativo documental. <https://revistas.sena.edu.co/index.php/RETO/article/download/3040/5520/27586>

- Marconi, F., & Daldrup, T. (2018). How The Wall Street Journal is preparing its journalists to detect deepfakes. NiemanLab: <https://www.niemanlab.org/2018/11/how-the-wall-street-journal-is-preparing-its-journalists-to-detect-deepfakes/>
- Pérez, J. (2019). Delitos regulados en leyes penales especiales. Gaceta Jurídica.
- Pimentel, G. (2020). La inteligencia artificial y su influencia en la eficiencia del comercio internacional 2020. Universidad San Ignacio de Loyola: <https://repositorio.usil.edu.pe/server/api/core/bitstreams/e190d249-c1ca-4006-bf5f-cf1b0d0a12cd/content>
- Rimaicuna, M. (2021). Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/82458/Rimaicuna_TMF-SD.pdf?sequence=1&isAllowed=y
- Rimaicuna, M. F. (2021). Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/82458/Rimaicuna_TMF-SD.pdf?sequence=1&isAllowed=y
- Russel, S., & Norvig, P. (2022). Artificial Intelligence: A Modern Approach (4 ed.). Pearson. <https://aima.cs.berkeley.edu>
- UNIR. (2022). Tipos de delitos informáticos y legislación aplicable. UNIR: <https://www.unir.net/derecho/revista/tipos-delitos-informaticos/>
- Vidal, E. (2018). La falta de regulación frente a la suplantación y usurpación de identidad en Internet.

https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal_Torres_Elionor.pdf?sequence=1&isAllowed=y