



**UNIVERSIDAD CÉSAR VALLEJO**

**FACULTAD DE DERECHO Y HUMANIDADES**

**ESCUELA PROFESIONAL DE DERECHO**

**Incorporación de las consecuencias nocivas del deepfake como  
agravantes del delito de suplantación de identidad en la Ley N°  
30096**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

**AUTORA:**

Rimaicuna Torres, Mareli Fiorella (ORCID: 0000-0001-6316-3534)

**ASESORA:**

Mg. Saavedra Silva, Luz Aurora (ORCID: 0000-0002-1137-5479)

**LÍNEA DE INVESTIGACIÓN:**

Derecho Penal

CHICLAYO – PERÚ

2021

## DEDICATORIA

A Dios, por guiar mi camino y permitirme cumplir una meta más de las muchas propuestas, sé que de su mano no hubiera logrado mis propósitos académicos.

A mi familia, por forjarme en la persona que soy hoy en día en base a los valores que me inculcaron desde pequeña y encaminarme a actuar con probidad dentro del ámbito personal y profesional; su apoyo constante ha sido pieza fundamental para la materialización de cada uno de mis logros durante mi trayecto académico.

A mi abuelo Agustín Torres Vásquez, mi ángel en el cielo, por enseñarme a nunca rendirme a pesar de las adversidades, por demostrarme que con paciencia y amor todo puede cambiar. Sé que celebras mis logros como los tuyos y aunque ya no estés presente físicamente, siempre me acompañas espiritualmente. Hoy te puedo decir: Lo logramos.

A mi tía María Vilma Agip Nuñez, quien hoy disfruta del descanso eterno, por sus palabras de aliento y superación, por su fuerza, voluntad e inmenso cariño demostrado a todos los que quiso.

A mi tío Carlos Antonio Agip Nuñez, quien dejó este espacio terrenal para estar al lado del Señor, por sus cálidos recibimientos que reconfortaban el alma y sus sinceros deseos de verme realizada como profesional.

A todos aquellos que confiaron en mí, que me impulsaron a ser mejor persona y profesional y me brindaron la oportunidad de expandirme académicamente.

A quienes me brindaron una palabra de aliento, un abrazo fraterno y una amistad sincera.

## **AGRADECIMIENTO**

Agradezco al docente Jorge Luis Fernández Terán, Dr. Walter Eduardo Chambergó Chavesta, Luis Dandy Esquivel León y Luz Aurora Saavedra Silva, por enseñarme que la cátedra universitaria no se limita a las aulas de clase, que se puede ser docente y trascender en sus alumnos a través de su vocación para servir. Gracias por las experiencias vividas en aulas de clases, por hacer tan grata mi estadía dentro de mi trayecto universitario, por sus consejos y sus palabras de aliento y motivación para quienes tuvimos la dicha de ser sus alumnos.

Agradezco al Dr. Félix Chero Medina, Dr. René Zelada Flores y Dr. Tito Esteves Torres, por fomentar en mi persona el interés y la pasión por el campo del Derecho Penal y Procesal Penal, por brindarme las herramientas necesarias para forjarme en una buena profesional y por darme la oportunidad de compartir espacios académicos en diversos concursos de litigación oral. Mi respeto, aprecio y admiración hacia ustedes siempre.

## Índice de contenido

<b>DEDICATORIA</b> .....	ii
<b>AGRADECIMIENTO</b> .....	iii
<b>Índice de contenido</b> .....	iv
<b>Índice de tablas</b> .....	vi
<b>Índice de figuras</b> .....	viii
<b>Índice de abreviaturas</b> .....	x
<b>Resumen</b> .....	xi
<b>Abstract</b> .....	xii
<b>I. INTRODUCCIÓN</b> .....	1
<b>II. MARCO TEÓRICO</b> .....	3
<b>III. METODOLOGÍA</b> .....	21
<b>3.1. Tipo y diseño de investigación</b> .....	21
<b>3.2. Variables y operacionalización</b> .....	21
<b>3.3. Población, muestra y muestreo</b> .....	23
<b>3.4. Técnicas e instrumentos de recolección de datos</b> .....	23
<b>3.5. Procedimientos</b> .....	24
<b>3.6. Método de análisis de datos</b> .....	24
<b>3.7. Aspectos éticos</b> .....	24
<b>IV. RESULTADOS</b> .....	26

<b>V. DISCUSIÓN</b> .....	41
<b>VI. CONCLUSIONES</b> .....	45
<b>VII.RECOMENDACIONES</b> .....	46
<b>VIII.PROPUESTA</b> .....	47
<b>REFERENCIAS</b> .....	50
<b>ANEXOS</b> .....	57

## Índice de tablas

<b>Tabla N° 01.</b> Condición de encuestados: Abogados.....	26
<b>Tabla N° 02.</b> ¿Cree usted, que la suscripción del convenio de Budapest, ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información?.....	26
<b>Tabla N° 03.</b> ¿Considera usted, que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos? .....	27
<b>Tabla N° 04.</b> ¿Considera usted, que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen? .....	28
<b>Tabla N° 05.</b> ¿Considera usted, que colocar a una persona en situaciones bochornosas afecta su honor? .....	29
<b>Tabla N° 06.</b> El uso de tecnología deepfake, permite que mediante fotos y audios de una persona, se pueda manipular su rostro y voz. En relación a lo anterior, ¿cree usted, que a través de esta tecnología se puede fomentar o ejercer violencia material o psicológica sobre una persona? .....	30
<b>Tabla N° 07.</b> ¿Considera usted, que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación?.....	31
<b>Tabla N° 08.</b> En su opinión, ¿un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación?.....	32
<b>Tabla N° 09.</b> En países como EE.UU y China, se han empezado a adoptar ciertas medidas legislativas para regular el uso de tecnología deepfake. ¿Considera usted, que nuestro país debe empezar a legislar al respecto? .....	33

<b>Tabla N° 10.</b> En EE.UU., existió una proliferación de videos deepfake en contiendas políticas, así como de los llamados pornovenganzas, colocando a las personas situaciones bochornosas, haciendo y diciendo algo que no sucedió. En ese sentido, ¿considera usted que los videos deepfakes suplantan la identidad de una persona?.....	34
<b>Tabla N° 11.</b> En China, se ha legislado la prohibición de videos deepfake que son utilizados para crear, publicar y difundir noticias falsas. En su opinión,¿ este tipo de videos deberían prohibirse en nuestro país por generar desinformación?.....	35
<b>Tabla N° 12.</b> ¿Considera usted, que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones? .....	36
<b>Tabla N° 13.</b> En su opinión, ¿los operadores de justicia se encuentran debidamente capacitados en materia informática?.....	37
<b>Tabla N° 14.</b> ¿Considera usted, que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes para la detección de videos deepfake? .....	38
<b>Tabla N° 15.</b> El uso de tecnología deepfake, genera como consecuencias nocivas, la afectación al derecho al honor, a la imagen, fomenta o ejerce violencia física o material sobre una persona, crea manipulación y coadyuva a la desinformación. En ese sentido ¿considera usted que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad?.....	39

## Índice de figuras

<b>Figura N° 01.</b> Condición de encuestados: Abogados.....	26
<b>Figura N° 02.</b> ¿Cree usted, que la suscripción del convenio de Budapest, ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información?.....	27
<b>Figura N° 03.</b> ¿Considera usted, que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos? .....	28
<b>Figura N° 04.</b> ¿Considera usted, que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen? .....	29
<b>Figura N° 05.</b> ¿Considera usted, que colocar a una persona en situaciones bochornosas afecta su honor? .....	30
<b>Figura N° 06.</b> El uso de tecnología deepfake, permite que mediante fotos y audios de una persona, se pueda manipular su rostro y voz. En relación a lo anterior, ¿cree usted, que a través de esta tecnología se puede fomentar o ejercer violencia material o psicológica sobre una persona? .....	31
<b>Figura N° 07.</b> ¿Considera usted, que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación?.....	32
<b>Figura N° 08.</b> En su opinión, ¿un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación?.	33
<b>Figura N° 09.</b> En países como EE.UU y China, se han empezado a adoptar ciertas medidas legislativas para regular el uso de tecnología deepfake. ¿Considera usted, que nuestro país debe empezar a legislar al respecto?.....	34



**Figura N° 10.** En EE.UU., existió una proliferación de videos deepfake en contiendas políticas, así como de los llamados pornovenganzas, colocando a las personas situaciones bochornosas, haciendo y diciendo algo que no sucedió. En ese sentido, ¿considera usted que los videos deepfakes suplantan la identidad de una persona? ..... 35

**Figura N° 11.** En China, se ha legislado la prohibición de videos deepfake que son utilizados para crear, publicar y difundir noticias falsas. En su opinión, ¿ este tipo de videos deberían prohibirse en nuestro país por generar desinformación? ..... 36

**Figura N° 12.** ¿Considera usted, que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones? ..... 37

**Figura N° 13.** En su opinión, ¿ los operadores de justicia se encuentran debidamente capacitados en materia informática? ..... 38

**Figura N° 14.** ¿Considera usted, que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes para la detección de videos deepfake? ..... 39

**Figura N° 15.** El uso de tecnología deepfake, genera como consecuencias nocivas, la afectación al derecho al honor, a la imagen, fomenta o ejerce violencia física o material sobre una persona, crea manipulación y coadyuva a la desinformación. En ese sentido ¿considera usted que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad?

## Índice de abreviaturas

R.S.....	Resolución legislativa
Art.....	Artículo
EE.UU.....	Estados Unidos
CAS.....	Casación

## **Resumen**

La presente investigación tuvo como objetivo analizar las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096, el diseño de esta investigación fue no experimental y de tipo básica; cuya muestra fue no probabilístico selectivo por conveniencia, constituida por 50 abogados especialistas en Derecho Penal pertenecientes al Colegio de Abogados de Lambayeque.

Asimismo, se aplicó como técnica la encuesta y como instrumento el cuestionario, mismos que coadyuvaron a arribar como resultados que tabla y figura N° 09, se observó que el 98.2% de abogados consideró que en nuestro país se debe empezar a legislar en torno al uso de tecnología deepfake, por otro lado, el 1.8% de ellos consideró que no es necesario legislar al respecto.

Concluyendo 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.

**Palabras clave:** Deepfake, suplantación de identidad y Ley N°30096.

## **Abstract**

The present research aimed to analyze the harmful consequences of deepfake as aggravating factors of the crime of identity theft in Law No. 30096, the design of this research was non-experimental and of a basic type; whose sample was non-probabilistic selective for convenience, constituted by 50 lawyers specialized in Criminal Law belonging to the Bar Association of Lambayeque.

Likewise, the survey was applied as a technique and as an instrument the questionnaire, which helped to arrive as results that table and figure N° 09, it was observed that 98.2% of lawyers considered that in our country we should begin to legislate around the use of deepfake technology, on the other hand, 1.8% of them considered that it is not necessary to legislate in this regard.

Concluding that the use of deepfake technology brings as consequences the generation of a detriment in the image, honor, contributes to foment or exercise material or psychological violence on a person, contributes to disinformation and creates manipulation with respect to information content that the population is willing to validate, attacking the identity and security of netizens.

**Keywords:** Deepfake, identity theft and Law N°. 30096.

## **I. INTRODUCCIÓN**

El avance de la era digital en nuestro país ha traído consigo impactos positivos a través del uso de las tecnologías de la información; sin embargo, con el transcurrir del tiempo se han ido adoptando nuevas modalidades para la comisión de hechos delictivos, como el que es materia de la presente investigación y que se encuentra regulado en el Art. 9 de la Ley 30096- Ley de Delitos Informáticos, denominado Suplantación de Identidad.

Mediante las tecnologías de la información, se ha implementado una nueva técnica conocida como “Deepfake”, que se constituye en una amenaza latente de la identidad y la seguridad del cibernauta dentro del ámbito digital, pues mediante la creación de videos hiperrealistas a través del acceso a fotos y audios de una persona, se puede no solo manipular su rostro sino también su voz, generando a simple vista una percepción de realidad, que genera un menoscabo a la imagen, el honor, fomenta o ejerce violencia material o psicológica sobre una persona, coadyuva a la desinformación y crea manipulación.

Es menester precisar, que dicha tecnología ya llegó a nuestro país y se ha evidenciado a través de la campaña “Perú Te quiero”, donde aparecen personajes como Miguel Grau, Chabuca Granda y Daniel Peredo, brindando un mensaje de reflexión en épocas de pandemia(TvPerú, 2020). Estando a lo anterior, si bien es cierto, actualmente se está utilizando esta técnica digital con fines de concientización social; sin embargo, deja abierta la posibilidad que sujetos inescrupulosos busquen generar un perjuicio valiéndose de estos instrumentos digitales, tal como está sucediendo en países como Estados Unidos y China, donde debido a la gran amenaza que esta técnica digital implica se han adoptado las medidas pertinentes para regular su uso indebido y hacer frente a las consecuencias nocivas de este avance tecnológico.

Siendo así se formuló la siguiente situación problemática ¿De qué manera el deepfake genera consecuencias nocivas que deben ser incorporadas como circunstancias agravantes en el delito de suplantación de identidad en la Ley N° 30096?

Este trabajo, se justificó porque actualmente el tipo penal no regula todas las consecuencias de esta nueva modalidad de suplantación de identidad, lo que da cabida a la impunidad ante la comisión de este hecho delictivo. Es por ello, que la Ley 30096- Ley de Delitos Informáticos debe anticiparse ante tales consecuencias, máxime si esta técnica digital ya está siendo utilizada en nuestro país.

En ese sentido, esta investigación tuvo como objetivo general: Analizar las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096.

Y como objetivos específicos: Identificar las consecuencias nocivas del deepfake que atentan contra la identidad de los cibernautas, Contrastar las regulaciones jurídicas del deepfake a nivel internacional y Proponer la incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096.

Para lo cual se formuló como hipótesis que, el deepfake genera consecuencias nocivas que afectan la identidad y que no se encuentran reguladas en la Ley N° 30096.

## II. MARCO TEÓRICO

Para el desarrollo de este proyecto de investigación se utilizará trabajos previos a nivel internacional, nacional y local, los cuales sirven como fundamento para determinar el objeto de estudio.

A nivel internacional tenemos: Hernández (2019) en su investigación titulada *La Suplantación de Identidad Cibernética en el Ecuador*. Tuvo como objetivo de estudio, determinar que la legislación Ecuatoriana no es suficientemente amplia para proteger los derechos de sus habitantes. Enfoque de estudio cualitativo y el corpus analizado fue la Legislación Ecuatoriana y Derecho Comparado en Chile; los instrumentos empleados fueron entrevistas. Se concluyó que:

Nunca se tomó en cuenta el crecimiento acelerado de la internet y la aparición de nuevas formas de delinquir mediante su uso, por ende, aquellos que están bajo esta jurisdicción no poseen las garantías y seguridades pertinentes para navegar tranquilamente por el ciberespacio. (p. 68)

El autor en su tesis hace referencia a la regulación ineficiente de nuevas modalidades de delitos informáticos que se están incorporando y es que con el transcurrir del tiempo han ido apareciendo otros peligros cibernéticos que ameritan ser regulados, a fin de evitar la impunidad de los mismos.

Montaperto (2018) en su trabajo investigación titulada *Suplantación de identidad: un análisis sobre su falta de regulación en el ordenamiento jurídico argentino*. Tuvo como objetivo de estudio, investigar sobre la falta de marco jurídico regulatorio de la denominada suplantación de identidad de la persona en el Derecho Penal Argentino y cómo dicha circunstancia puede afectar el principio penal de legalidad de la represión como garantía del debido proceso tanto en el art. 18 de la Constitución Nacional como en los tratados con jerarquía constitucional del art. 75 inc. 22 de nuestra carta magna. Enfoque de estudio cualitativo y el corpus analizado fue la Constitución Nacional, el Derecho Penal Brasileiro, el Derecho Penal Paraguayo, el Derecho Penal Colombiano, el Derecho Penal Peruano, el Derecho Penal Español; el instrumento empleado fue un análisis documental. Se concluyó que:

La suplantación de identidad (...) provoca perjuicios patrimoniales, como es la afectación del derecho de propiedad y también consecuencias dañosas en el ámbito extrapatrimonial, como es la vulneración verbigracia del buen nombre, reputación, imagen, prestigio o intimidad de la persona. (p. 81)

El autor en su trabajo de fin de grado enfatiza que, mediante la suplantación de identidad, se genera un detrimento tanto a nivel patrimonial, materializado en una consecuencia netamente económica y un detrimento extrapatrimonial, que abarca la esfera subjetiva del agraviado, conocido como el daño moral.

Vidal (2017) en su trabajo investigación titulado *La falta de regulación frente a la suplantación y usurpación de identidad en Internet*. Tuvo como objetivo de estudio, establecer que la población ecuatoriana posee un conocimiento amplio para preservar sus datos dentro de la era tecnológica. Enfoque de estudio cualitativo y el corpus analizado fue el Código Penal Español de 1995, que regula los delitos informáticos; el instrumento empleado fue un análisis documental. Se concluyó que:

La usurpación de identidad en internet en sus diversas modalidades (...) suponen un peligro para el (...) derecho al honor, a la intimidad personal y familiar o a la propia imagen, así como el patrimonio entre otros (...). (p. 74)

El autor en su trabajo de fin de grado precisa que, suplantar la identidad de una persona a través de un medio tecnológico, se constituye en una grave amenaza que atenta a distintos bienes jurídicos de carácter personal y patrimonial y que ello se debe a que no se cuenta con una adecuada regulación.

Ruiz (2016) en su trabajo de investigación titulada *Análisis De Los Delitos Informáticos Y Su Violación De Los Derechos Constitucionales De Los Ciudadanos*. Tuvo como objetivo de estudio, analizar y conceptualizar la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales. Fue un estudio analítico, como población de estudio se tuvo a profesionales de la abogacía en libre ejercicio y a ciudadanos comunes, como muestra a 30 profesionales de la abogacía en libre ejercicio y a 30 ciudadanos comunes; los instrumentos empleados fue la entrevista y la encuesta. Los principales resultados



fueron de los 30 ciudadanos encuestados, 27 de los encuestados, que corresponde al 90%, consideran que los delitos informáticos vulneran los derechos establecidos en la Constitución; 3 de los encuestados que representan el 10%, no consideran que los delitos informáticos transgredan los derechos establecidos en la Constitución. Se concluyó que:

El poco conocimiento de las tecnologías de la información y la comunicación, es el factor determinante para que profesionales del derecho y magistrados, y los reformadores de la legislación penal en materia informática, hayan omitido ciertos aspectos que deberían incorporarse en la legislación ecuatoriana. (p. 100)

El autor en su investigación precisa que muchos avances tecnológicos son desconocidos por nuestros legisladores, lo que da hincapié a omitirse la incorporación de nuevos supuestos que se deben regular como parte sustantiva de los delitos informáticos.

Zea (2016) en su investigación titulada *Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala*. Tuvo como objetivo de estudio, describir el fenómeno del Robo de identidad en la ciudad de Guatemala mediante dispositivos electrónicos. Fue un estudio descriptivo, como población de estudio se tuvo a profesionales del derecho que litigan en cualquiera de los ámbitos legales; el penal, mercantil o civil en la ciudad capital y usuarios de dispositivos electrónicos en Guatemala, como muestra a 24 profesionales del derecho que litigan en cualquiera de los ámbitos legales; el penal, mercantil o civil en la ciudad capital; los instrumentos empleados fueron diversas entrevistas semiestructuradas a funcionarios de la Policía Nacional Civil (PNC), Ministerio Público y Organismo Judicial. Se concluyó que:

El Estado no está preparado para abordar el fenómeno delictivo informático y por ende contra el robo de identidad a través de dispositivos electrónicos. Lo cual se refleja ante la ausencia de presupuestos de tecnificación y prevención. (p. 90)

El autor en su tesis menciona que los delitos informáticos, en especial el de suplantación de identidad, conocido en Ecuador como robo de identidad, precisando

que no se han adoptado las medidas pertinentes para prevenir la comisión de este hecho delictivo, situación que sucede en forma similar a la realidad peruana.

A nivel nacional tenemos: Caycho & Saguma (2021) en su tesis titulada *Medidas de protección informática y su eficacia en la prevención del delito de suplantación de identidad cibernética en la ciudad de Trujillo, 2020*. Tuvo como objetivo de estudio analizar las medidas de protección y su eficacia en la prevención del Delito de Suplantación de Identidad Cibernética en el distrito de Trujillo, año 2020. Fue un estudio no experimental - básica. como población de estudio se tuvo abogados especializados en Derecho Civil y Penal capacitados en el rubro del Derecho a la Identidad y Delitos Informáticos, ubicados en la ciudad de Trujillo, como muestra a 20 abogados especializados en Derecho Civil y Derecho Penal, en el rubro del derecho a la identidad; el instrumento empleado fue la guía de observación. Los principales resultados fueron el 60 % de abogados que coinciden en opinar que resulta necesario incorporar medidas de protección en la prevención del delito de suplantación de identidad cibernética. Se concluyó que:

El Estado no aplica en su política criminal, medidas de prevención que eviten la comisión del delito de suplantación de identidad cibernética, vulnerando así la seguridad jurídica. (p. 60)

El autor en su tesis hace mención que las estrategias adoptadas por el Estado para contrarrestar el delito de suplantación de identidad no son las adecuadas, ello debido a que la Ley de delitos informáticos no ha incorporado nuevas modalidades de suplantación, poniendo en riesgo de esta manera, la seguridad de los cibernautas.

Zorrilla (2018) en su trabajo de investigación titulado *Inconsistencias y Ambigüedades en la Ley de Delitos Informáticos Ley N° 30096 y su Modificatoria Ley N° 30171, Que Imposibilitan Su Eficaz Cumplimiento*. Tuvo como objetivo de estudio determinar de qué manera se muestran las inconsistencias y ambigüedades en la Ley de delitos informáticos Ley N° 30096 y su modificatoria Ley N° 30171, los cuales imposibilitan su eficaz cumplimiento. Fue un estudio transversal, como población de estudio se tuvo a profesionales de Derecho, Jueces y Fiscales en la ciudad de Barranca, como muestra a 30 entre profesionales de Derecho, Jueces y Fiscales en la ciudad de Barranca; los instrumentos empleados fueron las fichas, especialmente las

Literales y de Resumen, así como la ficha de análisis y la encuesta. Los principales resultados fueron un 53.3% que SI, considera que la ausencia de especialistas en materia de delitos informáticos es un problema para los legisladores pues no tienen un asesoramiento adecuado y un 46.7 % señalaron que NO. Se concluyó que:

Falta que la intención de pertenecer a este Tratado se materialice y se cambie nuestra normativa para amparar a los usuarios y poder navegar en la cuarta dimensión como es el Internet, con la seguridad de no ser víctimas de delincuentes informáticos. (p. 105)

El autor en su trabajo precisa que, si bien es cierto, el Perú se encuentra suscrito al Convenio de Budapest, se debe modificar la regulación de ciertos delitos enmarcados dentro de la Ley de Delitos Informáticos, para así brindar una mayor seguridad a los cibernautas ante las grandes amenazas surgidas de las tecnologías de la información y así garantizar el efectivo cumplimiento de la suscripción al referido convenio.

Romero (2017) en su tesis titulada *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio publico en la ciudad de Huánuco, 2016*. Tuvo como objetivo de estudio determinar los delitos informáticos cometidos mediante redes sociales y el tratamiento que le brinda el Ministerio Publico en la ciudad de Huánuco, 2016. Fue un estudio observacional, prospectivo, transversal, como población de estudio se tuvo todas las denuncias en el Ministerio Público de Huánuco dentro del periodo de enero a diciembre del 2016, haciendo un total 620 procesos, como muestra a 38 casos; los instrumentos empleados fueron entrevistas y encuestas. Los principales resultados fueron el Tratamiento de los delitos informáticos presentados en el Ministerio Publico en la ciudad de Huánuco, fue de la siguiente manera: un 57,9% fueron archivados y un 42,1% terminaron en un proceso normal y con la sentencia dictada. Se concluyó que:

El Perú (...) lamentablemente se encuentra a la deriva en lo que respecta a la adaptación de sus leyes a la nueva era tecnológica, manteniéndose ajeno a aquello que es necesario para su regulación y aplicación eficaz. (p. 106)

El autor en su trabajo refiere que la Ley de delitos informáticos en nuestro país se encuentra desactualizada y ello debido a que no está regulando la incorporación de nuevas circunstancias que están surgiendo a raíz del perfeccionamiento de la tecnología, lo que está generando que su regulación devenga en ineficaz.

A local nacional tenemos: Carrillo & Montenegro (2018) en su trabajo de investigación titulado *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos*. Tuvo como objetivo de estudio analizar la criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. Fue un estudio Descriptiva – Analítico, como población de estudio se tuvo a los Jueces, Los fiscales y los Abogados especialistas en Derecho Penal del Distrito Judicial de Lambayeque, como muestra no probabilística por conveniencia aplicada a 45 personas, divididas en 15 Jueces, 15 Fiscales, y 15 abogados del Distrito Judicial de Lambayeque; los instrumentos empleados fueron las fichas, formatos y cuestionario. Los principales resultados fueron de las 45 personas encuestadas se tiene que el 62% considera estar totalmente de acuerdo y con un 29% que consideraron estar de acuerdo, que el avance tecnológico es el mayor factor que constituye el incremento de delitos informáticos, mientras que el 9% se considera en desacuerdo. Se concluyó que:

Mediante el uso de la tecnología han surgido ciertas modalidades para perpetrar un delito, que no se encuentran correctamente reguladas en el ordenamiento jurídico peruano (...). (p. 108)

El autor en su trabajo precisa que, el avance tecnológico contribuye a la aparición de nuevas modalidades informáticas para perpetrar un hecho delictivo, las cuales no se encuentran totalmente previstas en la Ley 30096.

En relación a las teorías relacionadas al tema de investigación se utilizaron las siguientes:

La génesis regulatoria de los delitos informáticos, aparecieron mediante la promulgación de la Ley N° 27309, el 17 de julio de 2000, donde se incorporaron los delitos informáticos recaídos en el Art. 207-A, Art. 207-B, Art. 207-C y Art. 208 dentro

del Código Penal Peruano, los cuales fueron derogados e incorporados en la Ley N° 30096, que fue publicada el 22 de octubre del 2013, con el propósito de regular en una ley especial nuevas tipificaciones de delitos cometidos mediante tecnologías de la información debido a su peculiar comisión delictiva, constituyéndose en una gran amenaza en el ciberespacio que no podría pasar desapercibido por el legislador; sin embargo, ante la existencia de ciertos vacíos legales se publicó el 10 marzo 2014 la Ley N° 30171, que modificaba algunos artículos de la Ley N° 30096.

Estando a lo anterior, el Perú dentro del marco de la lucha contra la cibercriminalidad, se adhirió al Convenio de Budapest mediante R.L. N° 30913, del 12 de febrero de 2019, con la finalidad de efectivizar la aplicación de la Ley 30096- Ley de delitos informáticos mediante la cooperación internacional con otros países miembros y así combatir la comisión de delitos informáticos, logrando que los ciudadanos se sientan seguros en espacios cibernéticos.

La constante evolución de la tecnología digital genera dificultad para poder distinguir un contenido real de uno falso, y es a razón de ello que surgen los deepfakes, que son *hyper-realistic videos that apply artificial intelligence (AI) to depict someone say and do things that never happened* videos hiperrealistas que aplican inteligencia artificial (IA) para representar a alguien que dice y hace cosas que nunca sucedieron (Westerlund,2019), imitando sus expresiones faciales y su voz debido a la tecnología de mapeo facial que se aplica en su desarrollo.

La amenaza más grande está en el alcance de estos vídeos, dado que *anyone with imagination, a modicum of technical skill, and a personal computer* cualquier persona con imaginación, un mínimo de habilidad técnica y una computadora personal (Lin,2019) puede crear un video falso que a simple percepción puede adoptarse como auténtico y ser masificado por medios sociales *without the consent of those involved* sin el consentimiento de los involucrados (Maras & Alexandrou, 2018) suplantando su identidad.

El delito de suplantación de identidad se encuentra recogido en el Art. 9 de la Ley N° 30096, cuyo tipo objetivo recae en la acción de suplantar, entendida esta como el apoderamiento de la identidad de una persona natural o jurídica. Se debe precisar que, el derecho a la identidad se establece como un derecho de rango fundamental que le

atañe a toda persona desde que nace (Sandoval, 2020) y que es entendido como el conjunto de atributos y características que permiten individualizar a la persona en la sociedad (Álvarez, 2016)

Situación similar, sucede con la identidad digital, que se constituye en una vertiente de la identidad personal, entendida como el conjunto de rasgos y características particulares que una persona expresa a través de internet (Borghello y Temperini, 2017).

En esa misma línea este apoderamiento se realiza mediante acciones ejecutadas por el sujeto activo quien mediante el uso de las tecnologías de la información, se hace pasar por la víctima a través de vía informática, con el propósito de generar un perjuicio material y moral.

Estamos frente a un perjuicio material, cuando se genera un menoscabo patrimonial que puede valorarse económicamente y que se sub divide en 2 vertientes, el daño emergente, que se constituye en las pérdidas dentro del patrimonio del titular del bien, o los gastos que deba asumir para reparar o sustituir la cosa (Vega, 2020), esto es, hace alusión a la pérdida o disminución económica del patrimonio generado a causa del evento dañoso; y el lucro cesante, que es la ganancia esperada que no se obtuvo debido al incumplimiento del contrato o al hecho dañino (Peñailillo,2018), esto es, la frustración de un ingreso que si bien es cierto, todavía no se ha materializado existía una alta probabilidad de ingresar a su patrimonio.

Y por perjuicio moral, a la afectación de la esfera subjetiva de una persona como consecuencia de un actuar ilícito de otra, que conforme lo detalla la Corte Suprema en la CAS. N° 1594-2014 – LAMBAYEQUE se materializa en la lesión a cualquier sentimiento de la víctima considerado socialmente legítimo; (...), no recayendo sobre cosas materiales sino afectando sentimientos.

Por su parte, el tipo subjetivo es eminentemente doloso, puesto que se suplanta con el propósito de generar un perjuicio de índole material o moral, excluyendo la modalidad culposa.

En palabras de Caycho & Saguma (2021): la comisión del Delito de Suplantación de Identidad Cibernética no solo afecta su identidad, sino también su patrimonio, intimidad, imagen; incluyendo (...) la seguridad jurídica (p.14). En ese sentido, se

podría precisar que este delito no solo afecta un bien jurídico protegido, sino que esta conducta (suplantar la identidad de una persona) afecta a una diversidad de bienes jurídicos, por lo que estamos frente a un delito pluriofensivo, cuyo bien jurídico protegido según el tipo penal sería la fe pública, manifestada en la información pero esta considerada en diferentes formas, ya sea como un valor económico o como un valor intrínseco de la persona, por su fluidez y tráfico jurídico (Acurio,2016).

En cuanto a los sujetos del delito, se puede precisar que el sujeto activo es atribuible a cualquier persona que posea habilidades sobre el dominio de sistemas informáticos, por su parte el sujeto pasivo recae tanto en una persona natural como jurídica conforme se desprende de la misma redacción del tipo penal.

La suplantación de identidad puede calificarse como un delito de resultado (Zorrilla, 2018), puesto que además de cometer la conducta establecida en el tipo penal que en este caso sería la acción de “suplantar”, esta acción debe consumir el resultado de generar un perjuicio material o moral, caso contrario estaríamos frente a un supuesto de tentativa.

Estando a lo anterior, esta nueva modalidad de suplantación de identidad, trae como principales consecuencias la afectación al derecho al honor y a la imagen, el primero como aquel derecho que busca proteger el honor tanto en su sentido objetivo y subjetivo, entendido como la reputación o valoración que tenga la sociedad sobre uno mismo, (...) y la consideración que cada uno tenga de sí mismo (Villanueva, 2019), respectivamente. Y el segundo, que otorga protección frente a la captación, reproducción y publicación de la imagen en forma reconocible y visible. (Risso, 2019)

En efecto, el uso de tecnología deepfake, colocan a las personas en situaciones bochornosas que realmente no hubieran realizado, como los llamados “pornovenganzas”, donde si bien es cierto no se difunden imágenes íntimas reales, pero sí creadas o figuradas, para que parezcan verosímiles, de la intimidad de sus protagonistas (Cerdán y Padilla, 2019), o como en el caso de Nancy Pelosi, presidenta de la Cámara de Representantes de Estados Unidos, mediante la circulación de un video donde habían modificado su voz, para aparentar que esta se encontraba bajo los efectos del alcohol y que incluso fue compartido por Donald Trump mediante

Twitter, donde se evidencia el potencial del deepfake como arma política de desinformación, propaganda o ataque al contrario (Cerdán, García y Padilla, 2020).

En esa misma línea, esta tecnología puede fomentar o ejercer violencia material o psicológica sobre una persona, puesto que, al mostrarnos una realidad tergiversada y estando a que *as redes sociais digitais influenciam diretamente o comportamento humano* las redes sociales digitales influyen directamente en el comportamiento humano (Robles, Tinoco y Fachetti, 2020), se puede propiciar la realización de determinados actos de violencia producto de un video falso, representando una seria amenaza para la seguridad social.

Tan solo pongámonos en el hipotético suceso, en que mediante un video deepfake, se presente a una persona emitiendo una opinión racista que nunca emitió, que al ser difundida mediante las redes sociales genera el repudio y la indignación de la población, ocasionando que los cibernautas constantemente le publiquen o lo llamen para mostrarle su rechazo, y pese a que esta persona salga a desmentir tal suceso, su palabra tiene poca credibilidad puesto que lo que se visualiza denota otra versión, ocasionándole una profunda depresión.

Asimismo, los deepfakes originan desinformación, dado que esta nueva tecnología tergiversa la realidad generando que personas mediante su utilización *leverage fabrications and mistruths* aprovechen sus fabricaciones y las falsedades (Wilner, 2018) para obtener algún beneficio, mediante la producción y distribución de contenidos falsos o no veraces (Tandoc, Lim y Ling, 2018).

Y en mérito a que se está frente a una sociedad que consume información proveniente de plataformas de medios de comunicación y redes sociales, es más fácil la difusión de este tipo de videos, puesto que no existe un filtro que permite diferenciar un video auténtico de un video deepfake debido a *scale, and sophistication of the technology involved* la escala y sofisticación de la tecnología involucrada (Fletcher, 2018), obstaculizando de esta manera que los ciudadanos confíen en la información que se les proporciona, llegando a un punto en el que todo será considerado como falso y no se pueda diferenciar la verdad de la falsedad.

En el campo político, puede coadyuvar a generar campañas de desinformación, afectando gravemente la democracia de un país, la cual se ve socavada por la difusión



de noticias falsas (Figueira & Oliveira, 2017), proporcionando *false information spreads very quickly and can be decisive for voter choice*, información falsa que se difunde muy rápidamente y puede ser decisiva para la elección de los votantes. (Ferreira, 2018)

Pero además de ello, crean manipulación, que en palabras de Levitskaya & Fedorov(2020): “*refers to (...) the skillful inducement of another to achieve (pursue) the goal indirectly nested by the manipulator*” se refiere al hábil incentivo de otro para lograr (perseguir) la meta anidada indirectamente por el manipulador. Esto quiere decir que, a través de la creación de estos deepfakes, se pretende adoctrinar a los receptores de esta información, forjando en si una postura que resulta ser de interés de la persona que crea y difunde estos videos engañosos, pues bien se sabe, que dentro del mundo de la información, *evidence is growing of the sophisticated manipulation of technology platforms* cada vez hay más pruebas de la sofisticada manipulación de las plataformas tecnológicas (Morgan,2018) con el propósito de encausar *the opinion in a particular direction* la opinión en una dirección particular. (Morgan,2018)

La gran preocupación radica en el impacto que genera, pues (...) *believing in false things can lead to the failure of our behaviors, and can threaten our well-being and even our lives* (...) creer en cosas falsas puede conducir al fracaso de nuestros comportamientos y puede amenazar nuestro bienestar e incluso nuestras vidas (Ripoll & Matos, 2020).

En países desarrollados como Estados Unidos y China, se han adoptado ciertas medidas legislativas para hacer frente a los videos deepfake, evitar la propagación de esta clase de contenidos o en su defecto restringir aquellos videos que no consignen taxativamente que se trata de un contenido creado y no verídico que pueda inducir a la población a asumirlo como real.

A raíz de la comisión de una serie de casos de deepfakes en Estados Unidos donde personajes políticos y famosos fueron focos del uso de esta tecnología, se procuró establecer su regulación, con el propósito de evitar que casos como estos incrementen y por ende generen una proliferación de noticias falsas valiéndose de medios de comunicación social.

Para citar algunos ejemplos, en diciembre del 2017, se viralizó un video donde aparecía el rostro de la actriz israelí Gal Galdot, quien participó en producciones como

“La Mujer Maravilla” en el cuerpo de una actriz porno, el cual fue reproducido inmediatamente a través de redes sociales. Situación similar ha sucedido con las actrices Emma Watson, Scarlet Johanson y la cantante Taylor Swift.

En el año 2020, el director de redes sociales de la Casa Blanca, Dan Scavino, compartió en Twitter un video de Biden durmiendo y roncando ante la cámara mientras una presentadora de noticias en California intentaba que se despertara para una entrevista, siendo masivamente compartido y utilizado por Donal Trump, su mayor detractor y sus partidarios, para aseverar que debido a la edad que posee se encuentra incapacitado para asumir la presidencia de los Estados Unidos.

Para obtener ese resultado, se tomaron imágenes de la presentadora Leyla Santiago, cuando entrevistaba al artista y activista Harry Belafonte, quien tenía los ojos cerrados y no respondió a sus exhortaciones de "despertar". Mientras que las imágenes de Biden fueron tomadas de una conversación en video del 2020 con la exsecretaria de Estado Hillary Clinton, donde Joe Biden miró hacia abajo y sus ojos parecían al menos parcialmente cerrados durante parte de la conversación.

Estando a lo anterior en EE.UU, los estados de Texas y California, han empezado a legislar sobre los videos deepfake desde el año 2019, a raíz de los innumerables deepfakes creados en campaña política para perjudicar a los demás contendores políticos e influir en el resultado de una elección.

Así pues, se tiene que en el Estado de Texas entró en vigencia el 01 de septiembre del 2019, la Ley SB 751, con la que se buscó evitar una contienda política maliciosa y sancionar a aquella persona que utilizando tecnología artificial crea un video deepfake, para lograr que un candidato político sea mal visto frente a la población, y asimismo se sanciona a quien lo difunde o distribuye dentro del margen de los 30 días próximos a una elección, por cuanto mediante este tipo de tecnologías de la información se expone la imagen de dicho candidato en una situación que genera el rechazo de la población.

Situación similar se adoptó en el Estado de California, mediante la Ley AB-730, que fue aprobado el 03 de octubre del 2019, donde en su sección 3, estableció la adopción de una medida preventiva durante la campaña electoral tendiente a evitar la generación de confusión de los videos deepfake, razón por la cual se legisló que

aquellos videos que posean un contenido no realista y se desee difundir, se consigne expresamente "Esta imagen no es una representación precisa de un hecho". Sin embargo, en su sección 4, hace precisión a un margen temporal que excluye lo establecido en la sección 3, puesto que se prohíbe cualquier contenido engañoso durante los 60 días de una elección, que se haya creado con el propósito de dañar al candidato o de engañar al elector para que vote a favor o en contra de un candidato determinado.

Asimismo, se encuentra pendiente el Proyecto de Ley AB-1280, que aborda el aspecto relacionado a grabaciones engañosas mediante tecnología deepfake el cual se pretende incorporar en la sección 644 del Código Penal, donde se hace mención al consentimiento de la persona presentada en videos deepfake siendo partícipe de una conducta sexual, situación que también es denominada "pornovenganza", puesto que este tipo de contenido es generado a raíz de un acto de venganza hacia una persona con el propósito de denigrarlo frente a los demás, exigiendo además de una pena privativa de libertad no menor de 01 año, una multa de \$ 1,000, sancionándose pecuniariamente en una magnitud mayor con \$ 10,000 cuando la persona que es exhibida mediante videos deepfake, tenga menos de 18 años.

Este proyecto, sigue la misma línea que las 02 leyes antes mencionadas en cuanto a la difusión de videos deepfake durante una contienda electoral, al sancionarse a aquel que dentro de los 60 días de una elección sin el consentimiento de la víctima difunda material producto de la tecnología deepfake.

Ahora bien, en Pensilvania- EE.UU, uno de los estados que aún no ha regulado el uso de tecnología deepfake, tuvo su primer caso mediante la utilización de un deepfake malicioso, donde una madre fue detenida por enviar a las porristas, sus padres y los dueños del gimnasio, una serie de mensajes anónimos que contenían imágenes y videos manipulados que intentaban incriminar a tres adolescentes del gimnasio de porristas Victory Vipers en Doylestown, con representaciones falsas que mostraban a algunos de ellos desnudos, bebiendo alcohol o vapeando, con el propósito de que fueran retiradas del equipo de porristas y su hija pueda obtener uno de esos puestos.

Ante ello, al no encontrarse regulado el uso de esta tecnología digital, las autoridades optaron por tipificarlo como acoso cibernético en contra de las menores porristas.

Con fines didácticos, es menester hacer una precisión en cuanto al delito de acoso cibernético frente al delito de suplantación de identidad en su modalidad de deepfake, puesto que, si bien en ambos se utiliza tecnología digital, la diferencia radica en las acciones que se despliegan en cada una de ellas, mientras en el primero se vigila, esto es, se mantiene en observación constante sobre todo lo que realiza la víctima; persigue, esto es que la busca en forma constante; hostiga, en relación al denotar insistencia para obtener una respuesta y asedia, con el que se busca incomodar a una persona a razón de una acción constante; en el segundo valiéndose de la tecnología se suplanta la identidad de una persona.

Asimismo, respecto al fin que se persigue, en tanto en el ciberacoso se busca lograr un contacto con una persona pese a la negativa de la víctima generando una alteración del normal desarrollo de su vida, entendida esta como el fomento de intranquilidad y angustia por el constante acecho del acosador, que ocasiona cambios de ciertos hábitos tradicionales de la víctima, limitando su libertad de actuación (Carranza, 2019), en la suplantación de identidad, se pretende lograr una afectación material o moral.

En ese sentido, el caso antes señalado, bien podría encausarse como un delito de suplantación de identidad en su modalidad de deepfake; sin embargo, al no contar con una regulación explícita en cuanto al uso de esta tecnología, se optó por su consideración como delito de acoso cibernético.

Por su parte en China, las alarmas del uso de tecnología deepfake se activaron a raíz de la creación de la aplicación China Zao, en septiembre del 2019, a través del cual los usuarios podían intercambiar su rostro por el de una celebridad con una sola foto en tiempo record, convirtiéndolo en la aplicación con más descargas en la App Store de IOS en China; sin embargo, la preocupación se incrementó cuando los usuarios se percataron que en las políticas de privacidad, cedían los derechos de propiedad intelectual sobre su rostro, permitiendo que la empresa Zao utilice su imagen con fines de marketing.

Por lo que, ante tal suceso en China, entró en vigencia desde el 01 de enero del 2020 el "Reglamento sobre la administración de servicios de información de audio y vídeo en línea", con el propósito de promover el desarrollo sano y ordenado de los servicios de información de audio y vídeo en línea, proteger los derechos e intereses legítimos de los ciudadanos, las personas jurídicas y otras organizaciones y salvaguardar la seguridad nacional y los intereses públicos. El referido reglamento en su Art. 11 y 12 reza lo siguiente:

**第十一条** 网络音视频信息服务提供者和网络音视频信息服务使用者利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播非真实音视频信息的，应当以显著方式予以标识。

网络音视频信息服务提供者和网络音视频信息服务使用者不得利用基于深度学习、虚拟现实等的新技术新应用制作、发布、传播虚假新闻信息。

生產、發布或傳播法律、法規禁止的信息內容的任何人，必須依法停止信息的傳播，並採取刪除等措施，以防止信息傳播，保留相關記錄並告知信息，文化和環境。互聯網，廣播電視的旅遊部門。

En este dispositivo legal, en su artículo 11 se hace referencia a los deepfake, como audio y video en red mediante tecnologías y aplicaciones basadas en la realidad virtual que posee un contenido no real, señalando que aquellas personas que elaboran estos videos y los que lo difundan con el propósito de transmitir alguna información, deben obligatoriamente marcarlos de una manera llamativa, de modo que se pueda diferenciar a simple percepción que el vídeo que están visualizando no es un reflejo verídico de un audio o video real, sino que mediante esta tecnología se buscó transmitir un contenido informativo.

Por otro lado, también precisa que aquellos deepfake que estén destinados a proporcionar una información no real queda prohibida, por cuanto el uso de este tipo de tecnologías es utilizado para crear, publicar y difundir noticias falsas generando desinformación.

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

Lamentablemente en el Perú, no se han adoptado las medidas pertinentes para poder contrarrestar esta grave amenaza que se acerca de a pocos a nuestra realidad, dejando abierta la posibilidad de cometer suplantaciones de identidad en base a la creación de estos vídeos deepfake sin recibir una sanción adecuada, máxime si esta nueva tecnología crea mundos paralelos (...) que los ciudadanos están dispuestos a validar. (Marcos, Sanchez & Olivera, 2017)

En efecto, la combinación de resultados fotorrealistas y la facilidad de uso plantean un desafío para la detección de estos vídeos (Cerdán, García & Padilla, 2020), más aún si nuestro país, no se encuentra debidamente capacitado y preparado para hacer frente a la tecnología deepfake.

A lo largo de este trabajo, se ha mencionado sobre los impactos negativos de esta técnica digital; sin embargo, ¿todos los deepfakes son meritorios de sanción?

La respuesta es no, ello debido a que múltiples deepfakes también son utilizados con fines cinematográficos, de información o entretenimiento, es en ese sentido, que para determinar cuándo un deepfake debe ser sancionado, se debe tomar en cuenta, los siguientes aspectos, conforme lo precisa Ruiters. (2021): (i) *whether the deepfaked person(s) would object to the way in which they are represented;* (ii) *whether the deepfake deceives viewers;* and (iii) *the intent with which the deepfake was created.*(párr.1) i) si las personas que aparecen en un deepfake objetarían la forma en que están representadas; (ii) si el deepfake engaña a los espectadores; y (iii) la intención con la que se creó el deepfake.

En relación al primer aspecto, la persona que aparece en un deepfake, debe verse afectada por la creación del video, y la representación digital de sí mismo en una

situación bochornosa, exponiéndolas *in ways in which they do not wish to be portrayed* en formas en que no desean ser retratados (De Ruiter, 2021)

Sobre el segundo aspecto, el contenido deepfake debe ser realista y adoptado como auténtico por la simple percepción de los demás, quienes, debido a la sofisticación y calidad del video creado, genera una apariencia realista de personas que hacen o dicen cosas que no necesariamente hicieron o dijeron, poniendo en duda la confiabilidad visual.

Finalmente, sobre el tercer aspecto, está dirigido al propósito de su creación, que se evidencia a través del impacto que el video deepfake genera, sea esta con un fin cinematográfico, de información, de entretenimiento o para causar un perjuicio, es en este último supuesto, en que se amerita actuar de inmediato.

A continuación, para una mejor comprensión del tema objeto de investigación, se presenta la definición de los términos más relevantes utilizados en el presente proyecto:

1. Deepfake: Video falso creado mediante inteligencia artificial, que simula gestos y voz de una persona presentándola ante situaciones que nunca hubieran realizado o dicho.
2. Pornovenganza: Difusión de imágenes de contenido íntimo de una persona sin el consentimiento de esta con el propósito de generarle un perjuicio y bajo un móvil de venganza.
3. Ciberacoso: Acoso realizado a través de medios virtuales, mediante mensajes o llamadas constantes pese al rechazo de la víctima, con la finalidad de tener cercanía con ella.
4. Cibernauta: Persona que hace uso de medios digitales para navegar en la virtualidad.
5. Suplantación de identidad: Acción consistente en asumir como suya la identidad de una persona mediante el uso de medios informáticos.
6. Tecnología artificial: Tecnología utilizada para presentar características similares del ser humano, mediante la creación de programas dotados de medios sofisticados que se perfeccionan con el tiempo.

7. Redes sociales: Son plataformas mediante las cuales se tiene acceso e intercambia información con el propósito de ser masificada y tener mayor alcance social.



### **III. METODOLOGÍA**

#### **3.1. Tipo y diseño de investigación**

El tipo de investigación fue básica, porque en mérito a la problemática evidenciada a través de las consecuencias nocivas del deepfake, se justificó la pertinencia para su estudio y la relevancia dentro el campo del Derecho Penal y en mérito a un análisis sistematizado de la información encontrada se pretendió arribar a ciertas conclusiones que brindan una respuesta al problema de investigación, para finalmente proponerse la incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad.

El diseño de la investigación fue no experimental, porque se utilizó un método descriptivo-explicativo, destinado a describir y analizar los aspectos teóricos jurídicos en concordancia con los objetivos de investigación propuestos y contrastarlo con los antecedentes, para evidenciar la problemática latente en cuando a cibercriminalidad en el Perú, en materia de suplantación de identidad y así discutir e interpretar las notables falencias en la Ley de delitos informáticos.

#### **3.2. Variables y operacionalización**

##### **3.2.1. Variable independiente**

Deepfake

###### **3.2.1.1. Definición conceptual:**

Videos hiperrealistas que aplican inteligencia artificial (IA) para representar a alguien que dice y hace cosas que nunca sucedieron. (Li,2019).

###### **3.2.1.2. Definición operacional:**

Saberes de los operadores jurisdiccionales respecto a las consecuencias nocivas del deepfake. Se medirá con un cuestionario a partir del análisis de los conocimientos de los operadores jurisdiccionales sobre las consecuencias nocivas del deepfake.

###### **3.2.1.3. Dimensiones:**

3.2.1.3.1. Política criminal.

3.2.1.3.2. Consecuencias del Deepfake.

3.2.1.3.3. Deficiencias en relación a la regulación del deepfake.

#### **3.2.1.4. Indicadores**

2.2.1.4.1. Suscripción del Convenio de Budapest, Promulgación de la Ley N° 30096 y Creación de la Fiscalía Especializada de Delitos Informáticos.

2.2.1.4.2. Afectación a la imagen, Afectación al honor, Fomenta o ejerce violencia material o psicológica sobre una persona, Coadyuva a la desinformación y Crea manipulación.

2.2.1.4.3. Conocimiento de las consecuencias del deepfake, Capacitación a los operadores de justicia en materia informática y Herramientas digitales pertinentes para la detección de videos deepfake.

#### **3.2.1.5. Escala de Medición:**

Nominal.

### **3.2.2. Variable dependiente**

Delito de suplantación de identidad.

#### **3.2.2.1. Definición conceptual:**

Consiste en un ataque informático, de ingeniería social que tiene por finalidad la adquisición de información confidencial de la víctima (...) pudiendo provocar perjuicios patrimoniales, (...) y extrapatrimonial, (...). (Montaperto, 2018).

#### **3.2.2.2. Definición operacional:**

Saberes de los operadores jurisdiccionales respecto a la aparición de nuevas modalidades de suplantación de identidad. Se medirá con un cuestionario a partir del análisis de los conocimientos de los operadores jurisdiccionales sobre suplantación de identidad.

#### **3.2.2.3. Dimensiones:**

3.2.2.3.1. Política criminal

3.2.2.3.2. Consecuencias

#### **3.2.2.4. Indicadores**

3.2.2.4.1. Suscripción del Convenio de Budapest, Promulgación de la Ley N° 30096 y Creación de la Fiscalía Especializada de Delitos Informáticos.

3.2.2.4.2. Perjuicio material y Perjuicio moral.

**3.2.2.5. Escala de Medición:**

Nominal.

**3.3. Población, muestra y muestreo**

**3.3.1. Población:**

La población estuvo constituida por Abogados especialistas en Derecho Penal.

**3.3.1.2. Criterio de Inclusión:**

Como criterio de inclusión, se tuvo a Abogados especialistas en Derecho Penal, pertenecientes al Colegio de Abogados de Lambayeque.

**3.3.1.2. Criterio de Exclusión:**

Como criterio de exclusión, se tuvo a aquellos abogados del Colegio de Abogados de Lambayeque, cuyas ramas de especialización en el campo del derecho fuera distinta al campo del Derecho Penal.

**3.3.2. Muestra:**

La muestra que se utilizó estuvo constituida por 50 abogados especialistas en Derecho Penal.

**3.3.3. Muestreo:**

Se aplicó un muestreo no probabilístico selectivo por conveniencia, dado que para la determinación del mismo no se empleó una formula estadística, sino que estuvo sujeto a los criterios de inclusión y exclusión establecidos por el investigador.

**3.3.4. Unidad de análisis:**

Como unidad de análisis se tiene al abogado especialista en Derecho Penal, perteneciente al Colegio de Abogados de Lambayeque.

**3.4. Técnicas e instrumentos de recolección de datos**

Para la recolección de datos, se ha hecho uso de la técnica de encuesta, que fue aplicada a los especialistas en Derecho Penal, pertenecientes al

Colegio de Abogados de Lambayeque, con la cual se recolectó la información necesaria que sirvió para contrastar las bases teóricas del proyecto de investigación.

Y como instrumento de recolección de datos, se utilizó un cuestionario, el cual fue elaborado en base a los indicadores del cuadro de operacionalización elaborado, que buscó dar respuesta a las variables independiente y dependiente planteadas y validado por el asesor temático, otorgando el grado de confiabilidad necesario para su aplicación.

### **3.5. Procedimientos**

Se elaboró la encuesta online vía Google drive, que permita obtener la base de datos idónea para complementar la investigación, la misma que fue difundida mediante enlace de formulario de Google a la muestra de investigación establecida. Luego de la recopilación de los datos mediante la aplicación del cuestionario, se esquematizó la información obtenida por esta fuente especializada en la materia, mediante el sistema de SPSS, Word y Excel como técnicas de procesamiento de datos, las cuales fueron analizadas estadísticamente, generando la elaboración de tablas y figuras que plasmaron los resultados arribados en la investigación.

### **3.6. Método de análisis de datos**

El método de análisis de datos utilizado fue el deductivo, porque se partió del estudio de datos generales hacia datos particulares, partiendo de un todo a un aspecto en específico dando respuesta a los objetivos propuestos en la investigación; y analítico, porque en mérito a la información y a los resultados que se obtuvieron, se analizarán las consecuencias nocivas del deepfake y cómo estas deberían ser incorporadas como agravantes en el delito de suplantación de identidad.

### **3.7. Aspectos éticos**

La investigación desarrollada se encontró sujeto a los parámetros establecidos en la guía de productos observables proporcionada por la institución, respetándose el contenido propio de los autores utilizados en el marco teórico de la investigación mediante la correcta cita y parafraseo en

formato APA, predominando la creación teórica propia del investigador y que se coteja con el programa Turnitin.

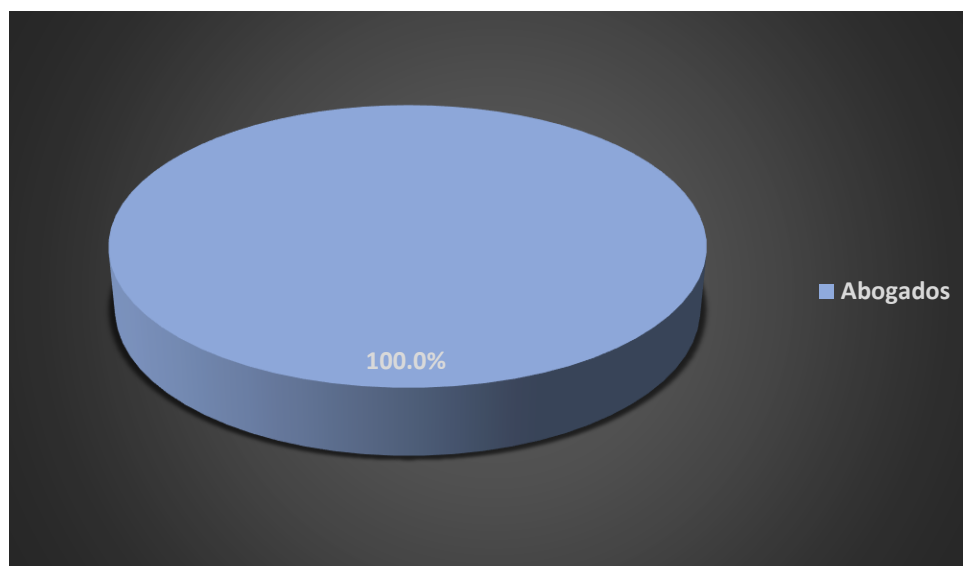
#### IV. RESULTADOS

**Tabla N° 01. Condición de encuestados: Abogados.**

	<b>Cantidad</b>	<b>Porcentaje</b>
<b>Abogados</b>	55	100%

Fuente: Investigación Propia

**Figura N° 01.**



Fuente: Investigación Propia

De acuerdo con la tabla y figura N° 01, el instrumento de recolección de datos (cuestionario) fue aplicado a 55 abogados del Ilustre Colegio de Abogados de Lambayeque, equivalente al 100%.

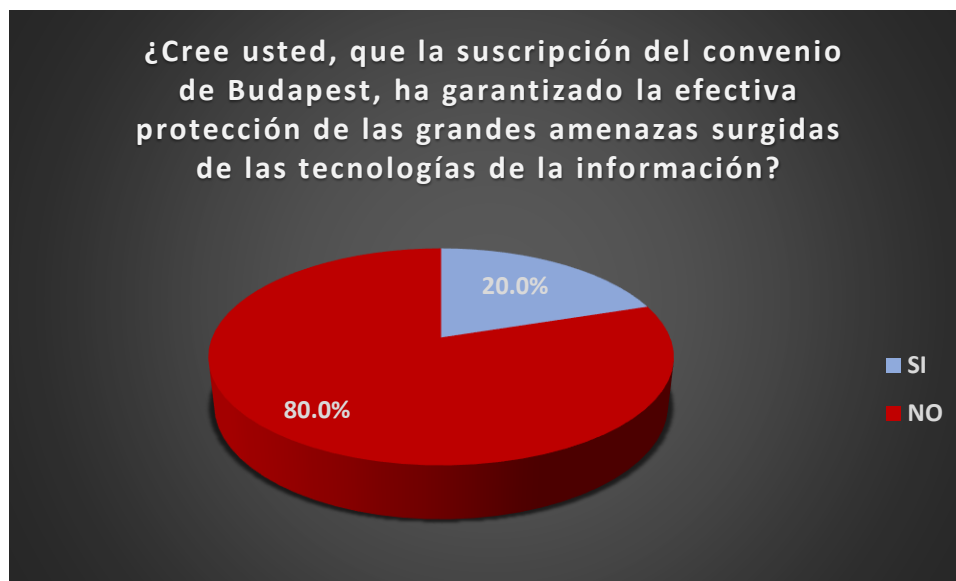
**Tabla N° 02. ¿Cree usted, que la suscripción del convenio de Budapest, ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información?**

<b>Respuesta</b>	<b>Cantidad</b>	<b>Porcentaje</b>
<b>SI</b>	11	20%

<b>NO</b>	44	80%
<b>TOTAL</b>	55	100%

Fuente: Investigación Propia

**Figura N° 02.**



Fuente: Investigación Propia

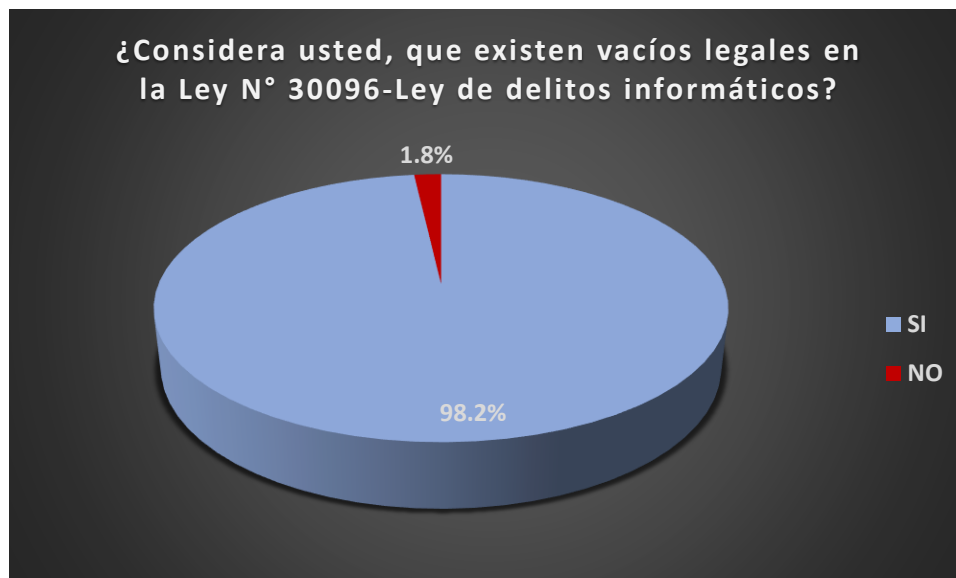
En relación a la tabla y figura N° 02, se observó que el 80% de abogados consideró que la suscripción del convenio de Budapest, no ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información, mientras que el 20% de ellos consideró que sí.

**Tabla N° 03. ¿Considera usted, que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos?**

Respuesta	Cantidad	Porcentaje
<b>SI</b>	54	98.2%
<b>NO</b>	01	1.8%
<b>TOTAL</b>	55	100%

Fuente: Investigación Propia

**Figura N° 03.**



**Fuente:** Investigación Propia

Según la tabla y figura N° 03, se observó que el 98.2% de abogados consideró que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos, mientras que el 1.8% de ellos consideró que no.

**Tabla N° 04. ¿Considera usted, que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen?**

Respuesta	Cantidad	Porcentaje
SI	54	98.2%
NO	01	1.8%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia



**Figura N° 04.**



**Fuente:** Investigación Propia

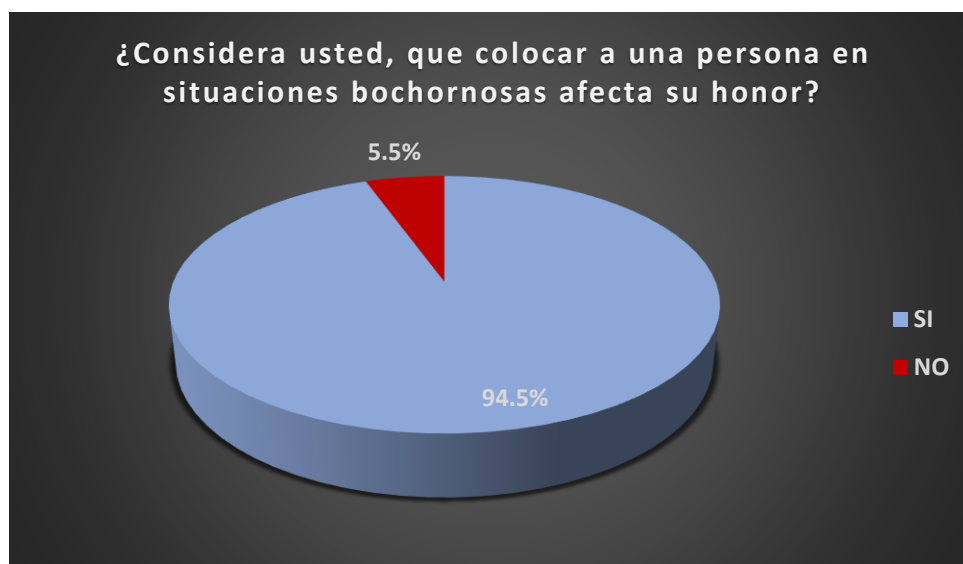
En mérito a la tabla y figura N° 04, se observó que el 98.2% de abogados consideró que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen, mientras que el 1.8% de ellos consideró que no se genera afectación alguna.

**Tabla N° 05. ¿Considera usted, que colocar a una persona en situaciones bochornosas afecta su honor?**

Respuesta	Cantidad	Porcentaje
SI	52	94.5%
NO	03	5.5%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 05.**



**Fuente:** Investigación Propia

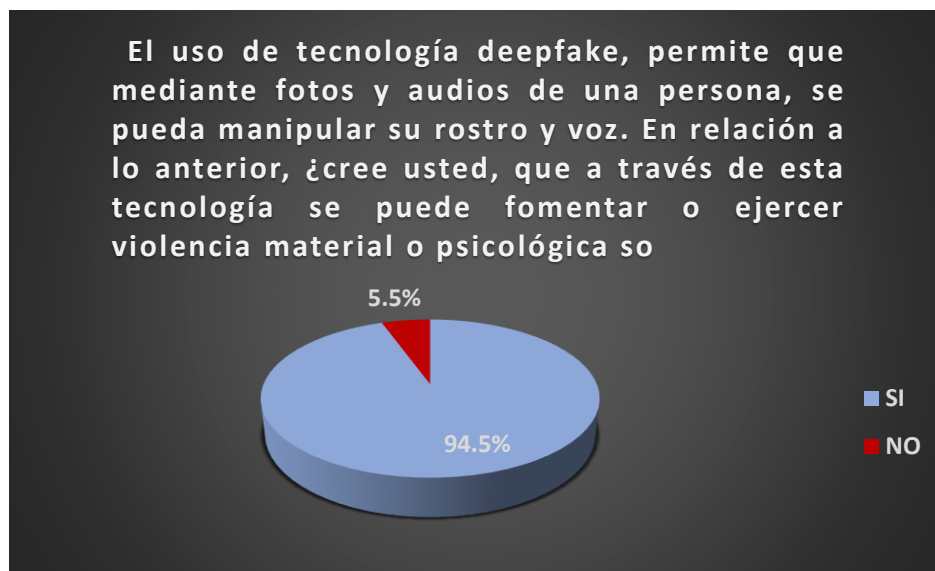
En mérito a la tabla y figura N° 05, se observó que el 94.5% de abogados consideró que colocar a una persona en situaciones bochornosas afecta su honor, mientras que el 5.5% de ellos consideró que no.

**Tabla N° 06. El uso de tecnología deepfake, permite que mediante fotos y audios de una persona, se pueda manipular su rostro y voz. En relación a lo anterior, ¿cree usted, que a través de esta tecnología se puede fomentar o ejercer violencia material o psicológica sobre una persona?**

Respuesta	Cantidad	Porcentaje
SI	52	94.5%
NO	03	5.5%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 06.**



**Fuente:** Investigación Propia

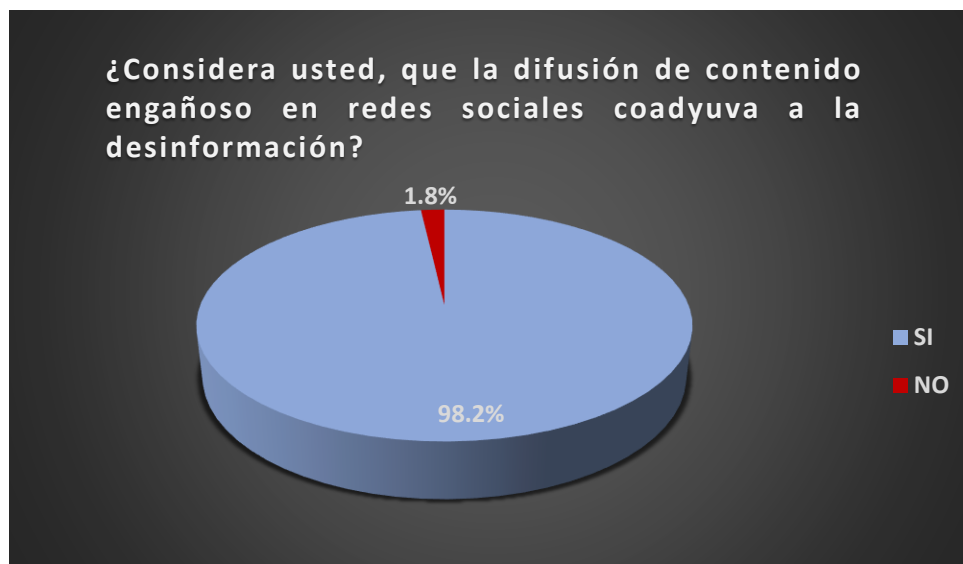
En mérito a la tabla y figura N° 06, se visualizó que el 94.5% de abogados consideró que mediante el uso de tecnología deepfake se puede fomentar o ejercer violencia material o psicológica sobre una persona, mientras que el 5.5% de ellos consideró que no.

**Tabla N° 07. ¿Considera usted, que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación?**

Respuesta	Cantidad	Porcentaje
SI	54	98.2%
NO	01	1.8%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 07.**



**Fuente:** Investigación Propia

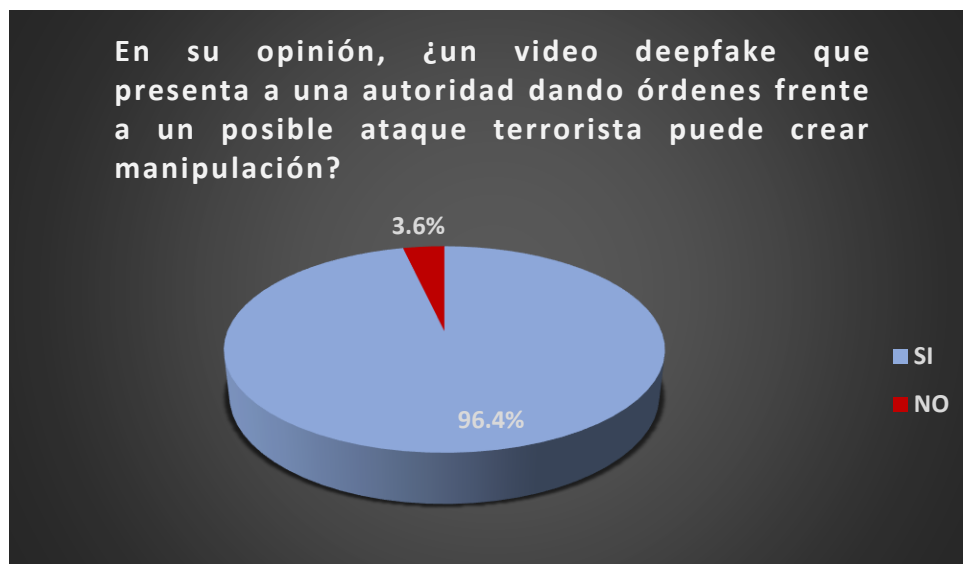
En mérito a la tabla y figura N° 07, se visualizó que el 98.2% de abogados consideró que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación, mientras que el 1.8% de ellos consideró que no.

**Tabla N° 08. En su opinión, ¿un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación?**

Respuesta	Cantidad	Porcentaje
SI	53	96.4%
NO	02	3.6%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 08.**



**Fuente:** Investigación Propia

En mérito a la tabla y figura N° 08, se observó que el 96.4% de abogados consideró que un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación, por otro lado el 3.6% de ellos consideró que no.

**Tabla N° 09. En países como EE.UU y China, se han empezado a adoptar ciertas medidas legislativas para regular el uso de tecnología deepfake. ¿Considera usted, que nuestro país debe empezar a legislar al respecto?**

Respuesta	Cantidad	Porcentaje
SI	54	98.2%
NO	01	1.8%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 09.**



**Fuente:** Investigación Propia

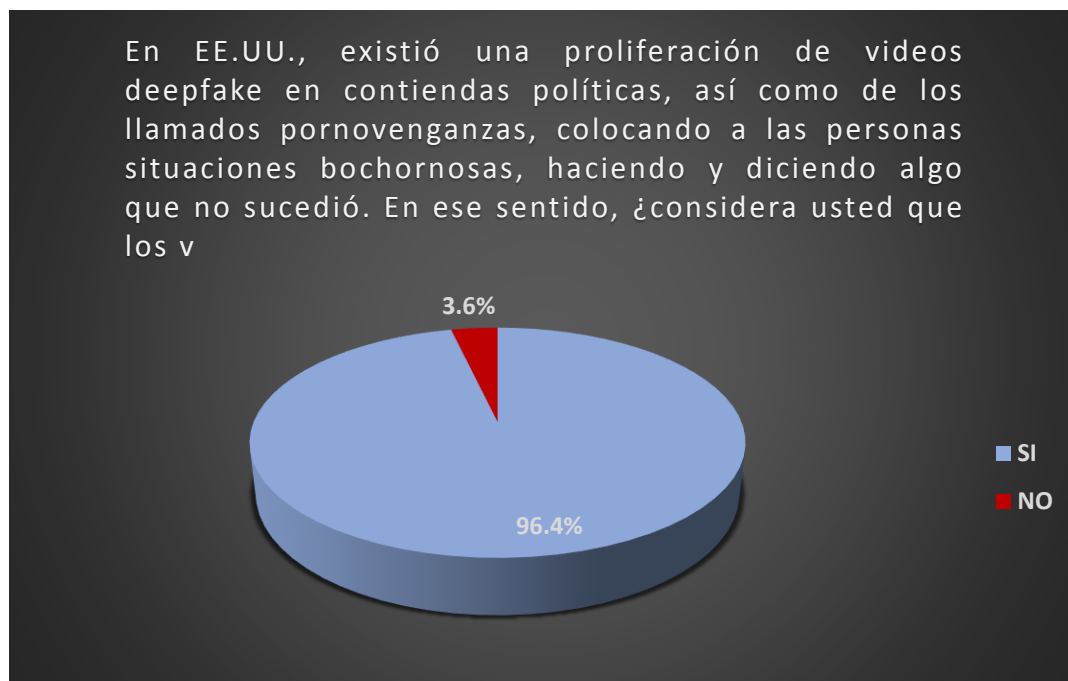
En mérito a la tabla y figura N° 09, se observó que el 98.2% de abogados consideró que en nuestro país se debe empezar a legislar en torno al uso de tecnología deepfake, por otro lado el 1.8% de ellos consideró que no es necesario legislar al respecto.

**Tabla N° 10. En EE.UU., existió una proliferación de videos deepfake en contiendas políticas, así como de los llamados pornovenganzas, colocando a las personas situaciones bochornosas, haciendo y diciendo algo que no sucedió. En ese sentido, ¿considera usted que los videos deepfakes suplantan la identidad de una persona?**

Respuesta	Cantidad	Porcentaje
SI	53	96.4%
NO	02	3.6%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 10.**



**Fuente:** Investigación Propia

En mérito a la tabla y figura N° 10, se observó que el 96.4% de abogados consideró que los videos deepfakes suplantan la identidad de una persona, por otro lado el 3.6% de ellos consideró que no suplanta la identidad.

**Tabla N° 11. En China, se ha legislado la prohibición de videos deepfake que son utilizados para crear, publicar y difundir noticias falsas. En su opinión,¿ este tipo de videos deberían prohibirse en nuestro país por generar desinformación?**

Respuesta	Cantidad	Porcentaje
SI	52	94.5%
NO	03	5.5%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 11.**



**Fuente:** Investigación Propia

En mérito a la tabla y figura N° 11, se observó que el 95.4% de abogados consideró que los videos deepfakes deberían prohibirse en nuestro país por generar desinformación, por otro lado el 5.5% de ellos consideró que no genera desinformación.

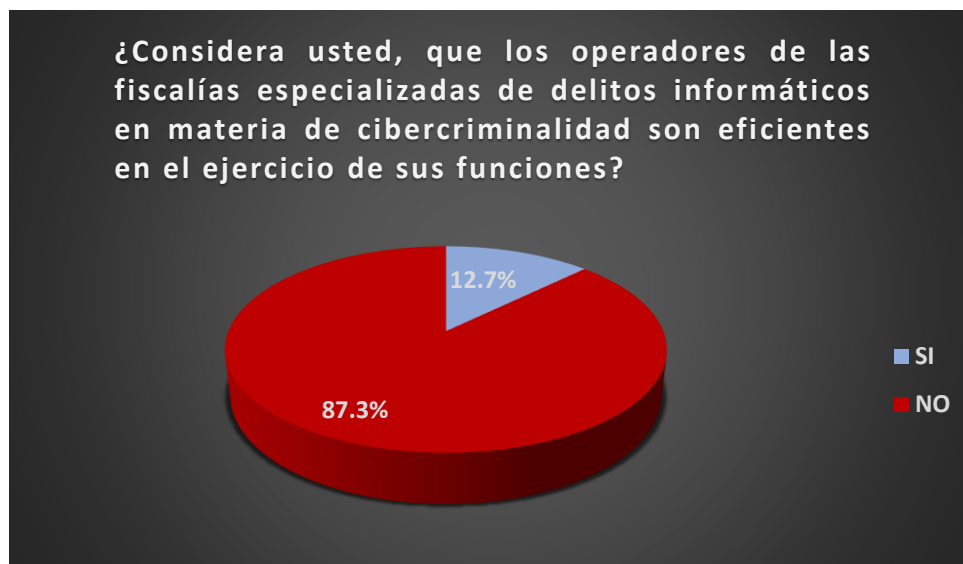
**Tabla N° 12. ¿Considera usted, que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones?**

Respuesta	Cantidad	Porcentaje
SI	07	12.7%
NO	48	87.3%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia



**Figura N° 12.**



**Fuente:** Investigación Propia

En mérito a la tabla y figura N° 12, se observó que el 87.3% de abogados consideró que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad no son eficientes en el ejercicio de sus funciones, por otro lado el 12.7% de ellos consideró que sí.

**Tabla N° 13. En su opinión, ¿los operadores de justicia se encuentran debidamente capacitados en materia informática?**

Respuesta	Cantidad	Porcentaje
SI	01	1.8%
NO	54	98.2%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 13.**



**Fuente:** Investigación Propia

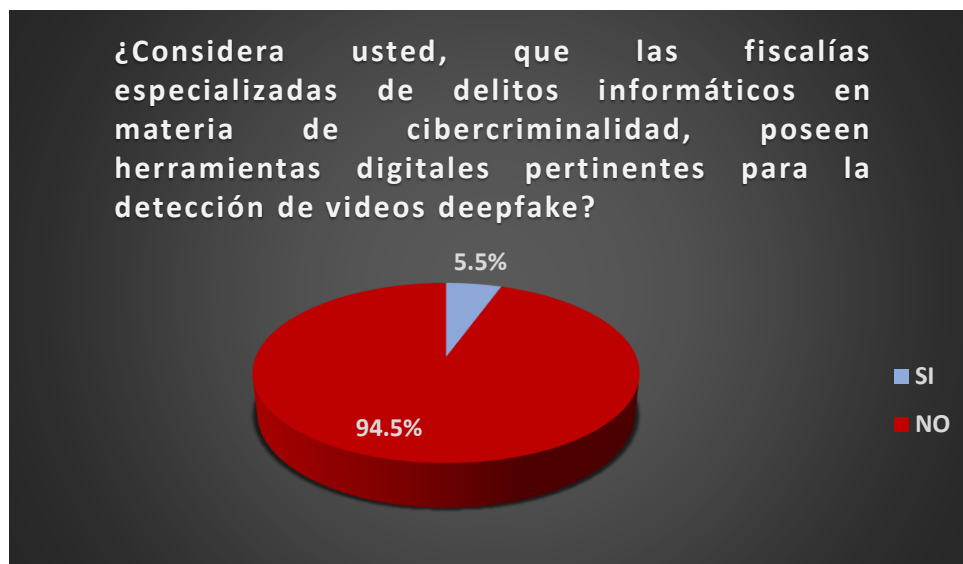
En mérito a la tabla y figura N° 13, se observó que el 98.2% de abogados consideró que los operadores de justicia no se encuentran debidamente capacitados en materia informática, por otro lado el 1.87% de ellos consideró que sí.

**Tabla N° 14. ¿Considera usted, que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes para la detección de videos deepfake?**

Respuesta	Cantidad	Porcentaje
SI	03	5.5%
NO	52	94.5%
<b>TOTAL</b>	<b>55</b>	<b>100%</b>

**Fuente:** Investigación Propia

**Figura N° 14.**



**Fuente:** Investigación Propia

En mérito a la tabla y figura N° 14, se observó que el 94.5% de abogados consideró que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, no poseen herramientas digitales pertinentes para la detección de videos deepfake, por otro lado, el 5.5% de ellos consideró que sí.

**Tabla N° 15. El uso de tecnología deepfake, genera como consecuencias nocivas, la afectación al derecho al honor, a la imagen, fomenta o ejerce violencia física o material sobre una persona, crea manipulación y coadyuva a la desinformación. En ese sentido ¿considera usted que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad?**

Respuesta	Cantidad	Porcentaje
SI	54	98.2%
NO	01	1.8%

---

<b>TOTAL</b>	55	100%
--------------	----	------

---

Fuente: Investigación Propia

**Figura N° 15.**



Fuente: Investigación Propia

En relación a la tabla y figura N° 15, se observó que el 98.2% de abogados consideró que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad, por otro lado, el 1.8% de ellos consideró que no es necesario.

## V. DISCUSIÓN

En mérito al objetivo general se obtuvieron como resultados de la tabla y figura 2 y 3, que del total de encuestados un 80% consideran que la suscripción al convenio de Budapest, no ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información y un 98.2% consideran que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos.

Contexto que se condice con lo señalado por Romero (2017), mismo que fue citado en el desarrollo del marco teórico, cuando concluye que el Perú no ha ido adaptando sus leyes a la nueva era tecnológica. Para la autora, en efecto, la Ley de delitos informáticos en nuestro país se encuentra desactualizada y ello debido a que no está regulando la incorporación de nuevas circunstancias que están surgiendo a raíz del perfeccionamiento de la tecnología, lo que está generando que su regulación devenga en ineficaz.

En relación al primer objetivo específico se buscó identificar las consecuencias nocivas del deepfake que atentan contra la identidad de los cibernautas; en relación a ello, se arribó como resultados de la tabla y figura 4,5,6,7 y 8, que un 98.2 % considera que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a la imagen, que como bien lo precisaba el Dr. Elías, es un derecho conexo al derecho a la identidad de la persona suplantada o de quien se hace uso para generar estos mensajes falsos, que como lo precisa en el marco teórico Risso (2019), se ve vulnerado por la captación, reproducción y publicación de la imagen en forma reconocible y visible.

Por su parte, un 94.5% considera que colocar a una persona en situaciones bochornosas afecta su honor, como los llamados pornovenganzas, donde conforme lo señala Cerdán y Padilla (2019), si bien es cierto no se difunden imágenes íntimas reales, pero sí creadas o figuradas, para que parezcan verosímiles, de la intimidad de sus protagonistas. Un mismo porcentaje, considera que a través del uso de tecnología deepfake, se puede fomentar o ejercer violencia material o psicológica sobre una persona, lo que se condice con lo precisado por (Robles, Tinoco y Fachetti, 2020), en mérito a que las redes sociales digitales influyen directamente en el comportamiento humano.

Por otro lado, un 98.2% considera que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación, que de acuerdo con Tandoc, Lim y Ling (2018), se realiza para obtener algún beneficio, mediante la producción y distribución de contenidos falsos o no veraces y un 96.4% opinan que un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación, atentando gravemente contra la seguridad pública, a tenor de lo señalado por el Dr. Elías (2021), pues conforme lo señaló en el marco teórico Ripoll & Matos (2020), creer en cosas falsas puede conducir al fracaso de nuestros comportamientos y puede amenazar nuestro bienestar e incluso nuestras vidas.

En esa línea, dichos resultados se contrastan con lo precisado por Montaperto (2018) y Caycho y Saguma (2021), en relación a que el uso de esta tecnología genera consecuencias, no solo a nivel patrimonial, sino también a nivel extrapatrimonial. Mismas que se materializan a través de la afectación al derecho a la imagen, el honor, coadyuvar a la desinformación y crear manipulación.

El segundo objetivo específico pretendió contrastar las regulaciones jurídicas del deepfake a nivel internacional, así pues, se tiene la tabla y figura 9,10 y 11, donde un 98.2% considera que el Perú debe empezar a legislar respecto al deepfake, un 96.4% considera que los videos deepfakes suplantan la identidad de una persona y un 94.5% opinan que este tipo de videos deberían prohibirse por generar desinformación.

En países desarrollados como Estados Unidos y China, se adoptaron ciertas medidas legislativas para hacer frente a los videos deepfake; así pues, en los Estados de Texas y California, entraron en vigencia la Ley SB 751 y la Ley AB-730, respectivamente, con las cual se buscaba evitar una contienda política maliciosa.

Y en China entró en vigencia el "Reglamento sobre la administración de servicios de información de audio y vídeo en línea", con el que se pretendió salvaguardar la seguridad nacional y los intereses públicos.

En suma, estas medidas, buscan hacer frente a la lucha contra la cibercriminalidad, mediante la prohibición de creación y difusión de videos deepfake tendientes a desinformar, o en su defecto optar por el retiro de videos ya difundidos.

Medidas que podrían ser adoptadas por el Perú, en el delito de suplantación de identidad y subsumirse dentro de ese tipo base de La Ley 30096, dado que conforme

se desprende de la tabla y figura 12 y 15, el 87.3% considera que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad no son eficientes en el ejercicio de sus funciones y ello debido a lo establecido en la tabla y figura 14, que demuestra que estas fiscalías especializadas no poseen herramientas digitales pertinentes para la detección de videos deepfake, mismas que en palabras del Dr. Elías (2021), tendría que ser un software, lícito y con licencia, por lo que, resulta dificultoso el despliegue de medidas tendientes a identificar este tipo de videos, máxime si conforme refiere Marcos, Sanchez y Olivera (2017), esta nueva tecnología crea mundos paralelos (...) que los ciudadanos están dispuestos a validar.

Sin embargo, un aspecto limitante, que se pudo identificar en el desarrollo de esta investigación, fue que se desconoce si a la actualidad la fiscalía especializada de delitos informáticos en materia de cibercriminalidad, posee dicha tecnología, dado que, al tratarse de una fiscalía especializada, no se cuenta con el acceso a dicha información, aspecto que nuestro entrevistado comentaba, pese a que él conoce muy de cerca dicha fiscalía por fines investigativos.

Aunado a ello, existen series deficiencias tanto a nivel interno dentro del ámbito institucional y a nivel legislativo, dado que, tomando en cuenta que el Derecho es cambiante, debe adoptarse esta nueva modalidad dentro de la Ley de delitos informáticos, misma que debe complementarse con la capacitación a los operadores de justicia en materia informática, pues se ha evidenciado en la tabla y figura 13, que de acuerdo a nuestros encuestados, el 98.2% de los operadores de justicia no se encuentran debidamente capacitados en materia informática, aspecto que incluso fue precisado por el Dr. Elías, por lo que urge realizar cambios trascendentales tendientes a capacitar masivamente a los operadores judiciales, a fin de que conozcan el despliegue tecnológico de esta nueva modalidad y las implicancias negativas que genera.

Que en palabras del Dr. Elías (2021), esta capacitación debe estar dirigida a fortalecer las competencias especializadas que requiere un investigador tanto de la policía como de la fiscalía, así como la comprensión del contexto y de la importancia del Poder Judicial.

Con lo que se demuestra, lo arribado en la tabla y figura 15, en relación a que un 98.2%, considera que deben incorporarse las consecuencias nocivas del deepfake como circunstancias agravantes del delito de suplantación de identidad.

Pues si bien, conforme lo mencionaba el Dr. Ricardo Elías Puelles- Presidente del Observatorio de Cibercriminalidad, la tecnología no es de por sí ni buena ni mala, es el uso que se le está dando, motivo por el que sugiere que necesitamos una regulación para por lo menos pautear lo que se puede y qué es lo que no se debe hacer con esta tecnología, no limitarlas, pero sí regularlas.

En efecto, la autora, comparte la misma posición, dado que el deepfake no es negativo en sí, lo negativo es el uso no apropiado que se le da y las consecuencias negativas que esta genera, dado que para que determinar cuándo un deepfake debe ser sancionado, se debe tomar en cuenta, los siguientes aspectos i) si las personas que aparecen en un deepfake objetarían la forma en que están representadas; (ii) si el deepfake engaña a los espectadores; y (iii) la intención con la que se creó el deepfake.

El primero, en relación a que la persona que aparece en un deepfake, debe verse afectada por la creación del video, y la representación digital de sí mismo en una situación bochornosa, exponiéndolas en formas en que no desean ser retratados.

El segundo, en referencia al contenido deepfake, mismo que debe ser realista y adoptado como auténtico por la simple percepción de los demás, poniendo en duda la confiabilidad visual.

Y el tercero, dirigido al propósito de su creación, que se evidencia a través del impacto que el video deepfake genera.

En esa línea, es necesario empezar a regular esta nueva modalidad de suplantación de identidad en La Ley N° 30096, máxime si esta tecnología ya está siendo utilizada en el país y su creación pueda estar encaminada a generar algún perjuicio, aspecto que el legislador aún no ha previsto, pero que es imperioso, empezar a adoptar medidas legislativas al respecto.



## **VI. CONCLUSIONES**

1. Los constantes avances tecnológicos, están generando la aparición de nuevas modalidades de suplantación de identidad, tal es el caso de los deepfake, los cuales ya se encuentran en el Perú y que han sido utilizados con fines de concientización; sin embargo, ante la llegada de esta tecnología en nuestro país, se deja abierta la posibilidad de cometer actos delictivos, situación que el legislador no ha previsto y puede generar que la Ley de delitos informáticos devenga en ineficaz.
2. 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.
3. El deepfake a nivel internacional ha sido regulado jurídicamente en los países de Estados Unidos y China, adoptándose las medidas pertinentes para hacer frente a este tipo de videos, mediante la prohibición de creación y difusión de deepfakes, el retiro de este tipo de contenidos dentro del tráfico cibernético para evitar la desinformación o en su defecto permitir la creación de videos deepfake que contengan la consignación taxativa de que se trata de un contenido creado y no verídico que pueda inducir a la población a asumirlo como real.
4. Es menester, incorporar las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad, a fin de regular el uso de esta nueva tecnología que deriva en la generación de impactos negativos que pongan en peligro a la sociedad.

## **VII. RECOMENDACIONES**

- Se recomienda al legislador incorporar las consecuencias del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096, con el propósito de evitar la impunidad ante la comisión de esta nueva modalidad de suplantación de identidad.
- Se recomienda capacitar a los operadores de justicia en materia informática, en específico respecto a la tecnología deepfake que ya se encuentra en nuestro país, pero que se desconoce respecto a las consecuencias nocivas que este tipo de tecnología digital pueden representar.
- Se recomienda a la Fiscalía Especializada de delitos informáticos, implementar las herramientas digitales pertinentes para la detección de videos deepfake, puesto que, al tratarse de videos hiperrealistas, resulta dificultoso la diferenciación entre un video deepfake y un video de contenido verídico.
- Se recomienda al Poder Judicial, Ministerio Público y Policía Nacional del Perú, promover la investigación en materia de cibercriminalidad, a fin de poner en evidencia los múltiples vacíos legales existentes en la Ley de Delitos Informáticos que dificultan su correcta aplicación.

## VIII. PROPUESTA

### PROYECTO DE LEY N° 001/2020

La alumna RIMAICUNA TORRES MARELI FIORELLA, de la Universidad Cesar Vallejo, ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107° último párrafo de la Constitución Política del Perú a todo ciudadano, plantea la siguiente propuesta legislativa.

#### FÓRMULA LEGAL

### PROYECTO DE LEY QUE PROPONE LA INCORPORACIÓN DE CIRCUNSTANCIAS AGRAVANTES EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD EN LA LEY N° 30096.

#### **Artículo 1.- Objeto de Ley**

La presente propuesta legislativa tiene por objeto la incorporación de circunstancias agravantes en el delito de suplantación de identidad en la Ley N° 30096, con la finalidad de evitar que las consecuencias nocivas del deepfake incurran en impunidad.

**Artículo 2.-** Incorpórese los numerales 1,2 y 3, en los siguientes términos:

#### **Artículo 9. Suplantación de identidad**

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

***La pena será no menor de cinco ni mayor de siete años, si la suplantación es cometida para:***

- 1. Fomentar o ejercer violencia material o psicológica sobre una persona.***
- 2. Coadyuvar a la desinformación.***
- 3. Crear manipulación.***

## **I. EXPOSICIÓN DE MOTIVOS**

El derecho a la identidad se establece como un derecho de rango fundamental que le atañe a toda persona desde que nace (Sandoval, 2020) y que es entendido como el conjunto de atributos y características que permiten individualizar a la persona en la sociedad (Álvarez, 2016).

Situación similar, sucede con la identidad digital, que se constituye en una vertiente de la identidad personal, entendida como el conjunto de rasgos y características particulares que una persona expresa a través de internet (Borghello y Temperini, 2017).

Dentro del tráfico cibernético, han ido apareciendo con el transcurrir de los años, nuevas modalidades para delinquir valiéndose de medios informáticos; tal es el caso, del uso de tecnología deepfake, donde mediante la aplicación de inteligencia artificial, se puede imitar las expresiones faciales y voz de una determinada persona, suplantando su identidad.

Este apoderamiento de la identidad de una persona, se realiza mediante acciones ejecutadas por el sujeto activo quien mediante el uso de las tecnologías de la información, se hace pasar por la víctima a través de vía informática, con el propósito de generar un perjuicio material y moral.

El uso de esta tecnología, no resulta ser ajeno a nuestra realidad, pues en el año 2020, ingresó a nuestro país mediante el programa Perú Te Quiero, donde personajes como Miguel Grau, Chabuca Granda y Daniel Peredo, brindan un mensaje de conciencia en épocas de pandemia.

Sin embargo, deja abierta la posibilidad, para que personas inescrupulosas valiéndose del uso de esta tecnología, lo utilicen para perpetrar hechos ilícitos y generar un perjuicio que afecta a la sociedad.

Estando, a los argumentos antes esbozados, resulta necesario que el Estado implemente ciertas medidas legislativas destinadas a regular dicha tecnología y así evitar que sus consecuencias nocivas se difundan valiéndose de las redes sociales.

## **II. ANÁLISIS COSTO BENEFICIO:**

La aplicación de la presente norma no genera gasto alguno para el erario nacional. Por el contrario, tiene un efecto positivo para el país, ya que pretende evitar que personas inescrupulosas valiéndose de dicha omisión normativa, pretenda perpetrar actos ilícitos e incurrir en impunidad.

## REFERENCIAS

### TESIS:

1. Carranza, R. (2019). *Incorporación del delito de acoso sobre la base del principio de subsidiariedad*. (Tesis de pregrado). Universidad Nacional de Cajamarca, Cajamarca, Perú.  
<https://repositorio.unc.edu.pe/bitstream/handle/UNC/3814/EL%20DELITO%20DE%20ACOSO%20EN%20EL%20PER%20C3%9A-%20FINAL.pdf?sequence=5&isAllowed=y>
2. Carrillo, C. & Montenegro, A. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos*. (Tesis de Pregrado). Universidad Señor de Sipán, Pimentel, Lambayeque, Perú. <https://core.ac.uk/download/pdf/270318294.pdf>
3. Caycho, J. y Saguma, D. (2021). *“Medidas de protección informática y su eficacia en la prevención del delito de suplantación de identidad cibernética en la ciudad de Trujillo, 2020”*. (Tesis de Pregrado). Universidad privada de Trujillo, Trujillo, Perú. <http://repositorio.uprit.edu.pe/bitstream/handle/UPRIT/421/TESIS-%20CAYCHO%20PINCHI%20-%20SAGUMA%20RIVERA.pdf?sequence=1&isAllowed=y>
4. Hernández, D. (2019). *La Suplantación de Identidad Cibernética en el Ecuador*. (Tesis de Maestría). Universidad Externado de Colombia, Bogotá, Colombia. [https://bdigital.uexternado.edu.co/bitstream/001/1822/1/GAAA-spa-2019-La\\_suplantacion\\_de\\_identidad\\_cibernetica\\_en\\_el\\_Ecuador](https://bdigital.uexternado.edu.co/bitstream/001/1822/1/GAAA-spa-2019-La_suplantacion_de_identidad_cibernetica_en_el_Ecuador)
5. Montaperto, J. (2018). *Suplantación de identidad: un análisis sobre su falta de regulación en el ordenamiento jurídico argentino*. (Trabajo final de graduación). Universidad del siglo 21, Córdoba, Argentina. <https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/15652/MONTAPERTO,%20Javier%20Eduardo.pdf?sequence=1>
6. Romero, M. (2017). *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016*. (Tesis de Pregrado). Universidad de Huánuco, Huánuco, Perú.

[http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T\\_047\\_%2025858529\\_T.pdf?sequence=1&isAllowed=y](http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T_047_%2025858529_T.pdf?sequence=1&isAllowed=y)

7. Ruiz, C. (2016). *“Análisis De Los Delitos Informáticos Y Su Violación De Los Derechos Constitucionales De Los Ciudadanos”*. (Tesis de Pregrado). Universidad Nacional de Loja, Loja, Ecuador. <https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf>
8. Sandoval, E. (2020). *El Delito de Difamación en la Modalidad de Suplantación de Identidad a Través de la Red Social Facebook*. (Tesis de pregrado), Chiclayo, Lambayeque, Perú. [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46279/Sandoval\\_VEE-SD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46279/Sandoval_VEE-SD.pdf?sequence=1&isAllowed=y)
9. Vidal, E. (2017). *La falta de regulación frente a la suplantación y usurpación de identidad en Internet*. (Trabajo de fin de grado). Universitat de les Illes Balears, Palma, Illes Balears, España. [https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal\\_Torres\\_Elionor.pdf?sequence=1&isAllowed=y](https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal_Torres_Elionor.pdf?sequence=1&isAllowed=y)
10. Zea, A. (2016). *Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala*. (Tesis de Pregrado). Universidad Rafael Landívar, Guatemala. <http://recursosbiblio.url.edu.gt/tesiseortiz/2016/07/03/Zea-Arely.pdf>
11. Zorrilla, K. (2018). *Inconsistencias y Ambigüedades en la Ley de Delitos Informáticos Ley N° 30096 y su Modificatoria Ley N° 30171, Que Imposibilitan Su Eficaz Cumplimiento*. (Tesis de Pregrado). Universidad Nacional de Ancash Santiago Antunez de Mayolo, Huaraz, Ancash, Perú. [http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033\\_70221905\\_T.pdf?sequence=1&isAllowed=y](http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowed=y)

## **LIBROS:**

1. Acurio, S. (2016). *Delitos informáticos: generalidades*. [https://www.oas.org/juridico/spanish/cyb\\_ecu\\_delitos\\_inform.pdf](https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf)

2. Álvarez, R. (2016). Derecho a la identidad. *Temas selectos de vulnerabilidad y violencia contra niños, niñas y adolescentes*. (pp.3). México: Instituto de Investigaciones Jurídicas - UNAM  
<https://archivos.juridicas.unam.mx/www/bjv/libros/9/4242/8.pdf>
3. Borghello, C. y Temperini, M. (2017). Suplantación de Identidad Digital como delito informático. *Cibercrimen: aspectos de Derecho penal y procesal penal*. (párr. 1). Argentina: B de F. <https://ri.conicet.gov.ar/handle/11336/110190>

### **PERIÓDICO:**

1. BBC Mundo. (2018). La preocupación que despierta la tecnología que permite poner el rostro de cualquiera en los cuerpos de actores porno. *BBC New Mundo*.  
<https://www.bbc.com/mundo/noticias-42912261>
2. He, L., Guy, J. y Wang, S. (2019). Zao, la app china de rostros 'deepfake' que te permite ser una celebridad. *Expansion*.  
<https://expansion.mx/tecnologia/2019/09/07/zao-la-app-china-de-rostros-deepfake-que-te-permite-ser-una-celebridad>
3. Morales, C. (2021). Pennsylvania Woman Accused of Using Deepfake Technology to Harass Cheerleaders. *The New York Times*.  
<https://www.nytimes.com/2021/03/14/us/raffaella-spone-victory-vipers-deepfake.html>
4. O'Sullivan, D. y Dale, D. (2020). Four fake videos from Republicans draw tardy or no response from Facebook, Twitter. *The Mercury News*.  
<https://www.mercurynews.com/2020/09/01/four-fake-videos-from-republicans-draw-tardy-or-no-response-from-facebook-twitter/>
5. TvPerú. (2020). Perú te quiero, una campaña para cuidarnos en tiempos de pandemia. *TVpe*. <https://www.tvperu.gob.pe/videos/francamente/peru-te-quiero-una-campana-para-cuidarnos-en-tiempos-de-pandemia>

### **ARTÍCULOS CIENTÍFICOS:**

1. Cerdán, García y Padilla. (2020). Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales. *Revista Universidad Complutense de Madrid*,



25. <https://revistas.ucm.es/index.php/CIYC/article/download/68762/45644565539>  
36/.
2. Cerdán, V. y Padilla, G. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. *Revista Universidad Complutense de Madrid*, 24(02), 8. <https://revistas.ucm.es/index.php/HICS/article/view/66293/4564456552459>
  3. Ferreira, G. (2018). Social media, disinformation, and regulation of the electoral process: a study based on 2018 Brazilian election experience. *Revista Scielo*, 7(02),3. doi: 10.5380/rinc.v7i2.71057
  4. Figueira, A. y Oliveira, L. (2017). The current state of fake news: challenges and opportunities. *Procedia Computer Science*, 121. doi: 10.1016/j.procs.2017.11.106
  5. Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance. *Theatre Journal*, 70(4), 455–471. doi: 10.1353/tj.2018.0097
  6. Levitskaya, A. y Fedorov, A. (2020). Typology and Mechanisms of Media Manipulation. *International Journal of Media and Information Literacy*, 5(1),4. <https://cyberleninka.ru/article/n/typology-and-mechanisms-of-media-manipulation>
  7. Lin, H. (2019). The existential threat from cyber-enabled information warfare. *Bulletin of the Atomic Scientists*, 74(4), 16. doi: 10.1080/00963402.2019.1629574
  8. Maras, M. y Alexandrou, A. (2018). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, *Sage Journals*, 23(3), 1. doi: 10.1177/1365712718807226
  9. Marcos, J. Sanchez, J. y Olivera, M. (2017). La enorme mentira y la gran verdad de la información en tiempos de la postverdad, *Revista Ibersid*, 23(2), 2. <https://www.iversid.eu/ojs/index.php/scire/article/view/4446/3896>
  10. Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, 3(1), 1-2. doi: 10.1080/23738871.2018.1462395

11. Peñailillo, D. (2018). Sobre el lucro cesante. *Revista de derecho Concepción*, 86(243), párr.12. doi: 10.4067/S0718-591X2018000100007
12. Ripoll, L. y Matos, J. (2020). Information reliability: criteria to identify misinformation in the digital environment. *Revista Investigación Bibliotecológica: archivonomía, bibliotecología e información*, 34(84),9 .doi: 10.22201/iibi.24488321xe.2020.84.58115
13. Risso, M. (2019). Derecho a la propia imagen y expectativa de respeto a la privacidad. *Revista estudios constitucionales*, 17(1), párr. 34. doi: 10.4067/S0718-52002019000100119
14. Robles, M., Tinoco, H. y Fachetti, G. (2020). Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. *Revista Derecho Y Cambio Social*, (61) 464. <https://lnx.derechoycambiosocial.com/ojs-3.1.1-4/index.php/derechoycambiosocial/article/view/400>
15. Vega, Y. (2020). Nuevamente sobre el daño a la persona y el daño moral. *Revista Gaceta Civil y Procesal*, 80(1), p.8. <https://www.munizlaw.com/e-mailing/Publicaciones/Nuevamente%20sobre%20el%20dan%CC%83o%20a%20la%20persona%20y%20el%20dan%CC%83o%20moral.odf.pdf>
16. Villanueva, A. (2019). El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión y de información en el ordenamiento jurídico español. *Revista Dikaion*, 25(2), párr.18 .doi: 10.5294/DIKA.2016.25.2.3.
17. Westerlund. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11),1. <https://timreview.ca/article/1282>
18. Wilner, A. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal: Canada's Journal of Global Policy Analysis*, 73(2), 1. doi: 10.1177/0020702018782496

## **JURISPRUDENCIA:**

1. 《网络音视频信息服务管理规定》。现印发给你们，请认真遵照执行。， China, 29 de noviembre de 2019.
2. AB-1280 Crimes: deceptive recordings. California Legislative Information, California, 22 de abril del 2019.
3. AB-730 Elections: deceptive audio or visual media. California Legislative Information, California, 10 de abril del 2019.
4. CAS. N° 1594-2014 – LAMBAYEQUE. Diario Oficial El Peruano, Lima, 15 de octubre de 2014.
5. Convenio sobre la Ciberdelincuencia. Diario Oficial El Peruano, Lima, 22 de setiembre del 2019.
6. TX SB751: Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election. Legiscan, Texas, aprobado el 14 de junio del 2019.

## ANEXOS

### Anexo 01: Operacionalización de las Variables

*Operacionalización de la variable: deepfake*

Variable Independiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Deepfake	Videos hiperrealistas que aplican inteligencia artificial (IA) para representar a alguien que dice y hace cosas que	Saberes de los operadores jurisdiccionales respecto a las consecuencias nocivas del deepfake. Se medirá con un cuestionario a	Política criminal	Suscripción del Convenio de Budapest	Nominal
				Promulgación de la Ley N° 30096	
				Creación de la Fiscalía Especializada de Delitos Informáticos	
			Afectación a la imagen.		
				Afectación al honor.	

	nunca sucedieron.  (Li,2019).	partir del análisis de los conocimientos de los operadores jurisdiccionales sobre las consecuencias nocivas del deepfake.	Consecuencias del Deepfake	Fomenta o ejerce violencia material o psicológica sobre una persona.	
				Coadyuva a la desinformación.	
				Crea manipulación.	
		Deficiencias en relación a la regulación del deepfake	Conocimiento de las consecuencias del deepfake.		
			Capacitación a los operadores de justicia en materia informática.		
			Herramientas digitales pertinentes		

				para la detección de videos deepfake.	
--	--	--	--	---------------------------------------	--

*Operacionalización de la variable: delito de suplantación de identidad*

<b>Variable Dependiente</b>	<b>Definición conceptual</b>	<b>Definición operacional</b>	<b>Dimensiones</b>	<b>Indicadores</b>	<b>Escala de medición</b>
Delito de suplantación de identidad	Consiste en un ataque informático, de ingeniería social que tiene por finalidad la adquisición de información	Saberes de los operadores jurisdiccionales respecto a la aparición de nuevas modalidades de suplantación de	Política criminal	Suscripción del Convenio de Budapest	Nominal
				Promulgación de la Ley N° 30096	
				Creación de la Fiscalía Especializada de Delitos Informáticos	
			Perjuicio material		
				Perjuicio moral	

	<p>confidencial de la víctima (...) pudiendo provocar perjuicios patrimoniales, (...) y extrapatrimonial, (...). (Montaperto, 2018).</p>	<p>identidad. Se medirá con un cuestionario a partir del análisis de los conocimientos de los operadores jurisdiccionales sobre suplantación de identidad.</p>	<p>Consecuencias</p>		
--	--	--	----------------------	--	--

## Anexo N° 2 Instrumento de recolección de datos



UNIVERSIDAD CÉSAR VALLEJO

### Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096

#### CUESTIONARIO

**INSTRUCCIONES:** El presente instrumento de recolección de datos, permitirá obtener la información correspondiente que será contrastada con los objetivos de investigación planteados, a razón de ello seleccione la opción que considere pertinente.

**Condición:**

Jue

Abogado

Fiscal

**O.G: Analizar las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096.**

1. ¿Cree usted, que la suscripción del convenio de Budapest, ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información?

SI

NO

2. ¿Considera usted, que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos?

SI

NO

**O.E1: Identificar las consecuencias nocivas del deepfake que atentan contra la identidad de los cibernautas.**



3. ¿Considera usted, que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen?

SI

NO

4. ¿Considera usted, que colocar a una persona en situaciones bochornosas afecta su honor?

SI

NO

5. El uso de tecnología deepfake, permite que mediante fotos y audios de una persona, se pueda manipular su rostro y voz. En relación a lo anterior, ¿cree usted, que a través de esta tecnología se puede fomentar o ejercer violencia material o psicológica sobre una persona?

SI

NO

6. ¿Considera usted, que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación?

SI

NO

7. En su opinión, ¿un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación?

SI

NO

**O.E2: Contrastar las regulaciones jurídicas del deepfake a nivel internacional.**

8. En países como EE.UU y China, se han empezado a adoptar ciertas medidas legislativas para regular el uso de tecnología deepfake. ¿Considera usted, que nuestro país debe empezar a legislar al respecto?

SI

NO

9. En EE.UU., existió una proliferación de videos deepfake en contiendas políticas, así como de los llamados pornovenganzas, colocando a las personas situaciones bochornosas, haciendo y diciendo algo que no sucedió. En ese

sentido, ¿considera usted que los videos deepfakes suplantan la identidad de una persona?

SI

NO

10. En China, se ha legislado la prohibición de videos deepfake que son utilizados para crear, publicar y difundir noticias falsas. En su opinión, ¿este tipo de videos deberían prohibirse en nuestro país por generar desinformación?

SI

NO

**O.E3: Proponer la incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley**

11. ¿Considera usted, que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones?

SI

NO

12. En su opinión, ¿los operadores de justicia se encuentran debidamente capacitados en materia informática?

SI

NO

13. ¿Considera usted, que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes para la detección de videos deepfake?

SI

NO

14. El uso de tecnología deepfake, genera como consecuencias nocivas, la afectación al derecho al honor, a la imagen, fomenta o ejerce violencia física o material sobre una persona, crea manipulación y coadyuva a la desinformación. En ese sentido, ¿considera usted que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad?

SI

NO



**UNIVERSIDAD CÉSAR VALLEJO**

**Incorporación de las consecuencias nocivas del deepfake como agravantes  
del delito de suplantación de identidad en la Ley N° 30096**

**GUIÓN DE ENTREVISTA**

1. ¿Qué opinión le merece la aparición del uso de tecnología deepfake en nuestro país?
2. ¿Qué derechos podrían verse afectados con el uso de tecnología deepfakes?
3. ¿Con qué herramientas digitales deberían contar las fiscalías especializadas de cibercriminalidad, para identificar un video deepfake?
4. ¿Qué medidas debería adoptar el estado Peruano, para hacer frente a esta grave amenaza tecnológica surgida por la creación y difusión de videos deepfake?

## Anexo N° 3 Validez del Instrumento de recolección de datos



UNIVERSIDAD CÉSAR VALLEJO

### Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096

#### CUESTIONARIO

**INSTRUCCIONES:** El presente instrumento de recolección de datos, permitirá obtener la información correspondiente que será contrastada con los objetivos de investigación planteados, a razón de ello seleccione la opción que considere pertinente.

**Condición:**

Juez  Abogado  Fiscal

**O.G: Analizar las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096.**

1. ¿Cree usted, que la suscripción del convenio de Budapest, ha garantizado la efectiva protección de las grandes amenazas surgidas de las tecnologías de la información?

SI  NO

2. ¿Considera usted, que existen vacíos legales en la Ley N° 30096-Ley de delitos informáticos?

SI  NO

**O.E1: Identificar las consecuencias nocivas del deepfake que atentan contra la identidad de los cibernautas.**

3. ¿Considera usted, que utilizar fotos y audios de una persona sin su consentimiento, genera una afectación a su imagen?

SI  NO

4. ¿Considera usted, que colocar a una persona en situaciones bochornosas afecta su honor?

SI  NO

  
Hector L. Fernández De La Torre  
ABOGADO  
J.C.N. 5405

5. El uso de tecnología deepfake, permite que mediante fotos y audios de una persona, se pueda manipular su rostro y voz. En relación a lo anterior, ¿cree usted, que a través de esta tecnología se puede fomentar o ejercer violencia material o psicológica sobre una persona?

SI

NO

6. ¿Considera usted, que la difusión de contenido engañoso en redes sociales coadyuva a la desinformación?

SI

NO

7. En su opinión, ¿un video deepfake que presenta a una autoridad dando órdenes frente a un posible ataque terrorista puede crear manipulación?

SI

NO

**O.E2: Contrastar las regulaciones jurídicas del deepfake a nivel internacional.**

8. En países como EE.UU y China, se han empezado a adoptar ciertas medidas legislativas para regular el uso de tecnología deepfake. ¿Considera usted, que nuestro país debe empezar a legislar al respecto?

SI

NO

9. En EE.UU., existió una proliferación de videos deepfake en contiendas políticas, así como de los llamados pornovenganzas, colocando a las personas situaciones bochornosas, haciendo y diciendo algo que no sucedió. En ese sentido, ¿considera usted que los videos deepfakes suplantan la identidad de una persona?

SI

NO

10. En China, se ha legislado la prohibición de videos deepfake que son utilizados para crear, publicar y difundir noticias falsas. En su opinión, ¿este tipo de videos deberían prohibirse en nuestro país por generar desinformación?

SI

NO

**O.E3: Proponer la incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096.**

11. ¿Considera usted, que los operadores de las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones?

SI

NO

12. En su opinión, ¿los operadores de justicia se encuentran debidamente capacitados en materia informática?

SI

NO

13. ¿Considera usted, que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes para la detección de videos deepfake?

SI

NO

14. El uso de tecnología deepfake, genera como consecuencias nocivas, la afectación al derecho al honor, a la imagen, fomenta o ejerce violencia física o material sobre una persona, crea manipulación y coadyuva a la desinformación. En ese sentido, ¿considera usted que se deberían incorporar estas consecuencias nocivas como circunstancias agravantes del delito de suplantación de identidad?

SI

NO

  
Hector L. Fernandez De La Torre  
ABOGADO  
CAL 5405



**UNIVERSIDAD CÉSAR VALLEJO**

**Incorporación de las consecuencias nocivas del deepfake como  
agravantes del delito de suplantación de identidad en la Ley N° 30096**

**GUIÓN DE ENTREVISTA**

1. ¿Qué opinión le merece la aparición del uso de tecnología deepfake en nuestro país?
2. ¿Qué derechos podrían verse afectados con el uso de tecnología deepfakes?
3. ¿Con qué herramientas digitales deberían contar las fiscalías especializadas de cibercriminalidad, para identificar un video deepfake?
4. ¿Qué medidas debería adoptar el estado Peruano, para hacer frente a esta grave amenaza tecnológica surgida por la creación y difusión de videos deepfake?



Hector L. Fernández De La Torre  
ABOGADO  
C.N.L. 5405

## Anexo N° 4 Confiabilidad del Instrumento de recolección de datos

### CONSTANCIA DE FIABILIDAD DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

El presente documento es para constatar la fiabilidad del instrumento de recolección de datos del tema denominado: **“Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096”**

Se usó el método de KUDER RICHARDSON ( $KR_{20}$ ) por tener 14 ítems en escala dicotómica, la cual se verifica en la documentación adjunta en *Anexos*.

Para su interpretación del coeficiente  $KR_{20}$  se ha tomado la escala según **Ruiz (2020)**

De 0.01 a 0.20 **Muy baja**

De 0.21 a 0.40 **Baja**

De 0.41 a 0.60 **Moderada**

De 0.61 a 0.80 **Alta**


De 0.81 a 1.00 **Muy Alta**

Dando fe que se aplicaron las encuestas a la muestra objeto de estudio, se obtiene como resultado un **coeficiente de confiabilidad  $KR_{20}$  igual a 0.839**, lo cual significa según la escala de Ruiz (2020) un coeficiente **“MUY ALTO”** por lo que se concluye que el instrumento de recolección de datos presenta una muy alta confiabilidad de consistencia interna, siendo los resultados obtenidos en este cuestionario fieles a la realidad en favor de la investigación cumpliendo su propósito.

Por lo tanto

CERTIFICO: Que el instrumento es confiable en cuanto a su constancia interna.

Chiclayo, 12 de noviembre del 2021

GOBIERNO DE ESTADÍSTICAS DEL PERU  
  
Dr. Arana Cerna Branco Ernesto  
COESPE N° 238

Dr. Arana Cerna Branco Ernesto

DNI N° 16786967

COESPE N° 238

**confiabilidad**



## ANEXO

$$KR_{20} = \frac{K}{K-1} \left( 1 - \frac{\sum p * q}{S_t^2} \right)$$

**Donde:**

$KR_{20}$ : Coeficiente de confiabilidad Kuder Richardson 20

$\sum p * q$ : Sumatoria de los productos p y q

$S_t^2$ : Varianza de las puntuaciones totales

p : Total de respuestas afirmativas entre el número de entrevistados

q : 1 - p

K : El número de preguntas o ítems

Aplicando la formula Kuder Richardson 20

$$KR_{20} = \frac{14}{14-1} \left( 1 - \frac{0.6545}{2.9576} \right) = 0.839$$

**Tabla 1.** Indicador de confiabilidad con el COEFICIENTE KR20  
(14 ítems, aplicado a 55 profesionales del derecho)

<i>KUDER - RICAHRSON 20</i>	<i>Ítems</i>
<b>0.839</b>	<b>14</b>


Fuente: Cuestionario aplicado

**Tabla 2.** Base de datos del cuestionario aplicado a 55 profesionales del derecho, para el cálculo del coeficiente de **Kuder Richardson 20**

<b>Encuestado</b>	<b>P1</b>	<b>P2</b>	<b>P3</b>	<b>P4</b>	<b>P5</b>	<b>P6</b>	<b>P7</b>	<b>P8</b>	<b>P9</b>	<b>P10</b>	<b>P11</b>	<b>P12</b>	<b>P13</b>	<b>P14</b>
<b>1</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>2</b>	0	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>3</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>4</b>	0	0	0	0	0	0	0	0	0	0	0	1	1	0
<b>5</b>	1	0	0	0	0	0	0	0	0	0	1	1	0	0
<b>6</b>	0	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>7</b>	1	0	0	0	1	0	1	0	1	1	1	1	1	0
<b>8</b>	1	0	0	1	1	0	0	0	0	0	1	1	1	0
<b>9</b>	0	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>10</b>	1	0	0	0	0	0	0	0	0	0	1	1	0	0
<b>11</b>	0	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>12</b>	0	0	0	0	0	0	0	0	0	0	0	1	1	0
<b>13</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>14</b>	0	0	0	0	0	0	0	0	0	0	0	1	1	0
<b>15</b>	0	0	0	0	0	0	0	0	0	0	0	1	1	0
<b>16</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>17</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>18</b>	1	0	0	0	0	0	0	0	0	0	0	1	1	0
<b>19</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>20</b>	1	0	0	1	0	0	0	0	0	0	1	1	1	0
<b>21</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>22</b>	0	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>23</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>24</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>25</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>26</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>27</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0
<b>28</b>	1	0	0	0	0	0	0	0	0	0	1	1	1	0

29	1	0	0	0	0	0	0	0	0	0	1	1	1	0
30	1	0	0	0	0	0	0	0	0	0	1	1	1	0
31	0	0	0	0	0	0	0	0	0	0	0	1	1	0
32	1	0	0	0	0	0	0	0	0	0	1	1	1	0
33	1	0	0	0	0	0	0	0	0	0	1	1	1	0
34	1	0	0	0	0	0	0	0	0	0	1	1	1	0
35	1	0	0	0	0	0	0	0	0	0	1	1	1	0
36	1	0	0	0	0	0	0	0	0	0	1	1	1	0
37	1	0	0	0	0	0	0	0	0	0	1	1	1	0
38	1	0	0	0	0	0	0	0	0	0	1	1	1	0
39	1	0	0	0	0	0	0	0	0	0	1	1	1	0
40	1	0	0	0	0	0	0	0	0	0	1	1	1	0
41	1	0	0	0	0	0	0	0	0	1	1	1	1	0
42	1	0	0	0	0	0	0	0	0	0	1	1	1	0
43	1	0	0	0	0	0	0	0	0	0	1	1	1	0
44	1	0	0	0	0	0	0	0	0	0	1	1	1	0
45	1	0	0	0	0	0	0	0	0	0	1	1	1	0
46	1	0	0	0	0	0	0	0	0	0	1	1	1	0
47	1	0	0	0	0	0	0	0	0	0	1	1	1	0
48	0	0	0	0	0	0	0	0	0	0	1	1	1	0
49	1	0	0	0	0	0	0	0	0	0	1	1	1	0
50	1	0	0	0	0	0	0	0	0	0	1	1	1	0
51	1	0	0	0	0	0	0	0	0	0	1	1	1	0
52	1	0	0	0	0	0	0	0	0	0	1	1	1	0
53	1	0	0	0	0	0	0	0	0	0	1	1	1	0
54	1	0	0	0	0	0	0	0	0	0	0	0	0	0
55	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Fuente: Cuestionario aplicado

  
**COMANDO EN JEFE ESTADÍSTICOS DEL PERÚ**  
 Sr. Bruno Ernesto Armas García  
 GOESPE. N° 200

## Anexo N° 5 Reporte de originalidad

### TURNITIN- TESIS MARELI RIMAICUNA.pdf

#### INFORME DE ORIGINALIDAD

18%

INDICE DE SIMILITUD

17%

FUENTES DE INTERNET

1%

PUBLICACIONES

6%

TRABAJOS DEL ESTUDIANTE

#### FUENTES PRIMARIAS

1	<a href="http://repositorio.ucv.edu.pe">repositorio.ucv.edu.pe</a> Fuente de Internet	6%
2	<a href="http://repositorio.uprit.edu.pe">repositorio.uprit.edu.pe</a> Fuente de Internet	2%
3	<a href="http://core.ac.uk">core.ac.uk</a> Fuente de Internet	2%
4	<a href="http://repositorio.unasam.edu.pe">repositorio.unasam.edu.pe</a> Fuente de Internet	1%
5	<a href="http://recursosbiblio.url.edu.gt">recursosbiblio.url.edu.gt</a> Fuente de Internet	1%
6	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
7	<a href="http://repositorio.ulasamericas.edu.pe">repositorio.ulasamericas.edu.pe</a> Fuente de Internet	1%
8	<a href="http://link.springer.com">link.springer.com</a> Fuente de Internet	<1%
9	Submitted to Universidad de las Islas Baleares Trabajo del estudiante	<1%