



Universidad
Norbert Wiener

FACULTAD DE DERECHO Y CIENCIA POLÍTICA
PROGRAMA ACADÉMICO DE DERECHO Y CIENCIA
POLÍTICA

Tesis

La persecución del delito de Suplantación de Identidad mediante inteligencia artificial y la inoperancia de la Ley 32314, Lima 2025

Para optar el Título Profesional de
Abogada

Presentado por:

Autora: Díaz Aldaz, Jesús María

Código ORCID: <https://orcid.org/0000-0002-3750-542X>

Asesor: Mg. Meza Huamaní, Jhover Waldo

Código ORCID: <https://orcid.org/0000-0002-4843-0515>

Lima – Perú

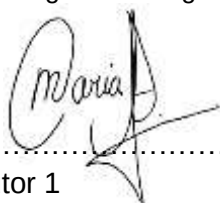
2026

	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo,.....**JESÚS MARÍA DÍAZ ALDAZ**..... egresada de la Facultad de **Derecho y Ciencia Política** y Escuela Académica Profesional de **Derecho y Ciencia Política** de la Universidad privada Norbert Wiener declaro que el trabajo de investigación **“La persecución del Delito de Suplantación de Identidad mediante Inteligencia Artificial y la inoperancia de la Ley 32314, Lima 2025”** Asesorado por el docente: **JHOVER WALDO MEZA HUAMANÍ**, DNI: **45137535**, con código ORCID: **0000-0002-4843-0515**, tiene un índice de similitud de **15 (quince) %** con código OID: **:::14912:592668800**, verificable en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.

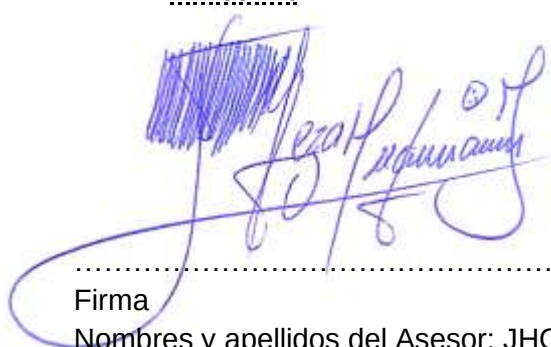


.....
Firma de autor 1

Nombres y apellidos del Egresado:

JESÚS MARÍA DÍAZ ALDAZ

DNI: **...72169470**.....



.....
Firma

Nombres y apellidos del Asesor: **JHOVER WALDO MEZA HUAMANÍ**

DNI: **...45137535**...

Lima, **...15...** de **...mayo...** de **...2026...**

DEDICATORIA

A mis padres, María Magdalena y Nery, que, su apoyo a sido muy fundamental para convertirme en la mujer que hoy en día soy. Gracias por su cariño, sus consejos llenos de sabiduría y la confianza de creer en mí incluso cuando yo dudaba. Este logro no solo es mío, sino que también es suyo.

AGRADECIMIENTO

A Dios, por brindarme la fortaleza y permitirme llegar hasta este momento.

A mis abuelos, que, aunque ya no están presentes, su amor y consejos siempre están presentes en mí.

A la Universidad Norbert Wiener, por abrirme las puertas de su casa de estudios en donde se me inculco la pasión por la investigación y/o permitió que creciera mi amor por el Derecho. Y a cada uno de los docentes, que compartieron sus conocimientos y experiencias, demostrándome así que el derecho puede ser tan apasionante.

A mis amistades que eh conocido a lo largo de esta hermosa carrera, quienes me enseñaron que a veces es necesario tomar riesgos para salir de mi zona de confort. Y que cada cosa llega en su respectivo tiempo.

A mi asesor, Jover Waldo Meza Mamami, por su paciencia, orientación y buenos consejos lo cual fue fundamental para el desarrollo y culminación de esta tesis.

Finalmente, a mi familia que confió en mi en este proceso.

Índice

DEDICATORIA	ii
AGRADECIMIENTO.....	iii
Resumen.....	vii
Abstract	viii
I. INTRODUCCIÓN	9
1.1 Contextualización del problema.....	11
1.2 Planteamiento del problema.....	15
1.3. Formulación del problema	19
1.3.1 Problema general.....	19
1.3.2 Problemas específicos	19
1.3.3. Objetivo general	20
1.3.4. Objetivos específicos.....	20
1.4 Justificación de la investigación.....	20
1.4.1 Justificación Teórica	21
1.4.2 Justificación Social.....	22
1.4.3 Justificación Metodológica	22
1.5 Antecedentes de la Investigación	23
1.6. Estado de la cuestión.....	28
II. METODOLOGÍA.....	41
2.1 Enfoque de la investigación	41
2.1.1. Tipo de estudio.....	41
2.1.2 Diseño de la investigación.....	42
2.1.3. Población y muestra	42
2.1.4 Técnicas de reproducción de datos.....	43
2.1.5 Procedimientos.....	43
2.1.6. Aspectos éticos.....	43
III. RESULTADOS.....	45
Tabla 1. Respuesta de entrevistados - Objetivo General.....	47

Tabla 2. Respuesta de entrevistados - Objetivo Específico 1.....	50
Tabla 3. Respuesta de entrevistados - Objetivo Específico 2.....	53
Tabla 4. Respuesta de entrevistados - Objetivo Específico 3.....	56
3.1. Análisis de resultados de entrevista	60
Tabla de análisis de los resultados relacionados al Objetivo General.....	60
Tabla de análisis de los resultados relacionados al Objetivo Específico 1.....	61
Tabla de análisis de los resultados relacionados al Objetivo Específico 2.....	62
Tabla de análisis de los resultados relacionados al Objetivo Específico 3.....	63
3.2. Análisis de resultados de jurisprudencias.....	64
Tabla. Análisis jurisprudencial internacional y nacional del objetivo general.....	64
Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 1	65
Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 2	66
Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 3	67
IV. DISCUSIÓN	68
4.1. Discusión del objetivo general	68
4.2. Discusión del objetivo específico 1	69
4.3. Discusión del objetivo específico 2.....	70
4.4. Discusión del objetivo específico 3.....	71
Figura 1. C1: Delito de Suplantación de Identidad y subcategorías / autores y discusión de los resultados	73
Figura 2. C2: Inteligencia Artificial y subcategorías / autores y discusión de los resultados.....	74
V. CONCLUSIONES Y RECOMENDACIONES	75
5.1. Conclusiones	75
5.2. Recomendaciones.....	77
5.3. Propuesta Normativa.....	79
REFERENCIAS	82
Anexo 1: Matriz de categorización apriorística	90
Anexo 2. Instrumento de recolección de datos	92
Anexo 3:Evaluación de Rigurosidad del Instrumento.....	146

Anexo 4: Consentimiento informado	148
Anexo 5: Carta de aprobación de la institución para investigación	168
Anexo 6: Aprobación del comité de ética	169
Anexo 7: Informe de turnitin.....	170

Resumen

Introducción: Hoy en día, con el avance de la tecnología ha generado un entorno idóneo para el desarrollo y adopción de herramientas digitales como la Inteligencia Artificial (IA), como es el caso de la suplantación de identidad mediante técnicas avanzadas como la clonación de voz, los *deepfakes* y la creación de identidades artificiales. Estas acciones afectan derechos esenciales como la autodeterminación informativa, la seguridad en el entorno digital y la identidad individual. **Objetivo:** Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima. **Metodología:** La presente investigación utiliza un enfoque cualitativo, de tipo documental y nivel descriptivo, adoptando un diseño no experimental. Para ello se recurre al análisis normativo, doctrinario y jurisprudencial, junto con una entrevista semiestructurada dirigidas a abogados penalistas, especialistas en la materia, el estudio se desarrolla bajo un método inductivo y analítico, respetando criterios éticos y de rigor metodológico. **Resultados:** Se demostró que la normativa revela una problemática que hoy en día los sistemas jurídicos de las nuevas modalidades en delitos informáticos. **Conclusión:** Se analizó de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través de inteligencia artificial en Lima. Lo relevante fue identificar el análisis de este delito. Lo difícil fue recopilar información especializada y jurisprudencias actuales, siendo necesario establecer un tipo penal específicos en los agravantes de la IA.

Palabras claves: Identidad, cibercrimen, delito informático, inteligencia artificial, anonimato y ciberespacio.

Abstract

Introduction: Today, technological advancements have created an ideal environment for the development and adoption of digital tools such as Artificial Intelligence (AI), as is the case with identity theft using advanced techniques like voice cloning, deepfakes, and the creation of artificial identities. These actions affect fundamental rights such as informational self-determination, security in the digital environment, and individual identity. **Objective:** To analyze how the ineffectiveness of Law No. 32314 manifests itself in the prosecution of identity theft through artificial intelligence in Lima. **Methodology:** This research uses a qualitative, documentary, and descriptive approach, adopting a non-experimental design. It employs normative, doctrinal, and jurisprudential analysis, along with semi-structured interviews with criminal lawyers specializing in the field. The study is developed using an inductive and analytical method, respecting ethical criteria and methodological rigor. **Results:** The study demonstrated that the regulations reveal a problem that current legal systems face regarding new forms of cybercrime. **Conclusion:** The study analyzed how the ineffectiveness of Law No. 32314 manifests itself in the prosecution of identity theft through artificial intelligence in Lima. The key finding was identifying and analyzing this crime. The challenge lay in compiling specialized information and current case law, making it necessary to establish a specific criminal offense for aggravated AI-related crimes.

Keywords: Identity, cybercrime, computer crime, artificial intelligence, anonymity, and cyberspace.

I. INTRODUCCIÓN

El avance tecnológico ha evidenciado cambios significativos en la manera en que las personas se comunican, interactúan y forman su identidad en un entorno digital. Actualmente, la integración progresiva de sistemas de inteligencia artificial ha transformado no solo los procesos de producción y gestión, sino también surge nuevas formas de criminalidad. Si bien este desarrollo aporta beneficios en diversas áreas, pero también crea riesgos relevantes, sobre todo en lo referente a la protección de la identidad personal y seguridad digital. En este contexto, la suplantación de identidad ha tomado un enfoque distinto a lo habitual, dado que trasciende el uso indebido de documentos o credenciales físicos, y se expresa mediante herramientas tecnológicas capaces de replicar características humanas con exactitud.

En relación con la realidad del Perú, el incremento de delitos cibernéticos evidencia que nuestro sistema penal presenta limitaciones para responder de manera eficaz a estas nuevas modalidades delictivas. Aunque el Estado ha promulgado la Ley N.º 32314, orientada a agravar determinadas conductas cuando interviene el uso de la inteligencia artificial, su aplicación en la práctica ha demostrado ser insuficiente frente a la complejidad técnica de los hechos investigados. La ley presenta vacíos en aspectos fundamentales como la recolección y evaluación de pruebas digitales, la asignación de responsabilidad penal en entornos de automatización algorítmica y la correcta

categorización de conductas mediadas tecnológicamente, lo que dificulta inicialmente en la investigación, incrementa el riesgo de impunidad dejando vulnerables a las víctimas.

Ante esta problemática, la presente investigación tiene como propósito analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima. Con el estudio se pretende identificar los principales obstáculos normativos y operativos que dificultan en una respuesta penal adecuada, así como también evaluar como estas limitaciones impactan en la protección de los derechos fundamentales comprometidos. En este sentido, el presente trabajo aporta al debate actual sobre el derecho penal tecnológico y la necesidad de modificar sus conceptos tradicionales para adaptarse a los retos que impone la criminalidad digital.

El Capítulo I desarrolla la contextualización y el planteamiento del problema, asimismo la formulación de preguntas de investigación, objetivos y justificación del estudio, además de presentar el marco teórico y jurídico que respalda el análisis. En esta sección se define el alcance conceptual del delito de suplantación de identidad y se destaca la relevancia de la inteligencia artificial como un factor que agrava la criminalidad en el entorno digital.

El Capítulo II aborda la metodología empleada, detallando el enfoque, tipo y diseño de la investigación, además de técnicas e instrumentos que se aplicaron en la recolección y análisis de datos. Así como también se especifica los procedimientos implementados y estándares éticos cumplidos a lo largo del estudio, asegurando la validez y consistencia del proceso investigativo.

En el Capítulo III se muestran los resultados obtenidos, basados en el análisis de entrevistas y revisión de la jurisprudencia seleccionada. En este capítulo se presenta los descubrimientos que ilustran las principales deficiencias de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad a través de inteligencia artificial.

En el Capítulo IV se presenta un análisis de hallazgos recolectados, y se realiza una evaluación crítica sobre la efectividad de la Ley N.º 32314, considerando su alcance y restricciones en relación a las necesidades del derecho penal digital y la garantía de derechos fundamentales.

Finalmente, en el Capítulo V: Conclusiones y Recomendaciones se resume las contribuciones clave del estudio realizado y presenta ideas destinadas a mejorar una respuesta adecuada. Las sugerencias se encuentran dirigidas tanto a las normas, como también a la acción de la fiscalía y los tribunales, con el objetivo de ayudar a establecer un sistema legal más adecuado y efectivo que se ajuste a los retos tecnológicos contemporáneos.

1.1 Contextualización del problema

En estos últimos diez años, con la transformación digital en el Perú ha transformado la manera en que las personas interactúan, realizan transacciones y controlan sus datos personales en entornos virtuales. Este avance tecnológico ha ampliado escenarios, en donde puede producirse la suplantación de identidad, no solo mediante redes sociales o plataformas financieras, sino por medio de herramientas de inteligencia artificial (IA), las cuales son capaces de replicar voces, gestos y patrones.

Ante el aumento de esta complejidad, el Estado promulgo la Ley N.º 32314 de fecha 29 de abril de 2025 publicada en el diario el “peruano”, con la finalidad de fortalecer la respuesta penal contra estas conductas. Sin embargo, su aplicación enfrenta desafíos debido a la velocidad con que se desarrolla la Inteligencia Artificial, en el futuro y las complicaciones para identificar a los responsables y obtener pruebas digitales válidas. En este contexto, es imprescindible analizar, cómo el sistema de justicia interpreta estos retos en Lima hacia el año 2025, en la persecución del delito.

En la metodología cualitativa, está permite situar el fenómeno dentro de un entorno social, institucional y normativo, lo cual resulta esencial para poder comprender las dinámicas que intervienen en la suplantación de identidad mediante IA. Considerando a Alvarado (2016) señala que contextualizar un problema implica describir las condiciones reales donde este se manifiesta, identificando actores, escenarios y vacíos de comprensión que fundamentan la pregunta de investigación. El avance tecnológico y la incorporación de la IA ha generado modalidades de suplantación de identidad complejas, comprometiendo derechos fundamentales como es la autodeterminación informativa, la privacidad y la seguridad digital.

Bajo esta circunstancia, la persecución del delito antes mencionado evidencia limitaciones normativas en la Ley N.º 32314, la cual no responde de manera eficaz e idónea a las necesidades de las dinámicas tecnológicas actuales. La ausencia de criterios técnicos claros sobre evidencia digital, autenticidad algorítmica y atribución de responsabilidad, dificulta la labor fiscal y judicial, revelando una brecha estructural entre el avance tecnológico y la capacidad regulatoria del derecho penal vigente.

La inoperancia de la Ley N.º 32314, evidencia una incapacidad para responder a las nuevas formas de suplantación de identidad generadas mediante inteligencia artificial delito no convencional. La norma no contempla supuestos tecnológicos complejos como identidades sintéticas, *deepfakes* o automatización algorítmica del fraude. Lo cual dificulta la actuación del Ministerio Público en la identificación del agente delictivo, la falta de criterios técnicos y jurídicos adecuados limita la eficacia de la persecución penal. En consecuencia, se debilita la protección penal de la identidad personal en entornos digitales en Lima.

En la norma no se establecen estándares probatorios para contenidos manipulados algorítmicamente, lo cual genera incertidumbre en la cadena de custodia y en la autenticidad de los medios probatorios digitales, sumado a ello la falta de regulación específica sobre la obtención, preservación y valoración de la evidencia digital vinculada con IA. Este vacío de criterios técnicos impide una correcta acreditación del hecho delictivo, lo cual debilita la persecución penal en la fase investigativa.

Con ello no garantiza una protección efectiva de la autodeterminación informativa frente al uso indebido de inteligencia artificial. Así como también, no integra de manera suficiente el enfoque de seguridad digital ni el control del uso ilícito de datos personales. Esta deficiencia limita la defensa jurídica de las víctimas cuya identidad es manipulada tecnológicamente. Además, no se establecen mecanismos claros de prevención ni de responsabilidad por el tratamiento automatizado de datos, ello afecta directamente la eficacia de la persecución penal del delito.

Esta situación incide negativamente en la seguridad jurídica y en la protección efectiva de las víctimas, al no garantizar una respuesta penal proporcional y coherente. Además, la debilidad normativa frente a la autodeterminación informativa limita la protección de los datos personales frente a usos ilícitos basados en IA. En consecuencia, la persecución penal se torna fragmentada e insuficiente.

Asimismo, la inoperancia de la Ley N.º 32314 se manifiesta en la falta de adecuación dogmática para una correcta tipificación penal de la suplantación de identidad cometida mediante inteligencia artificial. La norma presenta deficiencias para integrar elementos como la manipulación de datos biométricos, la generación de identidades sintéticas y el uso de sistemas automatizados, lo que afecta la subsunción típica del delito.

La inoperancia de la Ley N.º 32314 impacta negativamente en la correcta tipificación penal de la suplantación de identidad cometida mediante inteligencia artificial. La norma no incorpora elementos objetivos y subjetivos propios de la conducta digital automatizada. Esta omisión dificulta la subsunción típica y genera interpretaciones dispares en sede fiscal. Como resultado, se debilita el principio de legalidad penal. La falta de adecuación normativa impide una respuesta penal coherente y proporcional frente a estos delitos tecnológicos. Desde una perspectiva jurídico-investigativa, resulta necesario analizar críticamente esta inoperancia para proponer criterios normativos y técnicos que fortalezcan la eficacia del sistema penal frente a los nuevos desafíos digitales.

1.2 Planteamiento del problema

La evolución constante de la tecnología ha traído consigo el sistema de IA, el cual juega un papel muy importante en nuestra sociedad, debido a que su uso puede ser beneficioso como también puede conllevar un riesgo si se usa indebidamente. En el presente contexto, el uso indebido de la IA puede generar nuevas modalidades de suplantación de identidad, como los *deepfakes*, la clonación de voz y los modelos generativos permiten reproducir rasgos humanos con alta verosimilitud, lo que incrementa significativamente el riesgo de fraudes, extorsiones, manipulación de información y apropiación indebida de cuentas digitales y esto puede superar las capacidades tradicionales de detección y persecución penal.

Analizando la doctrina de marcos legales avanzados, considero que existen diversos desafíos como es la dificultad para atribuir responsabilidad penal, coordinar investigaciones transnacionales y recolectar evidencia digital confiable. Lo cual evidenciaría, que la respuesta normativa en materia penal aún no se adecúa plenamente al dinamismo tecnológico actual, generando espacios de impunidad.

En países como China y Japón, los autores Dubey y Choubey (2024) identifican que la suplantación de identidad digital ha experimentado un aumento notable debido al acceso masivo a bases de datos personales divulgados y al uso de herramientas automatizadas aptos para replicar información sensible. Los autores indican que millones de registros han sido expuestos brechas de seguridad, lo que permite a los ciberdelincuentes utilizar datos reales para obtener créditos, ejecutar fraudes bancarios y crear identidades falsas con un alto nivel de verosimilitud. Este fenómeno se agrava con

la incorporación de herramientas de IA, lo que facilita la imitación de comportamientos humanos y aumentan con éxito la tasa de las estafas.

En Estados Unidos, desde la perspectiva de Lin (2025) sostiene que la *Federal Bureau of Investigation* o Oficina Federal de Investigaciones (FBI), lidia con un incremento constante de delitos potenciados por inteligencia artificial, particularmente los que están relacionados con *deepfakes* y suplantaciones personalizadas dirigidas a víctimas específicas, aunque el país dispone de legislación avanzada en materia de delitos informáticos, esta no evoluciona con la misma rapidez que las tecnologías empleadas por los delincuentes, lo que genera vacíos operativos e insuficientes para analizar evidencia digital (FBI, 2025) (pag.251).

En Alemania, los autores Bharati et al. (2025) abordaron el problema debido a que muchos detectores ante la falta de fiabilidad y utilidad de la evidencia digital generada mediante nuevas tecnologías, en casos de suplantación de identidad por medio de un estudio de las dificultades en la regulación de la criminalidad informática que automatizan la ejecución del delito en la obtención de la prueba digital en la trazabilidad tecnológica por intermedio de la IA.

Dentro de contexto español, el investigador Galindo (2024) argumenta que existe un vacío normativo en el Código Penal debido que no se tipifica de manera autónoma la suplantación de identidad digital, sino únicamente sus consecuencias posteriores, como la estafa o los daños al honor, esta omisión permite que conductas como la creación de perfiles falsos, la apropiación indebida de identidades o el uso no autorizado de la imagen digital queden sin sanción.

En Colombia, el autor Briones et al. (2024) sostiene que en este país la IA ha facilitado la suplantación de identidad a través de técnicas que reproducen rostros, voces y patrones de comunicación con alto realismo, lo cual conlleva a un riesgo de fraudes electrónicos, extorsiones y vulneraciones a la intimidad. Además, su Sistema Penal aún no incorpora figuras específicas relacionadas con *deepfakes* o imitaciones digitales avanzadas.

Continuando, en el país de México, Trejo et al. (2025) estudia el fenómeno de la IA desde la perspectiva de derechos humanos, señalando así que este fenómeno incrementa la vulnerabilidad digital, especialmente en niños, adolescentes y otros grupos sensibles. respecto a la extracción masiva y el uso no autorizado de datos personales han derivado en prácticas de suplantación, difíciles de detectar, debido a que no se encuentra adaptado a desafíos de manipulación de contenido digital.

Respecto a Argentina, Díaz et al. (2023) destaca que la criminalidad informática, incluida la suplantación de identidad, se ha expandido significativamente debido a la proliferación de plataformas digitales y al uso de tecnologías automatizadas, manteniendo lagunas en la tipificación de conductas digitales y en la valoración probatoria de evidencia electrónica ante la limitada capacitación de fiscales y jueces para identificar patrones delictivos.

En Ecuador, bajo la óptica de Zavala (2025) considera que la apropiación fraudulenta por medios electrónicos y la suplantación de identidad constituye un componente esencial en la comisión de estafas bancarias y apropiaciones fraudulentas mediante medios electrónicos, técnicas como el *phishing*, la ingeniería social y la

falsificación digital de credenciales permiten a los delincuentes acceder a cuentas financieras con relativa facilidad ante las modalidades asociadas al uso de la IA.

En territorio peruano se observa, por un lado, en un estudio realizado por el (Observatorio Regional de Piura, 2025) señaló en su informe, que Piura registra una alta incidencia de ciberdelitos, ubicándose entre las zonas con más denuncias, especialmente por fraudes informáticos y suplantación de identidad mediante engaños digitales, tras la suplantación de un supuesto trabajador bancario, evidencian la vulnerabilidad de instituciones y ciudadanos frente a estos delitos (EBIZ NOTICIAS, 2025).

Por otro lado, en Lima Metropolitana, tiene una situación crítica según (INFOBAE, 2025) refiere que la Policía Nacional del Perú recibió alrededor de 42 000 denuncias por delitos informáticos registradas en año 2024, cerca de 23 700 corresponderían a Lima. Y que los casos de suplantación de identidad pasaron de 747 en año 2023 a 1 204 en año 2024, con incrementos anuales cercanos al 40 % (Dirección de Ciberdelincuencia PNP, 2025).

En este contexto, los autores Avalos et al. (2025) analizan la Ley N.º 32314 que modifica el Código Penal y a la Ley N.º 30096 en función al artículo 11º, para incluir el uso de la IA como circunstancia agravante en diversos delitos, entre ellos aquellos vinculados a la suplantación de identidad, la cual no ha sido acompañada de una reforma integral de los tipos penales, para identificar, probar y sancionar la utilización de IA en estos hechos.

1.3. Formulación del problema

En la presente investigación, a continuación, se presenta dos tipos de problemáticas, identificados como: i) Problema General; y, ii) Problemas específicos.

1.3.1 Problema general

- ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

1.3.2 Problemas específicos

- ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?
- ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?
- ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

1.3.3. Objetivo general

- Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1.3.4. Objetivos específicos

- Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.
- Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.
- Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

1.4 Justificación de la investigación

La investigación se justifica debido al aumento de casos por suplantación de identidad mediante inteligencia artificial en Lima, fenómeno que afecta derechos fundamentales como la seguridad informática, la privacidad y el patrimonio de los ciudadanos. Dado esto, es necesario señalar que, dentro de las funciones de la administración de justicia, la imposición de sanciones es fundamental, debido a que las conductas delictivas no pueden quedar impunes. En este sentido, falsificar la identidad

mediante herramientas de inteligencia artificial no debe quedar exenta de impunidad, ya que se considera una conducta contraria a derecho.

Analizar la Ley N.º 32314 permite evaluar su coherencia con instrumentos internacionales como el Convenio de Budapest y con doctrinas que regulan la responsabilidad penal en entornos automatizados. Asimismo, ofrece un marco para explorar cómo se conceptualiza actualmente la autoría, la tipicidad y la imputación penal cuando intervienen sistemas de IA capaces de generar contenido fraudulento. De este modo, la investigación amplía el debate académico sobre la necesidad de actualizar categorías dogmáticas para enfrentar delitos cometidos con tecnologías avanzadas.

1.4.1 Justificación Teórica

Desde una perspectiva teórica, el estudio contribuye al desarrollo del Derecho Penal Tecnológico y a la comprensión del bien jurídico “identidad digital” ante amenazas emergentes. Analizar la Ley N.º 32314 permite evaluar su coherencia con instrumentos internacionales como el Convenio de Budapest y con doctrinas que regulan la responsabilidad penal en entornos automatizados.

Asimismo, ofrece un marco para explorar cómo se conceptualiza actualmente la autoría, la tipicidad y la imputación penal cuando intervienen sistemas de IA capaces de generar contenido fraudulento. De este modo, la investigación amplía el debate académico sobre la necesidad de actualizar categorías dogmáticas para enfrentar delitos cometidos con tecnologías avanzadas.

1.4.2 Justificación Social

Desde el ámbito social, la suplantación de identidad digital constituye una amenaza latente que afecta a miles de usuarios en Lima y genera pérdidas económicas, afectaciones a la honra y riesgos contra la seguridad personal. La insuficiente eficacia de las normas actuales repercute directamente en la ciudadanía, que queda expuesta a nuevas modalidades de fraude y manipulación que se propagan con rapidez.

Evaluar la aplicación real de la Ley N.º 32314 permitirá identificar si el Estado está respondiendo adecuadamente a esta problemática y qué mejoras pueden implementarse para proteger los derechos digitales de la población. Por ello, la investigación tiene un impacto social significativo al contribuir al fortalecimiento de la confianza en los entornos digitales.

1.4.3 Justificación Metodológica

En el plano metodológico, el estudio se sustenta en un enfoque cualitativo que combina análisis documental y entrevistas semiestructuradas dirigidas a abogados penales, especialistas en la materia, lo que permite comprender la aplicación práctica de la Ley N.º 32314 desde la experiencia de los operadores jurídicos. Este método facilita identificar percepciones, limitaciones y patrones de actuación que no podrían captarse mediante enfoques cuantitativos, ya que la problemática involucra elementos interpretativos, normativos y tecnológicos.

Asimismo, posibilita contrastar el diseño normativo en la implementación real de un cambio normativo, lo cual genera evidencia relevante sobre dificultades en la obtención de prueba digital, atribución de autoría y acreditación del uso de IA en la

comisión del delito materia de estudio. Esto garantiza rigor metodológico y aporta profundidad analítica al estudio.

1.5 Antecedentes de la Investigación

Antecedentes internacionales

En España, Martínez (2024) en su artículo de revista sobre suplantación de identidad digital, el autor tiene como objetivo evidenciar que la identidad digital es una faceta de la privacidad personal, que está constantemente amenazada por las nuevas tecnologías, y que el simple hecho de aparentar ser alguien que no es en el ciberespacio debería ser considerado un delito. La metodología empleada en el estudio fue el análisis jurídico comparativo y propuesta de reforma legislativa. Los resultados evidenciaron una deficiente tipificación de la suplantación de identidad digital en el Código Penal, lo que afecta la protección del derecho a la identidad.

Concluye que es necesario regular de manera autónoma la suplantación de identidad digital, sancionándola directamente castigue directamente, con la finalidad de salvaguardar la identidad digital como un elemento esencial de lo personal y privado, sin limitarse únicamente a los delitos que puedan surgir después como el fraude o la usurpación.

En Italia, Giuca (2023a) en su artículo de revista sobre responsabilidad penal mediante la IA, la autora tiene como objetivo diferenciar la responsabilidad entre los creadores de la IA y los operadores que la utilizan. La metodología utilizada para el estudio es el enfoque normativo jurídico que se fundamenta en el análisis exhaustivo en Europa, comparación entre la culpa convencional y la nueva situación de algoritmos autónomos. Los hallazgos indican que la responsabilidad se asigna al ser humano cuando

no respeta las reglas o cuando no existe un control idóneo. Indica la necesidad de diferenciar entre negligencia específica y negligencia general para evaluar la conducta de productores y usuarios, evidenciando que los fallos de inteligencia artificial no eximen de culpabilidad penal a aquellos implicados en su desarrollo o aplicación.

Concluye que el concepto de "negligencia artificial" permite ajustar el ámbito del Derecho Penal al entorno tecnológico sin otorgar personalidad penal a la IA.

En Portugal, Masseno (2022) en su artículo de revista sobre responsabilidad penal en cuanto a error del algoritmo, el autor tiene como objetivo de estudio es demostrar cómo ciertas acciones pueden poner en riesgo derechos esenciales, siendo la autodeterminación informativa y la privacidad las más afectadas. La metodología se sustenta en el análisis normativo y jurídico del Reglamento General de Protección de Datos, directrices y sentencias del Tribunal de Justicia de la Unión Europea. Asimismo, considera doctrina especializada que examina los impactos del perfilado mediante algoritmos. Los resultados indican que la IA, al tomar decisiones automáticamente, causa discriminación, intrusiones en la privacidad y manejo indebido de información sensible. Además, advierte que el perfilado preventivo puede desarrollarse sin control.

Concluye que no es suficiente con las leyes penales, sino es necesario un enfoque que garantice la protección de los derechos fundamentales.

En Ecuador, los autores Loaiza et al. (2024) en su artículo de revista sobre la transformación de los sistemas de justicia ante la inteligencia artificial, su objetivo se centra en analizar los pros y contras de introducir algoritmos en los procesos judiciales. La metodología empleada es de enfoque cualitativo basado en el análisis de casos, revisión de regulaciones y compilación bibliográfica. Los resultados evidencian que la IA

puede potenciar la eficacia de los procedimientos, facilitar el examen de evidencias digitales y ayudar en la identificación de patrones delictivos.

Concluyen que la IA debe ser un complemento y no un sustituto del juicio humano, sugiriendo el desarrollo de marcos legales sólidos y mecanismos éticos que garanticen el control y aseguren los derechos fundamentales frente al avance de la tecnología.

En México, el autor Gutiérrez (2024) en su artículo de investigación sobre IA y Privacidad, se centra en estudiar las complicaciones que presenta la IA para proteger información personal frente al uso de datos realizada por empresas y gobiernos. La metodología utilizada es de análisis teórico-jurídico de regulaciones, doctrina y literatura destacada. Los hallazgos muestran que el uso intensivo de datos mediante IA disminuye el control que las personas tienen sobre su información. Asimismo, se evidencia que la recopilación masiva, la carencia de transparencia algorítmica y la falta de claridad en la toma de decisiones aumentan los peligros de vigilancia e invasión a la privacidad, afectado negativamente la autodeterminación informativa.

Concluye que es importante adecuar la normativa para la era digital. Y sugiere fortalecer la transparencia, la explicabilidad y la responsabilidad en los sistemas de IA.

Antecedentes nacionales

Desde otra arista, los autores Cieza et al. (2025) en su artículo el análisis forense de imágenes y videos en investigaciones criminales: una revisión sistemática”, tuvo como objetivo analizar el estado del uso de IA desde el contexto forense audiovisual en el ámbito de la criminalidad. La metodología fue cualitativa, análisis jurídico – descriptivo diseño, no experimental, método inductivo mediante entrevistas empíricas. Los resultados

demonstraron que hubo mejoras en autenticación audiovisual, detección de *deepfakes* e identificación facial.

Concluyendo que aún existen limitaciones en el desarrollo de la calidad de datos, en relación a los algoritmos por los sesgos forenses los cuales muchas veces son estándares para un uso responsable en los procesos penales que se llevan a cabo por estos casos.

Arredondo y Casique (2025), en su tesis “La responsabilidad penal de los operadores de telefonía en el delito de suplantación de identidad originada por la venta de chips en puntos no autorizados en el Perú”, pretenden identificar las responsabilidades civiles y penales que tienen las empresas de telefonía móvil en el contexto de delitos de suplantación de identidad, especialmente en situaciones donde la distribución de tarjetas SIM, que se lleva a cabo en lugares no autorizados. La metodología empleada es de enfoque cualitativo, tipo correccional, con diseño basado en la teoría fundamentada, adoptando un método inductivo. El resultado evidencia una ambigüedad doctrinal en relación a la suplantación de identidad y la responsabilidad penal de la persona jurídica, lo que ocasiona dificultades interpretativas.

La conclusión subraya la necesidad de un marco normativo penal específico que regule de manera clara la responsabilidad de las empresas operadoras en casos de suplantación de identidad.

Velásquez (2025), en su tesis “La figura jurídica de la suplantación de identidad frente a las barreras legales en las diligencias preliminares de investigación en el segundo despacho de la fiscalía de Miraflores – 2024”, indica como objetivo identificar los elementos que afectan la efectividad y la eficiencia en la indagación de delitos de suplantación de identidad digital en la Fiscalía Especializada de Ciberdelincuencia de

Arequipa durante el año 2023. La metodología usada es de enfoque cualitativo, tipo exploratorio, adoptando un método dogmático y fenomenológico para examinar la realidad de la investigación a partir de experiencias y documentos relevantes. Los resultados constataron que existe varios factores que dificultan la eficacia y la eficiencia, incluyendo la carencia de equipos tecnológicos adecuados para realizar pericias digitales.

La conclusión enfatiza la necesidad de fortalecer los recursos tecnológicos y recursos críticos como son los profesionales especializados en la Fiscalía para optimizar la indagación de estos delitos.

Santiago y Yesquen (2024), en su tesis “Suplantación de identidad con el uso de la inteligencia artificial”, se centran en evaluar de manera general cómo la usurpación de identidad mediante el uso de IA facilita la realización de delitos y cómo esta situación impacta en los derechos humanos y en el sistema de justicia, en consonancia con el Objetivo de Desarrollo Sostenible 16 de la Agenda 2030. La metodología utilizada es de enfoque cualitativo con una estructura fenomenológica hermenéutica, centrada en interpretar experiencias, analizar documentos y estudiar el fenómeno delictivo asociado con la IA. Los resultados indican que se ha incrementado la perpetración de delitos de suplantación de identidad mediante herramientas tecnológicas basadas en IA, lo cual afecta derechos fundamentales y conlleva un perjuicio moral y patrimonial.

La conclusión es que este fenómeno delictivo actual necesita ser difundido entre la población, para que todos nos informemos y tomemos conocimiento de las nuevas formas de ataque con el fin de prevenir los peligros que puedan presentarse.

Alava y Flores (2024), en su tesis “Análisis comparado de la inteligencia artificial y la suplantación de la identidad en el Perú 2023”, se centra en examinar de manera

comparativa el impacto de la IA en la falsificación de identidades en Perú en el año 2023 y qué disposiciones legales pueden aliviar sus consecuencias. La metodología adopta un enfoque cualitativo, integrado un análisis documental de leyes y teorías, se usó como instrumento una entrevista semiestructurada dirigida a profesionales en el ámbito jurídico y tecnológico. Los resultados muestran que la normativa peruana actual presenta deficiencias ante los desafíos que plantea la IA en la falsificación de identidades.

La conclusión destaca la relevancia de crear directrices éticas y marcos regulatorios firmes que orienten el uso de IA. Además, se sugiere que en nuestro país se familiarice con comparaciones normativas para fortalecer su propia regulación y garantizar los derechos de los ciudadanos.

1.6. Estado de la cuestión

El delito de suplantación de identidad mediante la IA, en el Perú presenta un escenario aún en desarrollo. Debido que las nuevas modalidades delictivas derivadas del avance tecnológico son cometidas en el ciberespacio, donde el anonimato dificulta la identificación de los responsables y obtención de pruebas.

Estudios concuerdan que, en nuestro ordenamiento jurídico, en materia de delitos informáticos resulta insuficiente en desafíos tecnológicos. En ese sentido, la Ley N.º 32314, si bien representa un intento de regulación, presenta limitaciones en su aplicación práctica, evidenciándose una falta de precisión normativa y dificultades en su implementación por parte de las autoridades encargadas de la persecución penal.

Actualmente, se logra identificar que las instituciones encargadas de investigar y sancionar estos delitos presentan problemas para la persecución de este ilícito. Entre ellos

tenemos la capacitación técnica inadecuada, carencia de recursos tecnológicos y carencia de lineamientos especializados.

Categoría 1: Delito de Suplantación de identidad

La suplantación de identidad se considera un daño estructural que excede una afectación patrimonial, debido que compromete directamente la dignidad, autonomía y reputación de la persona en entornos digitales. Este fenómeno se agrava por la velocidad de propagación de la información y la dificultad de revertir sus efectos una vez difundidos. Por consiguiente, el derecho penal y digital, tiene que integrar mecanismos preventivos y reparadores que reconozca a la identidad personal como un bien jurídico vulnerable frente a tecnologías emergentes, siendo insuficientes las respuestas tradicionales centradas solo en el fraude económico (Citron y Solove, 2022).

La suplantación de identidad digital se configura cuando terceros utilizan datos personales de una persona con la finalidad de actuar en su nombre, generando una ruptura entre el sujeto real y su representación digital. Este fenómeno plantea desafíos relevantes para la imputación penal, ya que el daño no siempre se manifiesta de forma inmediata o tangible. En tal sentido, se sostiene que el derecho debe reconocer la identidad digital como una proyección de la personalidad jurídica, cuya vulneración justifica una protección penal autónoma frente a usos indebidos de datos personales y credenciales digitales (Koops, 2022).

La suplantación de identidad es analizada como un delito característico de la sociedad digital, en el que la información personal se convierte en el principal medio para la comisión de lo ilícito. El autor señala que la facilidad de acceso a datos en línea ha incrementado, la frecuencia y sofisticación de estas conductas, dificultan su detección y

persecución. En este contexto, se destaca la necesidad de adaptar los tipos penales a las nuevas modalidades tecnológicas, incorporando criterios que permitan sancionar no solo el resultado, sino también la creación de riesgos graves para la identidad y seguridad digital de las personas (Brenner, 2010).

- Prueba digital y pericia digital

Los autores sostienen que la prueba digital, solo adquiere valor probatorio cuando su obtención y análisis se realizan bajo parámetros técnicos verificables. En este sentido, la pericia digital, debe garantizar la autenticidad e integridad de los datos mediante procedimientos reproducibles y controlables, incluso cuando se utilicen herramientas forenses de código abierto. Por ende, la admisibilidad judicial no depende del software utilizado, sino de la adecuada documentación metodológica, la preservación de la cadena de custodia y la posibilidad de explicar los márgenes de error ante el juez. (ISMAIL, 2025)

Los autores consideran que la cadena de custodia constituye el eje central de la credibilidad de la prueba digital, debido a la naturaleza volátil y fácil manipulación. Y, que la evidencia digital debe estar acompañada de registros detallados que permitan rastrear cada intervención humana o tecnológica desde su recolección hasta su presentación en juicio. Asimismo, indica que la ausencia de controles claros genera riesgos de manipulación o pérdida de integridad, lo que debilita la fuerza probatoria del peritaje. Por ello, proponen modelos estructurados que integren seguridad, trazabilidad y auditabilidad como requisitos mínimos para su aceptación judicial (Nath et al., 2024).

El estudio realizado señala que la cadena de custodia en el ámbito digital no es un simple requisito formal, sino una garantía sustancial de validez probatoria. Los autores explican que, a diferencia de la evidencia material tradicional, los datos digitales pueden duplicarse, modificarse o trasladarse sin dejar huellas visibles, lo que exige protocolos más estrictos de control. En este sentido, la pericia digital debe asegurar la continuidad lógica y técnica del manejo de la evidencia, documentando cada fase del proceso que cualquier ruptura o deficiencia en la custodia compromete seriamente la confiabilidad del dictamen pericial ante el órgano jurisdiccional (D'Anna et al., 2023).

- Reconocimiento de la autodeterminación informativa y la seguridad digital

En primer lugar, se percibe a la autodeterminación informativa como fundamento del derecho de protección de datos, argumentando que el concepto de “control individual” resulta limitado frente a la complejidad de los entornos digitales actuales. Aunque este derecho cumple una función relevante frente a la intervención estatal, su aplicación en el ámbito privado es insuficiente para garantizar una protección efectiva. En ese sentido, considera que la seguridad digital no puede basarse únicamente en el consentimiento del titular de datos, sino requiere de marcos normativos estructurales que impongan deberes, límites y responsabilidades a los agentes que tratan información personal (Thouvenin, 2021).

Por otro lado, se considera que la autodeterminación informativa se ve debilitada en la economía de plataformas digitales, donde los usuarios carecen de un control real sobre los algoritmos y los flujos de datos. El autor sostiene que los mecanismos tradicionales de protección, especialmente el consentimiento, resulta simbólico frente a las asimetrías de poder tecnológico. Por tanto, sugiere una reinterpretación colectiva del

derecho a la autodeterminación, orientada a fortalecer la gobernanza digital y la seguridad de los datos mediante formas de participación y regulación estructural. De esta manera la seguridad digital se concibe como una cuestión de equilibrio institucional y no solo como una decisión individual (Huapaya, 2024).

Finalmente, la seguridad digital no debe justificar prácticas invasivas sin límites claros, ya que ello transforma la protección en un mecanismo de control. En tal sentido, propone que la autodeterminación informativa opere como un criterio jurídico para evaluar la legitimidad, proporcionalidad y necesidad de las tecnologías de vigilancia. De este modo, la seguridad digital debe armonizarse con garantías efectivas de transparencia y control ciudadano. (Carter y McNealey, 2025).

- Elementos típicos en la imputación penal

En este sentido, la imputación penal debe construirse respetando los elementos típicos del delito, evitando atribuciones genéricas o presunciones automáticas de culpabilidad. Por ello, una imputación legítima exige identificar con claridad la conducta atribuida, su adecuación al tipo penal y la concurrencia del elemento subjetivo correspondiente. Asimismo, enfatiza que imputaciones poco fundamentadas vulneran el derecho de defensa y desnaturalizan el principio de culpabilidad. En consiguiente, la imputación debe estar sustentada en hechos concretos y en una subsunción jurídica razonada, sin atajos argumentativos (Taboada, 2024).

La imputación penal deliberada solo puede imputarse cuando existen indicios claros de que el sujeto decidió conscientemente no conocer el origen ilícito de los bienes.

De lo contrario, se incurre en una imputación expansiva incompatible con los principios de legalidad y culpabilidad (Mamani, 2026).

La imputación constituye el eje central del debido proceso, generan indefensión, así como también demora en las decisiones inconsistentes, en la coherencia del proceso penal, subrayando el respeto al principio de imputación específica, dado que delimita el objeto de la acusación y permite el ejercicio efectivo del derecho de defensa. Por lo cual, toda imputación debe describir de manera precisa los hechos atribuidos y su correspondencia con los elementos normativos penales, toda vez que, ante la carencia de claridad o ambigüedad en la imputación genera decisiones arbitrarias que vulnera la seguridad jurídica, en ese contexto; una imputación técnicamente correcta es condición indispensable para la validez del reproche penal (Marchena, 2026).

Categoría 2: Inteligencia artificial

Sistema sociotécnico capaz de tomar decisiones que influye directamente en derechos fundamentales, lo que exige una regulación jurídica orientada al control del riesgo. Desde esta perspectiva, se indica que la IA no es neutral, puesto que refleja decisiones humanas incorporadas en su diseño y entrenamiento. Bajo el ámbito legal, propone que el uso de IA debe someterse a principios como responsabilidad, transparencia y rendición de cuentas, con el fin de evitar efectos discriminatorios o lesivos. De este modo, el derecho debe anticiparse a los riesgos y no limitarse a reaccionar una vez producido el daño (Floridi et al., 2018).

La inteligencia artificial trae consigo desafíos para los modelos tradicionales, en materia de responsabilidad jurídica, debido a la opacidad y autonomía en los sistemas

algorítmicos. El autor sostiene que la delegación de decisiones en algoritmos no exonera a los operadores humanos de responsabilidad, especialmente cuando los riesgos son previsibles. En este sentido, se argumenta que la imputación jurídica debe centrarse en el control efectivo del sistema y en los deberes de diligencia de quienes lo implementan. Por ende, la IA requiere un marco normativo que asigne claramente responsabilidades y evite vacíos de imputación (Mittelstadt, 2019).

Considerada como una tecnología que refuerza el poder de decisión en las organizaciones, generando nuevas formas de riesgo social y jurídico. El autor sostiene que cuando las empresas utilizan sistemas automatizados con capacidad de causar daños, asumen una posición de garante frente a los efectos de dichas decisiones. Desde esta perspectiva, el derecho penal debe adaptarse para imputar responsabilidad cuando exista falta de supervisión o control adecuado del sistema. De este modo, la IA no elimina la responsabilidad humana, sino que redefine sus formas de atribución (Calo, 2017).

- Protección a la identidad digital de la víctima

Los estudiosos (Citron y Solove, 2022) indican que la identidad digital de la víctima constituye una extensión directa de su personalidad jurídica, por lo que su afectación mediante tecnologías digitales genera daños reales y persistentes. Argumentan que prácticas como la suplantación, la difusión no autorizada de datos o la manipulación de información erosionan la autonomía y dignidad de la persona. En términos legales, sostienen que la protección debe ir más allá del derecho a la privacidad, incorporando mecanismos de prevención, reparación y eliminación efectiva del daño digital. A tal efecto, proponen una tutela reforzada de la identidad digital, especialmente frente a plataformas que amplifican el perjuicio a gran escala.

El autor estudia la protección de la identidad digital desde el derecho de protección de datos y sostiene que la víctima debe mantener un control significativo sobre la información que la representa en entornos digitales. A su vez, indica que la pérdida de control sobre datos personales facilita delitos como la suplantación de identidad y la revictimización en línea, de los marcos normativos actuales suelen reaccionar de manera tardía frente al daño ya consumado respecto a la tutela de la identidad digital exige obligaciones preventivas claras para quienes procesan datos, reforzando la seguridad y la responsabilidad en el tratamiento de la información personal (Zuiderveen y Poort, 2017).

El autor sostiene que la identidad digital debe ser entendida como un bien jurídico autónomo que requiere protección frente a riesgos tecnológicos emergentes. Señala que la víctima de delitos digitales sufre un daño, debido a la información manipulada puede replicarse indefinidamente y afectar su reputación y derechos fundamentales, defensa de la identidad digital no solo es una cuestión individual, sino también un deber institucional orientado a prevenir daños sistémicos (Mantelero, 2025).

- Cooperación digital integral e interoperabilidad institucional

El autor sostiene que la interoperabilidad institucional es un elemento clave para una cooperación digital efectiva en la persecución de delitos tecnológicos. Argumenta que la fragmentación de sistemas informáticos entre entidades públicas dificulta el intercambio oportuno de información y debilita la respuesta estatal. En términos jurídicos, señala que la cooperación digital debe estar sustentada en reglas claras de competencia, protección de datos y responsabilidad institucional. De este modo, la interoperabilidad no solo es una cuestión técnica, sino un instrumento jurídico esencial para garantizar eficacia, legalidad y seguridad en la actuación estatal (Schartum, 2020).

Bajo el marco de derecho europeo, los autores señalan que la interoperabilidad institucional debe equilibrar eficiencia y protección de derechos fundamentales, se examina como iniciativa desde la perspectiva de la digitalización e interoperabilidad respecto a los datos personales, mediante el intercambio de información por agencias para enfrentar los delitos tecnológicos en aras de proteger los derechos fundamentales, dentro de los distintos marcos legales facilitando la recolección, transferencia o almacenes de datos en el ciberespacio. Asimismo, destacan que el intercambio automatizado de información entre entidades puede mejorar la persecución penal, pero también incrementar riesgos de uso indebido de datos. Por consiguiente, proponen un modelo de cooperación digital integral basado en principios de legalidad, finalidad específica y control institucional (Vavoula, 2025).

Estos autores sostienen que la cooperación digital integral exige superar los enfoques aislados de cada institución y avanzar hacia ecosistemas interconectados de información pública. Afirman que la interoperabilidad permite respuestas más rápidas frente a delitos complejos, como la ciberdelincuencia transnacional. Sin embargo, advierten que, sin una arquitectura jurídica común, el intercambio de datos puede generar inseguridad jurídica y conflictos de competencia. En consecuencia, plantean que la cooperación digital debe estar normativamente estructurada para garantizar coordinación, transparencia y responsabilidad entre las entidades involucradas (Sion et al., 2023).

- Responsabilidad penal algorítmica para las empresas

Los sistemas algorítmicos utilizados por las empresas generan riesgos jurídicos significativos cuando producen decisiones automatizadas con impacto en derechos fundamentales. Aunque los algoritmos no son sujetos de derecho, las organizaciones que

los diseñan, implementan o supervisan deben asumir responsabilidad por sus efectos. Desde la perspectiva penal, señala que la opacidad algorítmica no puede servir como excusa para eludir responsabilidad. En este sentido, sugiere un enfoque de responsabilidad basado en el control, previsibilidad del riesgo y deber de diligencia empresarial (Januário, 2023).

El autor analiza la responsabilidad empresarial frente a daños causados por sistemas automatizados y sostiene que el derecho penal debe adaptarse a los riesgos derivados de decisiones algorítmicas. En este contexto, argumenta que cuando una empresa introduce algoritmos capaces de causar perjuicios previsibles, asume una posición de garante referente a la imputación penal puede configurarse si se demuestra negligencia en el diseño, supervisión o corrección del sistema, la responsabilidad penal algorítmica se fundamenta en la omisión de deberes de control tecnológico adecuados. (Yazdanpanah et al., 2023).

Desde otra postura, los autores (Busch et al., 2019) perciben que la utilización empresarial de IA exige repensar los modelos clásicos de responsabilidad jurídica, incluida la penal. Bajo estas circunstancias, mencionan que las decisiones algorítmicas no son neutras, sino el resultado de elecciones humanas incorporadas en el diseño y entrenamiento del sistema. Por ello, proponen atribuir responsabilidad a las empresas cuando estas se benefician del uso de algoritmos sin implementar salvaguardas suficientes.

Marco Jurídico

La Ley N.º 32314 fue promulgada con la finalidad de fortalecer la persecución de conductas ilícitas vinculadas a entornos digitales; sin embargo, su formulación resulta insuficiente frente a delitos cometidos mediante inteligencia artificial. La norma no desarrolla elementos técnicos que permitan identificar la autoría en contextos de automatización algorítmica ni regula expresamente la manipulación de identidades digitales. Esta omisión genera dificultades prácticas en la investigación penal y debilita la eficacia de la persecución del delito. Desde una interpretación sistemática, la ley no se adecúa al principio de realidad tecnológica. Ello evidencia su inoperancia normativa frente a nuevas formas de criminalidad digital.

En los artículos 158º y 185º de nuestro Código Procesal regula la valoración probatoria bajo criterios de licitud y razonabilidad, así como la actuación de pericias especializadas. Sin embargo, estos artículos no desarrollan estándares específicos para la evidencia digital generada o manipulada mediante inteligencia artificial. La ausencia de lineamientos técnicos sobre autenticidad, integridad y trazabilidad digital genera incertidumbre probatoria. Esta debilidad afecta la acreditación del hecho delictivo y la responsabilidad penal. En delitos de suplantación digital, ello se traduce en una investigación ineficaz. Por tanto, el marco procesal resulta insuficiente frente a nuevas tecnologías.

Aunado a ello, el Código Penal – Estafa agravada (art. 196-A) por manipulación con IA, aborda el marco jurídico respecto a sancionar con agravante la estafa cuando se realiza a través de la manipulación de voz por medio de audios, imágenes o movimientos

corporales de terceros mediante el empleo de la IA o tecnologías análogas, como medio comisivo para lograr fraudes.

En Ley N.º 30096 (Ley de Delitos Informáticos), tipifica diversas conductas delictivas vinculadas al uso indebido de sistemas informáticos y datos digitales. No obstante, su enfoque se centra en accesos ilícitos, interferencias y fraudes informáticos, sin abordar la manipulación algorítmica de identidades. Esta limitación normativa impide su aplicación efectiva en casos de suplantación mediante inteligencia artificial. La ley no contempla criterios técnicos para la obtención de evidencia digital compleja. Ello evidencia una falta de actualización frente a la evolución tecnológica. En consecuencia, su aplicación resulta parcial e insuficiente.

En nuestra Carta Magna, establece en su Artículo 2º, inciso 6 el derecho fundamental a la autodeterminación informativa y a la protección de los datos personales. Este derecho garantiza que toda persona controle el uso de su información en entornos físicos y digitales. Sin embargo, la Ley N.º 32314 no desarrolla mecanismos eficaces para proteger este derecho frente al uso de inteligencia artificial. La ausencia de medidas específicas debilita la seguridad digital de las víctimas. Desde una interpretación constitucional, esta omisión afecta la tutela efectiva de derechos fundamentales. Por ello, se evidencia una desconexión entre la norma penal y el mandato constitucional.

La ley N.º 29733 (Ley de Protección de Datos Personales), establece principios y obligaciones para el tratamiento legítimo de datos personales. No obstante, su aplicación frente a la inteligencia artificial resulta limitada, ya que no regula de forma expresa el tratamiento automatizado de datos con fines ilícitos. La norma carece de mecanismos de

coordinación efectiva con el derecho penal. Esta falta de integración dificulta la persecución del delito de suplantación de identidad digital. En consecuencia, la protección de la autodeterminación informativa se ve debilitada. Ello evidencia la necesidad de una interpretación extensiva y una reforma normativa.

Por su parte, el principio de legalidad regulado en el Artículo II del Título Preliminar del Código Penal exige que las conductas delictivas estén claramente tipificadas por ley. La Ley N.º 32314 no incorpora elementos específicos relacionados con la inteligencia artificial, lo que afecta la previsibilidad de la norma penal. Esta deficiencia dificulta la correcta tipificación del delito de suplantación de identidad digital. Como resultado, se generan interpretaciones dispares que afectan la seguridad jurídica. Desde un análisis dogmático, ello vulnera el principio de taxatividad. En consecuencia, la respuesta penal resulta ineficaz.

II. METODOLOGÍA

2.1 Enfoque de la investigación

Los autores (Thomas et al., 2024) sostienen que el enfoque cualitativo debe abordarse desde una perspectiva interpretativa cualitativa, enfocándose en entender vivencias, significados y prácticas. Afirma que, cuando se utilizan con verdaderos valores cualitativos, pueden ofrecer datos profundos, ricos y con un sustento teórico, y así van más allá de la noción de que solo generan información superficial.

2.1.1. Tipo de estudio

El tipo de estudio de emplearse al presente es documental, de acuerdo a lo señalado por el autor (Ordoñez-Pacheco, 2025) refiriendo que el estudio basado en documentos se emplea como un método para reunir, examinar y estructurar información de textos y análisis anteriores, ayudando a formular de manera cuidadosa un marco teórico y metodológico sin la necesidad de obtener datos originales. Esta técnica posibilita organizar de manera lógica los componentes de la metodología y es congruente con una perspectiva cualitativa (p.5)

Respecto al nivel de investigación el autor (Supo, 2023) menciona que este nivel se enfoca en ilustrar de forma precisa las características, atributos y conductas de un fenómeno sin indagar sobre sus causas, sino en cómo se presenta en un contexto específico. De acuerdo con los especialistas en metodología, este nivel facilita la identificación, organización y exposición de información tal como se percibe en la realidad, logrando una representación fiel y ordenada del objeto de investigación. El nivel a emplearse al presente estudio es descriptivo, toda vez que busca analizar, comparar, examinar la eficacia de la Ley N.º 32314.

2.1.2 Diseño de la investigación

Se desarrolla al presente trabajo es el diseño no experimental y diseño jurídico – descriptivo, al respecto el autor Ordoñez (2025) sostiene que este tipo de diseño busca analizar y desarrollar descriptivamente el fenómeno de estudio en base al estudio de la fundamentación jurídica, teorías, literatura, jurisprudencias y marco legal (p.9)

2.1.3. Población y muestra

Los autores (Cash et al., 2022) señalan que la población y muestra compete al total de elementos, individuos o casos que poseen características significativas para la investigación. Aclara que la muestra es una parte representativa de esa población, escogida para facilitar el análisis cuando no es factible examinar a todos los miembros. Resalta que una muestra de calidad debe ser suficiente, relevante y apropiada para reflejar las cualidades de la población. También enfatiza la necesidad de usar criterios de inclusión y exclusión para establecer quiénes integran la muestra. Por último, argumenta que una clara definición de población y muestra permite obtener resultados válidos, fidedignos y aplicables en el ámbito de la investigación.

2.1.4 Técnicas de reproducción de datos

El autor (Taherdoost, 2021) sostiene que recolectar información, son una etapa crucial para asegurar la validez y la fiabilidad en una investigación. Además, indica que la selección depende del enfoque, las metas y las características del grupo estudiado. Diferencia entre métodos primarios, como encuestas, entrevistas y observación, y métodos secundarios, que incluyen documentos y registros ya disponibles.

La observación captura comportamientos reales sin una intervención directa. Además, subraya que la técnica elegida debe reducir sesgos y adherirse a un procedimiento ordenado. Finalmente, resalta la relevancia de respetar principios éticos, como el consentimiento y la confidencialidad.

2.1.5 Procedimientos

El autor (Chand, 2025) establece que los métodos de recopilación de datos en estudios cualitativos, enfocándose en entrevistas, grupos focales, observación y análisis de documentos. Se detalla el proceso a través del cual se obtienen datos enriquecedores que permiten abordar interrogantes de investigación y explorar fenómenos complejos. Adicionalmente, se menciona cómo cada método aporta al desarrollo del conocimiento desde diversas fuentes y ángulos, y se enfatiza la relevancia de aplicar enfoques combinados (triangulación) para garantizar la profundidad, cohesión y rigor en la metodología de los datos obtenidos en investigaciones cualitativas.

2.1.6. Aspectos éticos

Los autores (Vlckova et al., 2024) sostiene que los aspectos éticos se enfatiza la responsabilidad de garantizar el respeto, el bienestar, el consentimiento informado y la

protección de los participantes vulnerables, destacando que la investigación en este escenario es compleja y requiere atención especial en cada fase del proceso.

III. RESULTADOS

Para este apartado, se procederá con desarrollar la presentación de los resultados en base a las entrevistas realizadas a cada entrevistado y especialista en la materia. Cabe resaltar que este trabajo se destacó en tres fases relevantes, en primer lugar, la fase de recaudación de la información basado en las teorías identificadas con el objeto de estudio asociándolas con las categorías.

En segundo lugar, la fase descriptiva de las características de las categorías seleccionadas las cuales desprendieron a las subcategorías; y, en tercer lugar, la fase final que conllevó al análisis, tabulación y triangulación de las fuentes que permitieron poder transcribir y codificar toda la información resaltante del estudio, para de esta forma llegar a los resultados estimados y conclusiones finales para el problema abordado.

En ese contexto, se ajustarán acorde a cada objetivo presentado, es en ese mismo sentido, que el autor (Díaz Bustos et al., 2024) explicó que la triangulación es la descripción de un estudio donde se cruzaran datos e información a desarrollar del objeto observado para luego ser analizado e interpretado a través de los alcances obtenidos por el investigador en el fenómeno abordado.

Por consiguiente, los siguientes entrevistados son:

- (E1) Mery Salas De Torres
- (E02) Roger Ureta Cóndor
- (E03) Fernando Renzo Abanto Borgoño
- (E04) Klinton Abregu Gaspar
- (E05) Manuel Alvarado Rodríguez:
- (E06) Luis Salomón Felles Damian
- (E07) Melissa Nadine Rodríguez Yarasca
- (E08) Alan José Rodríguez Díaz
- (E09) Yosseling Yahaira Morales Higinio
- (E10) Edgar Alcides Mondaca Bejar

Tabla 1. Respuesta de entrevistados - Objetivo General

Entrevistado Preguntas	Entrevistado 1 (Salas)	Entrevistado 2 (Ureta)	Entrevistado 3 (Abanto)	Entrevistado 4 (Abregú)	Entrevistado 5 (Alvarado)	Entrevistado 6 (Felles)	Entrevistado 7 (Rodríguez Y.)	Entrevistado 8 (Rodríguez D.)	Entrevistado 9 (Morales)	Entrevistado 10 (Mondaca)
Pregunta 1: ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?	Se debe tomar en cuenta, que para la persecución de este tipo de delitos es necesario que tanto la Policía y como el Ministerio Público, deben llevar a cabo capacitaciones para el personal que la persecución de este delitos y todos los que conciernen a entornos digitales por medio de plataformas u otros análogos, que conforman de manera descentralizada, lo cual permitirá que se creen más Unidades Especializadas en Peritajes Digitales que puedan analizar evidencias que hayan sido generadas o usadas por medio tecnologías como la Inteligencia Artificial – IA. Aunado a ello, se debe contar con herramientas digitales optimas y actualizadas a los nuevos modelos tecnológicos en el caso de la ciberdelincuencia en cibercrimen, los cuales deben estar a la altura de la modernidad ejercida por los delincuentes de este tipo, a fin de evitar que los casos remitidos al Ministerio Público queden en un simple archivamiento o sobreseimiento.	La inoperancia se evidencia en la ausencia de una definición técnica clara sobre suplantación mediante sistemas de inteligencia artificial, especialmente frente a fenómenos como deepfakes o clonación de voz. La norma mantiene un enfoque tradicional del fraude informático sin incorporar las particularidades de la generación sintética de identidades. Ello dificulta la delimitación típica y genera interpretaciones extensivas que afectan la seguridad jurídica. En la práctica fiscal, se observa que los operadores recurren a tipos penales conexos por falta de precisión normativa. Esta deficiencia impacta en la formulación de imputaciones concretas. Además, la ley no contempla estándares probatorios diferenciados para entornos algorítmicos. Como consecuencia, la persecución penal se toma reactiva y no preventiva. Ello revela una brecha entre la evolución tecnológica y la respuesta legislativa.	La ineficacia normativa de Ley N.º 32314 se define primordialmente en la brecha existente entre la previsión normativa y la realidad criminológica digital. Si bien esta norma integra el uso de inteligencia artificial, como agravante en delitos específicos y modifica el Código Penal y la Ley de Delitos Informáticos, su esquema responde a un modelo clásico de ciberdelincuencia, que no incorpora estructuralmente las nuevas modalidades de manipulación algorítmica de la identidad digital. En el ámbito de política criminal, el problema se encuentra en la norma la cual, si bien es cierto que especifica la utilización de la inteligencia artificial como agravante, lo es también que no desarrolla completamente los supuestos fácticos específicos de suplantación de identidad utilizados con las mediante tecnologías de producción y generación de materiales digitales, tales como deepfakes, clonación de voz, identidades sintéticas o manipulación biométrica digital. Este punto de deficiencia crea complicaciones de subsunción típica en los operadores de justicia.	Sin duda, el avance tecnológico, no solo genera beneficios, sino problemáticas, que deben ser controlados. En tal sentido, la inoperancia de la Ley se manifiesta básicamente en el tema de especialización del personal del Ministerio Público, y en la implementación de Tecnología capaz de detectar estos ilícitos, y evidenciarlos en un proceso penal. así como en la obtención, validación, preservación y valoración de la evidencia digital.	La inoperancia de la Ley N.º 32314 se manifiesta principalmente en la brecha entre su contenido formal y su eficacia práctica. Conviene precisar que esta ley no crea tipos penales autónomos de suplantación mediante IA, sino que modifica el Código Penal y la Ley N.º 30096 para incorporar la inteligencia artificial como circunstancia agravante. Así, el artículo 46, literal ñ del Código Penal y el artículo 11, numeral 5 de la Ley de Delitos Informáticos establecen que el uso de IA o tecnologías similares eleva la pena hasta en un tercio por encima del máximo legal. El problema no es, pues, la ausencia de mención normativa, sino la ausencia de una regulación procesal complementaria que permita operativizar estos agravantes. En la práctica limeña, los operadores de justicia carecen de protocolos técnicos para acreditar que un determinado contenido fue generado mediante IA y no por manipulación convencional, lo que hace inoperante el agravante. No existen peritos judiciales certificados en análisis forense de sistemas de IA generativa, ni estándares de cadena de custodia para contenidos sintéticos. En consecuencia, la norma existe formalmente pero no puede ser aplicada eficazmente, configurando una inoperancia de carácter	Desde mi experiencia, la inoperancia se manifiesta principalmente en la falta de adecuación normativa frente a las nuevas modalidades delictivas basadas en inteligencia artificial, como los deepfakes o la clonación de voz. La ley no define con precisión estas conductas ni establece mecanismos claros de investigación digital, lo que genera vacíos al momento de tipificar y sustentar los casos. En la práctica, esto se traduce en dificultades para encuadrar jurídicamente los hechos y para obtener pruebas idóneas.	La inoperancia de la Ley N.º 32314 se manifiesta principalmente en que la norma no crea un tipo penal autónomo para la suplantación de identidad mediante inteligencia artificial, sino que incorpora el uso de la inteligencia artificial como circunstancia agravante o medio de comisión del delito dentro del Código Penal y la Ley de Delitos Informáticos. En la práctica, cuando se presentan casos de suplantación mediante deepfakes, clonación de voz o creación de identidades digitales falsas, los operadores jurídicos deben reconducir la conducta a tipos penales ya existentes, como estafa, difamación o suplantación informática. Esto genera dificultades en la tipificación y en la imputación penal, pues la norma no regula de manera específica estas nuevas modalidades tecnológicas. Por ello, la persecución penal termina dependiendo de interpretaciones extensivas de tipos ya existentes, lo cual limita la eficacia del sistema penal frente a nuevas formas de criminalidad digital.	Esto se manifiesta principalmente a través de la impunidad técnica. La norma tiene un carácter declarativo, pero carece de herramientas coercitivas y procesales específicas para lograr la identificación de autores que utilizan redes o servidores en el extranjero. La inoperancia es visible cuando el Ministerio Público intenta aplicar tipos penales clásicos a conductas donde el "sujeto activo" es un algoritmo operado anónimamente, resultando en el archivo de denuncias por falta de individualización del presunto autor.	La inoperancia enmarcada a la ley citada se evidencia en desconexión entre su formulación normativa aplicativa y la complejidad del incremento y avances por parte de las organizaciones criminales con respecto a los delitos realizados en entornos digitales. Si bien la normativa incorpora al delito cibernético el uso de la IA como agravante, no desarrolla de forma oportuna y real las nuevas formas de suplantación de identidad, siendo ello un factor limitante que imposibilita una adecuada subsunción jurídica de las conductas. Por todo lo expuesto, los operadores de justicia y las instituciones responsables de estos casos se enfrentan a vacíos interpretativos. En ese sentido, ello disminuye la posibilidad de una eficacia jurídica dentro del sistema penal, enfrentada a la evolución de las altas tecnologías. Como aporte puedo resaltar que es necesario diseñar una legislación tecnológica penal que incorpore una tipificación autónoma cuando se vea en conflicto los casos de suplantación de identidad por medio de la IA.	Considero que la inoperancia de esta normativa se traslada en la ausencia de agravantes específicos para materializar estos delitos por medio de las tecnologías modernas como la Inteligencia Artificial en la nueva era del derecho digital, y dentro de la esfera peruana, es de suma importancia operativizar y mejorar las instituciones a través de la transformación digital y gobierno digital para modernizar las instituciones del Estado que son partícipes de reducir estos delitos, .

					fundamentalmente institucional y procesal.					
Pregunta 2: Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.	Desde mi experiencia como jefa y miembro de la PNP, se entiende jurídicamente este concepto en la práctica, tiene la intención de avanzar, sin embargo, la realidad es otra porque la criminalidad digital avanza y ello se demuestra con la elevada estadística respecto a las denuncias por ciberdelitos, se debe actualizar el código penal y la Ley especial de Delitos Informáticos, considero inclusive que todo debe ser dentro del Código Penal.	Desde una perspectiva técnica, la ley resulta insuficiente frente a la sofisticación actual de la criminalidad digital. La inteligencia artificial permite crear identidades sintéticas con alto grado de verosimilitud. La norma no regula expresamente estas modalidades emergentes. Tampoco contempla criterios de prevención tecnológica. Su enfoque es esencialmente sancionador y no preventivo. Carece de articulación con políticas de ciberseguridad. Además, no integra estándares internacionales en materia de delitos tecnológicos. Por ello, su adecuación es parcial y limitada. Requiere actualización urgente.	En el ámbito jurídico-penal, la promulgación de Ley N.º 32314 constituye un progreso relevante en el interior del sistema penal peruano, al identificar claramente el uso de inteligencia artificial como instrumento potencial para la comisión de delitos y sus agravantes en las conductas ilícitas son realizadas con tecnologías basadas en inteligencia artificial o herramientas digitales análogas. No obstante, en lo dogmático y criminológico, el punto de vista del legislador podría definirse como parcial. La ley solo está limitada en el incremento de las penas o a insertar agravantes; sin embargo, no define una tipificación independiente de los delitos que son derivados de manipulación algorítmica de identidad digital, lo que disminuye su eficacia preventiva y represiva.	Evidentemente no, sin embargo, es un avance, que debe ser perfeccionado. Me refiero que es un avance en el sentido que, en el ámbito penal ya se ha considerado como una problemática el uso de la Inteligencia Artificial, sin embargo, a mi consideración el fenómeno que está causando el uso de la Inteligencia Artificial, cada vez se hace inmensamente compleja. Toda vez, que, si es que lo vemos desde una perspectiva individualista, resulta complejo su detección. Ahora, si lo colocamos el uso ilícito de estas tecnologías, en manos de organizaciones criminales altamente complejas. Definitivamente, se requerirá de personas altamente especializada para su entendimiento y posterior sanción. Mientras tanto, la tranquilidad y paz pública seguirán siendo menoscabadas (sociedad con miedo a ser suplantados, estafados, chantajeados, etc.)	Desde mi perspectiva profesional, la Ley N.º 32314 representa un avance normativo relevante, pues por primera vez en el Perú se incorpora explícitamente la inteligencia artificial como elemento de la reacción punitiva. La norma modifica el Código Penal y la Ley de Delitos Informáticos para tratar la IA como agravante en delitos como estafa (Art. 196-A, hasta 8 años), difamación mediante deepfakes (Art. 132, hasta 5 años), pornografía infantil con IA (Art. 129-M, entre 6 y 10 años), y los delitos informáticos en general vía el Art. 11 numeral 5 de la Ley 30096. En ese sentido, la norma no es ajena a la realidad tecnológica. Sin embargo, la ley resulta insuficiente para enfrentar los desafíos de la criminalidad digital vinculada a la IA porque adopta una lógica meramente punitiva-agravante, sin acompañarla de la infraestructura institucional necesaria. No establece protocolos de investigación digital específicos para casos de IA, no crea unidades especializadas en el Ministerio Público ni en la PNP, y no prevé obligaciones de colaboración para proveedores de tecnología. Una regulación eficaz requeriría no solo endurecer penas, sino construir la capacidad estatal para probarlas.	Considero que no responde de manera adecuada. Si bien representa un avance, su enfoque aún es general y no aborda de forma específica el uso de inteligencia artificial en la comisión de delitos. La criminalidad digital evoluciona más rápido que la legislación, y actualmente no se cuenta con herramientas normativas suficientes para enfrentar fenómenos como la automatización del fraude o la manipulación de identidad digital mediante IA. Esto limita la eficacia del sistema penal.	Desde una perspectiva práctica, la Ley N.º 32314 constituye un avance inicial, ya que reconoce que la inteligencia artificial puede ser utilizada como medio para cometer delitos y permite agravar las penas cuando se utilice esta tecnología. Sin embargo, la norma resulta insuficiente frente a los desafíos actuales de la criminalidad digital, debido a que no regula de manera integral fenómenos como: la creación de identidades sintéticas, los deepfakes, la clonación de voz, la manipulación algorítmica de información personal. En ese sentido, la ley tiene un enfoque reactivo y no preventivo, ya que se limita a aumentar sanciones sin desarrollar mecanismos específicos para la investigación, prueba o identificación de estos delitos.	No responde a ningún desafío, a pesar que se entiende que la ley es un esfuerzo loable pero insuficiente. Se queda en la superficie de la "regulación de uso" sin profundizar en la reforma procesal penal necesaria. Los desafíos de la IA requieren no solo una ley marco, sino protocolos de evidencia digital que la Ley 32314 no detalla, dejando a los operadores de justicia con una norma "letra muerta" ante ataques de material audiovisual falsos.	Considero desde mi experiencia realizando investigación sobre datos personales como investigadora que la ley representa un avance claro al reconocer el uso de la IA, empero la comisión de estos delitos tiene un alcance limitado al centrarse en agravantes, no se verifica tipos penales autónomos que aborden complicaciones de este fenómeno digital, por lo cual la normativa no puede cumplir su rol preventivo frente a los desafíos digitales actuales.	Desde mi experiencia como abogado penalista, he tenido clientes que han presentado denuncias por el empleo de la IA en delitos, sin embargo, su persecución es carente, debido a que no existen mecanismos de protección digital para las víctimas. En ese contexto, puedo indicar que existe un trabajo de parte del Estado y las instituciones para actualizarse a estas nuevas tendencias delictivas y lograr eficazmente sancionarlo.
Pregunta 3: ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la	Siempre se han preocupado en mejorar el marco legal para hacer frente a este tipo de	No se observa una mejora sustancial en la capacidad investigativa. La ley no ha venido	El uso de inteligencia artificial como agravante penal es un importante	No ha logrado mejoras efectivas, pero es un comienzo. Podría considerar como	La Ley N.º 32314 no ha logrado una mejora sustancial en la capacidad operativa del sistema	No de manera significativa. En la práctica fiscal, persisten serias dificultades para	No de manera significativa. La Ley N.º 32314 incrementa la gravedad de la	No de manera efectiva. Si bien pone el tema en la agenda pública, la capacidad	Considero que la normativa introduce avances formales al reconocer el uso de la IA, no obstante,	En el caso en particular, el sistema penal no cuenta con herramientas tecnológicas

capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?	delitos, sin embargo, como ya lo mencioné se necesita mayor capacitación al personal involucrado en este tipo de investigación y definitivamente descentralizar estas capacitaciones con la finalidad de contar con laboratorios forenses digitales en puntos críticos de nuestro país.	acompañada de fortalecimiento institucional. Sin capacitación técnica, la norma pierde eficacia real. Los fiscales enfrentan limitaciones probatorias complejas. Además, la ausencia de peritos especializados dificulta la acreditación del ilícito. La tipificación continúa siendo genérica. Esto limita la precisión de la imputación. Por ende, la mejora es marginal. La brecha tecnológica persiste.	avance en el sistema penal de nuestro país. No obstante, los avances en las técnicas de investigación utilizadas por el sistema penal, están enmarcadas tanto en la utilización de las normas penales y la utilización de infraestructura institucional para efectivizar su campo de acción. En ese sentido, como parte de la investigación de delitos informáticos, es un desafío lograr estándares altos por las limitaciones estructurales y profesionales, básicamente con la escasez de peritos especializados en informática forense, análisis algorítmico y verificación de contenido digital.	mejora el hecho de que el sistema de justicia ya considera la posibilidad de que se hayan cometido la suplantación con ayuda de la Inteligencia Artificial, por lo que debe ser sancionados.	penal para investigar, probar y sancionar la suplantación de identidad digital mediada por inteligencia artificial. Si bien la norma introduce herramientas punitivas concretas en particular el agravante del artículo 11, numeral 5 de la Ley 30096 y las modificaciones al artículo 46 del Código Penal estas no han venido acompañadas de reformas institucionales que permitan activarlas eficazmente en la práctica. El núcleo del problema radica en que el legislador confió en que el marco normativo sería suficiente por sí solo. Sin embargo, la aplicación del agravante por uso de IA exige que la Fiscalía pueda acreditar técnicamente que el contenido fue generado mediante inteligencia artificial, lo que requiere peritos especializados, laboratorios forenses digitales y protocolos de cadena de custodia diferenciados para contenido sintético. Nada de esto fue implementado. La ley delegó al Poder Ejecutivo la emisión de normativa adicional en sesenta días, pero esa regulación complementaria ha avanzado de forma insuficiente, dejando al sistema penal en la misma posición de impotencia técnica que antes.	la obtención de evidencia digital, la trazabilidad de los autores y la validación técnica de los medios probatorios. La ley no ha venido acompañada de protocolos especializados ni de capacitación suficiente para operadores del sistema, por lo que su impacto real en la investigación y sanción de estos delitos aún es limitado.	conducta cuando se utiliza inteligencia artificial, pero no introduce herramientas procesales ni técnicas para la investigación digital. En consecuencia, el sistema penal continúa enfrentando los mismos problemas que ya existían en los delitos informáticos, como: dificultades para rastrear el origen de contenidos digitales, problemas de jurisdicción cuando los servidores están en el extranjero, limitaciones técnicas en la obtención de evidencia digital. Por ello, aunque la norma aumenta las penas, no mejora de forma real la capacidad investigativa del sistema penal.	operativa (peritos especializados, software de detección de IA, cooperación internacional acelerada) no ha crecido al ritmo de la ley. Investigar una suplantación con IA en Lima sigue dependiendo de la Ley de Delitos Informáticos N°30096, la cual es previa al auge masivo de la Inteligencia Artificial.	su impacto práctico es limitado debido a las dificultades estructurales ante la falta de peritos especializados, toda vez que afectaría las investigaciones ante la falta de infraestructura tecnológica por ser insuficiente, dificultando la obtención de pruebas.	necesarias y básicas para proteger a las víctima de manera integral, contamos con muchas leyes modernizadas, pero muchas veces no se ajustan al contexto peruano normativo y a la realidad problemática, por la falta de equipamientos, recursos y capacitación de las autoridades competentes.
--	---	---	---	--	---	--	--	--	--	---

Tabla 2. Respuesta de entrevistados - Objetivo Especifico 1

Entrevistado Preguntas	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	(E7)	(E8)	(E9)	(E10)
Pregunta 4: ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través de inteligencia artificial?	Uno de los principales aspectos en el ámbito de la evidencia digital, es resaltar que la misma requiere siempre de una preservación adecuada e inmediata, así como la extracción forense sin embargo eso no sucede en razón que en la práctica no se presenta las evidencias de manera adecuada en varias ocasiones inclusive se presentan como evidencias de capturas de pantalla sin una validación adecuada, etc.	Es importante resaltar que los aspectos inoperantes de la normativa señalada radica en la falta de una regulación que identifique los tipos penales más específicamente sobre el ámbito probatorio respecto a los contenidos o delitos generados por el uso de la inteligencia artificial, toda vez que, la ley no explica los criterios técnicos ni los diferencia, ante la falta de recursos tecnológicos no se ajusta a la realidad de las nuevas modalidades en estos delitos ello genera una inseguridad jurídica, ya que los protocolos para establecer la materialidad de este delito es limitado cuando se aborda integralmente en el campo tecnológico de los entornos digitales por lo cual requiere de una adecuación o modificatoria más clara y taxativa de la normativa literalmente.	La falta de regulación detallada, sobre el procesamiento de la evidencia digital, generada mediante inteligencia artificial. La falta de establecer puntualmente los procesos específicos de investigación digital, hace difícil la generar una respuesta de criterios estandarizados en estos casos en sedes tanto fiscales como judiciales.	Como lo vengo sosteniendo, si bien es cierto, la referida ley tiene el mérito de evidenciar la problemática del uso ilícito de la inteligencia artificial, necesariamente, está por sí sola no podría sostenerse, puesto que no existen protocolos, directivas o lo que fuera necesario, para evidenciar en un proceso penal; quiero decir, para valorar contenido sintético y obligaciones para que plataformas o proveedores de IA entreguen registros que permitan identificar al auto. Además, no existen normativas sobre el tratamiento de este dipo de evidencias: cómo se debe seguir la cadena de custodia de evidencias digitales. Todas estas dificultades conllevan a que la defensa pueda cuestionarlos con facilidad y caiga en la impunidad. Dado que serán absueltos por duda razonable.	Los aspectos inoperantes más críticos de la Ley N.º 32314 en materia de evidencia digital son los siguientes. En primer lugar, si bien la norma reconoce el uso de IA como agravante incluyendo referencias a explícitas a deepfakes y tecnologías de manipulación de voz e imagen no establece qué estándares técnicos deben cumplirse para acreditar ese agravante ante el órgano jurisdiccional. Esto genera un vacío probatorio determinante: el fiscal que quiere aplicar el agravante del artículo 11, numeral 5 de la Ley 30096 debe demostrar que el contenido fue creado con IA, pero no existe en el ordenamiento una regulación que defina cómo hacerlo. En segundo lugar, no se han establecido cadenas de custodia específicas para contenidos sintéticos generados por IA, cuya naturaleza difiere sustancialmente de la evidencia digital convencional. Los protocolos actuales no contemplan la preservación de los vectores de generación, los modelos utilizados ni los metadatos de creación propios de sistemas generativos. En tercer lugar, la ausencia de peritos judiciales	Principalmente, la ley no desarrolla criterios claros sobre la obtención, validación y valoración de evidencia digital generada mediante inteligencia artificial. No regula, por ejemplo, cómo acreditar la autenticidad o manipulación de contenidos como deepfakes, ni establece estándares técnicos para su análisis pericial. Esto genera inseguridad jurídica y debilita la carga probatoria en estos casos.	Entre los principales aspectos inoperantes se pueden identificar: Ausencia de regulación específica sobre evidencia digital generada por IA. / Falta de criterios legales para determinar la autenticidad de contenidos manipulados, como deepfakes o audios sintéticos. / Falta de protocolos normativos para el análisis forense digital en casos de inteligencia artificial. / Dependencia de normas generales del proceso penal, que no fueron diseñadas para este tipo de tecnología. Esto provoca que, en muchos casos, la evidencia digital sea cuestionada en juicio por problemas de autenticidad o manipulación.	El principal aspecto es la omisión de estándares de validación para contenido sintético. La ley no establece cómo diferenciar legalmente una identidad real de una identidad sintética (deepfake) para efectos de imputación. Además, hay una inoperancia en la obligación de las plataformas tecnológicas de colaborar en tiempo real, lo que hace que la evidencia se pierda antes de que el fiscal emita la disposición de preservación.	Es primordial resaltar que, ante la falta de una regulación, clara, precisa y detallada respecto al tratamiento de la evidencia digital, todavía no contamos con mecanismos, ni protocolos claros para recolectar, analizar y conservar la inconsistencia en los procesos judiciales y penales, afectando significativamente la validez probatoria, ante la ausencia de un estándar que incremente los riesgos de nulidades por la persecución de este delito nuevo empleándose las nuevas tecnologías. Por tal motivo, se deben incorporar protocolos para el tratamiento jurídico de la evidencia digital.	Uno de los aspectos más relevantes es que no contamos con herramientas que permitan recopilar y resguardar la evidencia digital, por lo cual se puede perder sino se logra reservar a tiempo con mecanismos tecnológicos. Por ejemplo, los ciberdelincuentes se manifiestan por hackers crean bases de datos y luego las eliminar, perseguirlas es insuficiente y casi imposible sino se cuenta con un sistema mejor al que emplean para sus hechos delictivos.

					certificados en análisis forense de IA generativa hace que incluso el material técnico recopilado sea difícil de valorar y sustentar en juicio, restando eficacia real a la norma.					
Pregunta 5: ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?	Una de las dificultades principales es que en la práctica se pierde información cuando no se realiza una preservación inmediata, como, por ejemplo; las direcciones IP, el registro de acceso, los perfiles falsos se pueden eliminar al instante, se debe tener en cuenta igualmente que los metadatos son importantes para determinar la autenticidad de la evidencia. Asimismo, para que la prueba sea válida debe de garantizarse la integridad, autenticidad, etc. en si no existe un protocolo para una evidencia generada por la IA.	Desde el punto de vista técnico, otra de las complicaciones es la falta de intervención tecnológica en lo que comprende a la evidencia digital. Es menester mencionar que muchas veces los contenidos manipulados por medio de la IA pueden suprimirse, cambiar o tener replicas en múltiples servidores en pocos minutos. Por tal motivo, la obtención sería lenta para este compromete en la integridad probatoria. Asimismo, muchas plataformas realizan los denominados cifrados de extremo a extremo, lo cual termina dificultando la recuperación de los metadatos originales, por lo que muchas veces el avance digital supera la capacidad reactiva institucional.	La obtención de evidencia digital en este tipo de acciones punibles, evidencia varias complicaciones técnicas y jurídicas. Una de las principales es la volatilidad de la información digital, ya que muchos contenidos pueden eliminarse o modificarse rápidamente en entornos digitales. Por otro lado, los programas por ejemplo de anonimización y encriptación utilizados en internet hacen difícil identificar plenamente al autor material del este tipo de delitos, lo cual dificulta la atribución de responsabilidad penal individual.	En la demostración de su autenticidad, por su alta facilidad de manipulación, la no existencia de protocolos para el tratamiento de las pruebas indiciarias de índole digital (una correcta cadena de custodia), más que nada por su volatilidad y facilidad de manipulación. Otra dificultad es que estos ilícitos pueden ser cometidos desde el extranjero, por lo cual se dificulta aún más en la obtención de información e identificación de responsables. La insuficiente capacitación del personal del MP.	Las dificultades son tanto de orden técnico como jurídico. En el plano técnico, destaca la volatilidad inherente de la evidencia digital: los archivos de audio o video generados mediante IA pueden ser manipulados o eliminados en fracciones de segundo, y los metadatos que permitirían identificar su origen algorítmico son fácilmente alterables. Más aún, los modelos de IA generativa actuales no siempre dejan trazas identificables que permitan vincular el contenido con un sistema, plataforma o usuario concreto, especialmente cuando se utilizan herramientas de acceso abierto sin registro de usuario. En el ámbito jurídico, el principal obstáculo radica en la ausencia de un marco normativo que obligue a las plataformas tecnológicas a conservar y proporcionar a las autoridades los registros técnicos de generación de contenido. La Ley N.º32314 introduce los agravantes, pero no regula estas obligaciones de colaboración. A	Existen varias dificultades. A nivel técnico, la volatilidad de la evidencia digital y el uso de plataformas extranjeras dificultan su acceso y conservación. A nivel jurídico, hay limitaciones en los mecanismos de cooperación internacional y en la autorización oportuna de medidas como el levantamiento del secreto de las comunicaciones. Además, muchas veces no se cuenta con peritos especializados en inteligencia artificial, lo que afecta la calidad del análisis probatorio.	Las principales dificultades son: La volatilidad de la evidencia digital, ya que los contenidos pueden eliminarse o modificarse rápidamente. / La identificación del autor real del contenido, porque la inteligencia artificial permite generar material sin dejar rastros claros. / La ubicación internacional de los servidores o plataformas, lo que complica la cooperación judicial. / La falta de especialistas en informática forense dentro del sistema de justicia. Estas dificultades afectan la recolección, preservación y valoración de la prueba.	En las dificultades técnicas es la dificultad de rastrear el "prompts" original y la imposibilidad de realizar peritajes de autenticidad sobre archivos que han sido comprimidos por redes sociales (WhatsApp/Telegra m), lo que altera los metadatos. Y en el caso de dificultades jurídicas: El conflicto con la privacidad de datos en el extranjero y la demora en las Cartas Rogatorias o asistencias judiciales internacionales, que no son compatibles con la volatilidad de la IA.	Una de las principales dificultades es la volatilidad información digital y los contenidos que constituyen un obstáculo relevante, referente a contenidos que requieren de una eliminación o modificación con proximidad. Esto implica que los contenidos recolectados tardarían en ser modificados o suprimidos del ciberespacio al comprometer su validez, dificultando su preservación y afectando la trazabilidad de dicha evidencia, siendo necesario fortalecer los mecanismos de cooperación y los sistemas de preservación que tengan inmediatez para la obtención de la evidencia digital.	Una de las dificultades mas relevantes que he identificado en mi experiencia, se basa en que existe un mercado negro que vende información personal y datos de las personas, vulnerando todos los sistemas como por ejemplo, entidades bancarias, RENIEC y demás entidades como ESSALUD y el SIS que todavía tienen acceso a datos personales, así como paginas clandestinas que una vez que detectan su origen desaparecen del ciberespacio, por lo cual el principal problema a tratar son webs, plataformas y sancionar programas o canales como telegram que filtran un banco de información de los usuarios que terminan siendo victimas de estos sujetos delictivos que emplean la tecnología.

					ello se suma la falta de convenios internacionales operativos que permitan acceder expeditamente a servidores ubicados fuera del territorio peruano, donde frecuentemente residen los modelos y los datos más relevantes para la investigación.					
Pregunta 6: Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?	No garantiza plenamente la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas, aunque sí ofrece una base formal importante para su preservación; la cadena de custodia puede garantizar que el archivo presentado en juicio es el mismo que fue recolectado, pero no garantiza por sí sola que su contenido sea autentico.	En términos generales, la cadena de custodia digital vigente no garantiza plenamente la autenticidad de contenidos generados por IA. Si bien existen protocolos para preservación de dispositivos y archivos electrónicos, estos fueron diseñados para evidencia digital convencional. Los deepfakes presentan alteraciones imperceptibles al análisis ordinario. La autenticidad requiere herramientas avanzadas de verificación algorítmica. Sin certificación técnica especializada, la integridad puede ser cuestionada en juicio. La defensa podría alegar manipulación posterior. Esto debilita la eficacia probatoria. Se necesita actualización metodológica urgente.	La cadena de custodia digital, en el ámbito penal, es un instrumento básico para reforzar la integridad, autenticidad de la evidencia electrónica; no obstante, ante contenidos generados por inteligencia artificial, como deepfakes, clonaciones de voz o identidades sintéticas, su eficacia es regular. La principal problemática está en que las formalidades tradicionales de cadena de custodia tuvieron como fin la evidencia digital convencional, estos son: archivos, correos electrónicos, registros de acceso y no para material algorítmicamente alterado, cuya falsedad puede no es fácilmente perceptible por la vista humana.	No, puesto que, ante su gran facilidad de alteración de datos digitales, y la inexistencia de protocolos adecuados para su custodia respetando a Inteligencia Artificial, hacen que la información pueda ser cuestionado fácilmente.	La cadena de custodia digital vigente en el Perú no garantiza, de manera adecuada, la autenticidad e integridad de contenidos sintéticos como deepfakes, clonaciones de voz o identidades generadas por IA. Los protocolos actuales fueron diseñados para evidencia digital convencional registros de acceso, capturas de pantalla, documentos electrónicos y no contemplan las particularidades técnicas de los contenidos generados algorítmicamente. En el caso de un deepfake, la cadena de custodia debería incluir no solo el archivo de video, sino el análisis forense del modelo de IA utilizado para su generación, los artefactos audiovisuales característicos del sistema generativo empleado y los metadatos de creación. La Ley N.º 32314 reconoce el deepfake como medio comisivo relevante, pero no establece protocolos específicos para su preservación e incorporación al proceso. En consecuencia, la	Considero que no de manera suficiente. La cadena de custodia tradicional no está plenamente adaptada a la complejidad de la evidencia digital generada por IA. Si bien existen protocolos generales, estos no contemplan adecuadamente los riesgos de alteración, replicación o manipulación de este tipo de contenidos, lo que puede comprometer su valor probatorio en el proceso penal.	Actualmente, la cadena de custodia digital no siempre garantiza plenamente la autenticidad de este tipo de contenidos, debido a que las herramientas de inteligencia artificial permiten alterar o generar información con gran realismo. Si bien el proceso penal exige asegurar la integridad de la evidencia, no existen protocolos especializados para contenidos generados por inteligencia artificial, lo que puede generar cuestionamientos sobre su origen o manipulación.	No en su totalidad. La cadena de custodia tradicional (actas de visualización y lacrado) garantiza que el archivo no fue modificado después de su recojo, pero no puede certificar si el origen del archivo es humano o artificial. Se requieren pericias de análisis forense digital avanzado (detección de artefactos algorítmicos) que actualmente no forman parte del estándar básico de la cadena de custodia en las fiscalías corporativas de Lima.	Desde mi punto de vista, bajo un criterio analítico es relevante indicar que los deepfakes y tecnologías similares desafían los métodos comunes para validarlos, dicha cadena de custodia no garantiza eficientemente la integridad de todos los contenidos en lo que respecta a la credibilidad del proceso, por lo que se necesita una actualización y gestión pública adecuada para modernizar esta cadena implementando tecnologías de verificación digital.	Esta pregunta es ambigua, dado que mientras exista gente que consuma estos mercados clandestinos, los delitos no cesaran y la integridad de las víctimas se verá cada vez más vulnerable ante la falta de protección y garantía estatal para perseguir estas organizaciones criminales

					evidencia de este tipo puede ser fácilmente impugnada en juicio, convirtiendo la cadena de custodia digital en uno de los eslabones más débiles del sistema penal frente a los delitos cometidos mediante IA.					
--	--	--	--	--	---	--	--	--	--	--

Tabla 3. Respuesta de entrevistados - Objetivo Especifico 2

Entrevistados Preguntas	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	(E7)	(E8)	(E9)	(E10)
Pregunta 7: ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?	La inoperancia puede probarse por medio de un análisis entre la finalidad declarativa de la norma y sus efectos son de carácter prácticos en casos concretos, pese a tener una normativa vigente como la Ley N.º 32314, existen dificultades al momento de sancionar de forma efectiva este tipo de conductas en casos como la suplantación de identidad mediante el uso de la inteligencia artificial siendo una brecha entre la regulación y realidad para que sea una ley eficiente. Asimismo, tengo que resaltar que ante la ausencia de herramientas técnicas obligatorias se demuestra insuficiencia probatoria. Por tal motivo, si el sistema no garantiza prevención, ni reparación, resulta siendo insuficiente y limitada para estos delitos.	La inoperancia puede probarse mediante un análisis comparativo entre la finalidad declarativa de la norma y sus efectos prácticos en casos concretos. Si, pese a la vigencia de la Ley N.º 32314, persisten dificultades para sancionar eficazmente conductas de suplantación con IA, se evidencia una brecha entre regulación y eficacia real. Asimismo, la ausencia de herramientas técnicas obligatorias para la protección de datos biométricos demuestra insuficiencia normativa. La autodeterminación informativa implica control sobre los propios datos. Si el sistema no garantiza prevención ni reparación efectiva, la ley resulta funcionalmente limitada. La prueba puede sustentarse en jurisprudencia incipiente y estadísticas fiscales. También en informes técnicos sobre limitaciones periciales. Todo ello revela	Los defectos de Ley N.º 32314 logran evidenciar que pese a integrar la inteligencia artificial como factor de agravación en delitos específicos, no profundizan en técnicas suficientes de tutela efectiva ante la lesión del derecho fundamental, entendido como la facultad que tiene toda persona de controlar el uso, circulación y tratamiento de sus datos personales. Asimismo, la ley no instaure métodos inmediatos de neutralización tecnológica, como bloqueo urgente de contenidos, inmovilización digital, lo que revela una brecha entre sanción penal posterior y protección real del derecho afectado.	La inoperancia puede tener probanza por medio del análisis comparativo nacional e internacional, sin embargo, existen dificultades para sancionar eficazmente acciones que no pueden perseguirse por los avances tecnológicos ante la ausencia de herramientas tecnológicas de protección de datos por medio de la IA, lo cual ante el estudio estadístico podría dar un estimado del incremento de estos delitos perpetrados así como informes técnicos y capacitaciones internacionales para abordar como vienen combatiendo y trabajando otros países esta problemática.	La inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa puede demostrarse a través de un análisis estructural de sus propias limitaciones normativas. La ley incorpora la IA como agravante en el artículo 46 del Código Penal y en el artículo 11 de la Ley 30096, pero no establece mecanismos sustantivos de protección del derecho a la autodeterminación informativa cuando los datos biométricos de una persona son usados sin consentimiento para entrenar un modelo de suplantación. Este vacío es significativo y puede acreditarse a través del contraste entre el texto legal y la doctrina del Tribunal Constitucional peruano sobre autodeterminación informativa. Adicionalmente, la inoperancia se demuestra mediante el análisis estadístico de expedientes fiscales en Lima, que evidencia altas tasas de archivamiento en casos de suplantación	La inoperancia puede evidenciarse a partir de casos concretos donde, pese a existir una afectación clara a la identidad digital de la víctima, no se logra una respuesta penal eficaz. Esto se observa en la dificultad para tipificar adecuadamente la conducta, la limitada protección de los datos personales y la ausencia de medidas oportunas para frenar la difusión del contenido manipulado. En la práctica, la norma no garantiza una tutela efectiva del derecho a la autodeterminación informativa.	La inoperancia puede demostrarse observando que la ley: no regula de manera específica la protección de la identidad digital, no establece mecanismos claros para la prevención de suplantaciones mediante IA, no desarrolla instrumentos para proteger la autodeterminación informativa de las personas. Por ello, cuando se produce una suplantación digital, la respuesta penal suele llegar de forma tardía, cuando el daño a la identidad o reputación de la víctima ya se ha producido.	Se prueba mediante la tasa de reincidencia y victimización. Cuando un ciudadano ve su rostro o voz suplantados por IA y la autoridad no puede retirar dicho contenido de la red ni sancionar al responsable debido a vacíos en la Ley 32314, el derecho a controlar la propia información (autodeterminación) queda anulado. La inoperancia se refleja en la falta de "tutela correctiva" inmediata.	En el caso de probar la inoperancia, se puede advertir que existe una gran brecha entre lo penal y la protección efectiva de los derechos fundamentales cuando se trata de uso de tecnologías ante la ausencia de contención. Es menester indicar que, la ley no puede cumplir con su funcionalidad protectora al no contar con mecanismos óptimos para su ejecución y aplicación con recursos que permitan garantizarlo, por lo que se debe adecuar medidas cautelar digitales de carácter inmediato, citando por ejemplo bloqueos, alertas y eliminación de contenidos delictivos generados por la IA	Para probar la inoperancia se puede evidenciar que la falta de mecanismos inmediatos y preventivos no prioriza la sanción ni persecución del delito posterior al hecho por la falta de herramientas tecnológicas y sistemas operativos que se adecuen a estas nuevas tendencias digitales como la IA, por lo cual se genera una desprotección y tutela insuficiente.

		ineficacia estructural.			digital por insuficiencia probatoria, precisamente porque el agravante del uso de IA no puede ser acreditado técnicamente. La norma declara proteger la autodeterminación informativa al sancionar la suplantación, pero carece de los instrumentos procesales y técnicos que harían esa protección efectiva frente a los sistemas de IA generativa.					
Pregunta 8: ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.	Implica la protección efectiva de la identidad, datos y entornos digitales frente a accesos indebidos, manipulación o suplantación. La Ley 32314 modifica el Código Penal, pero no establece mecanismos preventivos de protección de datos, no desarrolla herramientas específicas para restitución de identidad digital, y contempla reparación integral especializada para víctimas de deepfake o clonación de voz.	La Ley N.º 32314 protege la autodeterminación informativa de manera indirecta, al tipificar conductas relacionadas con la suplantación de identidad. No obstante, su enfoque es predominantemente penal y reactivo. La protección del dato personal frente a manipulación algorítmica exige mecanismos preventivos y técnicos que la norma no desarrolla expresamente. No se establecen obligaciones específicas sobre tratamiento automatizado de datos biométricos. Tampoco se regulan medidas de seguridad diferenciadas para entornos de IA generativa. Por tanto, la tutela resulta parcial. La norma sanciona el resultado, pero no regula adecuadamente el riesgo tecnológico previo. Existe un vacío en protección integral.	La protección es actualmente parcial, toda vez que si bien identifica riesgo penal determinado por el uso de inteligencia artificial; no obstante, omite la incorporación de una tutela integral, direccionada puntualmente a controlar el dato personal distorsionado algorítmicamente.	Básicamente que la regulación no es sufriente para proteger la autodeterminación informativa ni garantizar la seguridad digital, frente a ilícitos cometidos por IA, dado que la ley no especifica cuando se debe considerar que es un hecho ilícito. Además, no existen protocolos especializados de cadena de custodia que garanticen la autenticidad de los datos obtenidos que tienen el carácter de prueba. En conclusión, es insuficiente las herramientas con los que se cuenta para la persecución de este tipo de delitos.	La protección que brinda la Ley N.º 32314 al derecho a la autodeterminación informativa es muy limitada y parcial. La norma sanciona agravadamente la suplantación de identidad realizada mediante IA, pero no aborda el ciclo completo de la vulneración: no regula la recolección ni el uso no consentido de datos biométricos para el entrenamiento de modelos de IA destinados a la suplantación, ni establece la prohibición expresa de desarrollar, comercializar o distribuir sistemas de IA diseñados específicamente para suplantar identidades. En materia de protección de datos personales en contextos de manipulación algorítmica, la ley tampoco incorpora mecanismos eficaces. No prevé el derecho a la eliminación de modelos entrenados con datos personales ilícitamente, ni	La protección es aún limitada. Si bien la ley reconoce la relevancia de los datos personales, no incorpora mecanismos específicos para enfrentar escenarios de manipulación algorítmica, como el uso de IA para recrear identidades o alterar contenidos. Tampoco establece obligaciones claras para plataformas digitales ni protocolos de respuesta rápida frente a la vulneración de datos, por lo que la tutela del derecho a la autodeterminación informativa resulta insuficiente.	La protección es limitada. La Ley N.º 32314 se centra principalmente en agravar las penas cuando se utiliza inteligencia artificial para cometer delitos, pero no desarrolla mecanismos específicos de protección de datos personales ni medidas preventivas frente a la manipulación algorítmica. En ese sentido, la protección del derecho a la autodeterminación informativa sigue dependiendo principalmente de otras normas, como la legislación sobre protección de datos personales.	La protección es nominal. La norma menciona el respeto a los derechos fundamentales, pero no incorpora mecanismos de "bloqueo preventivo" o "derecho al olvido" automatizado cuando se detecta una manipulación algorítmica. Sin una articulación real con la Autoridad Nacional de Protección de Datos Personales (ANPD), la Ley 32314 es un saludo a la bandera en términos de protección de datos.	Para esta interrogante es importante señalar que la medida en la normativa se manifiesta ante el derecho a la autodeterminación es escasa, toda vez que, no articula un enfoque de carácter garantista e integral, si bien es cierto no todas las normas pueden ser garantistas por las implicancias que se presentan en su interpretación, empero en los casos de protección de datos personales, no se cuentan con herramientas óptimas para ejercer un control del uso ilícito e indebido de estos datos, en donde no solo se afecta la seguridad digital sino también la integridad psicológica de las víctimas, resulta siendo limitada. Es necesario integrar a la normativa penal una regulación más protectora de datos personales.	Considero que no se garantiza ni protege el derecho a la autodeterminación informativa frente a estos delitos modernizados por la IA, debido a que la protección de datos personales es vulnerable en la actualidad y no se puede probar la conducta delictiva ante la ausencia de tecnologías optimizadas a estos nuevos delitos.

					establece obligaciones de transparencia algorítmica para los proveedores de tecnología. En ese sentido, la norma se limita a sancionar el resultado delictivo la suplantación consumada, pero deja desprotegido el proceso previo de captura y procesamiento de datos personales que hace posible esa suplantación, que es precisamente donde reside la vulneración a la autodeterminación informativa.					
Pregunta 9: ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?	La falta de una regulación específica y sistemática sobre seguridad digital sí puede contribuir a la revictimización de las personas afectadas.	Sí, la ausencia de regulación específica en materia de seguridad digital puede generar revictimización. Cuando el ordenamiento no establece mecanismos de protección inmediata, la víctima permanece expuesta a la circulación continua del contenido manipulado. En casos de deepfakes o clonaciones de identidad, la difusión masiva amplifica el daño. La falta de protocolos claros de eliminación rápida prolonga la afectación. Además, la demora en investigaciones incrementa la incertidumbre jurídica. Esto impacta en la dignidad y reputación de la persona. La revictimización se produce por omisión normativa. La protección debe ser preventiva y no meramente reactiva.	Sí, porque en delitos cometidos mediante inteligencia artificial el daño no termina con la acción inicial, sino que se amplifica en cuanto el contenido permanezca accesible, replicable o redistribuible digitalmente. La revictimización sucede cuando continua la exposición de la víctima a nuevas reproducciones del contenido ilícito, comentarios en redes sociales, el menoscabo de la reputación, lo cual conlleva a la afectación emocional prolongada, inclusive durante el trámite judicial. En base a la teoría del daño penal, esta circunstancia constituye una lesión dinámica y expansiva, diferente al delito base de resultado instantáneo, toda vez que el perjuicio a la parte agraviada se reactualiza cada vez que el contenido vuelve a circular.	Por supuesto que sí, dado que no se ejerce adecuadamente el derecho a la efectiva tutela jurisdiccional, que conllevan a la contravención de los derechos de la víctima, como es el derecho a saber la verdad y el derecho a la justicia.	La ausencia de regulación específica sobre seguridad digital en el contexto de la suplantación de identidad por IA genera un ciclo de revictimización que opera en múltiples niveles. A nivel normativo, aunque la Ley N.º 32314 sanciona la conducta, no establece vías expeditas para que la víctima solicite la eliminación inmediata del contenido sintético que la suplanta, ni obliga a los intermediarios digitales a actuar de forma preventiva. A nivel procesal, la víctima carga con la dificultad práctica de probar que el contenido fue generado mediante IA para activar el agravante, lo que supone una carga técnica desproporcionada. A nivel social, la prolongación del daño reputacional derivado de la circulación continua del contenido falso durante toda la duración del	Sí, definitivamente. La falta de regulación específica permite que el contenido manipulado continúe circulando sin control, prolongando el daño a la víctima. Además, la ausencia de mecanismos rápidos de eliminación y de protección efectiva de su identidad genera una exposición constante, lo que agrava la afectación psicológica y social. En ese sentido, la deficiencia normativa contribuye directamente a la revictimización.	Sí. La falta de regulación específica provoca que las víctimas enfrenten dificultades para: denunciar los hechos, demostrar la manipulación digital, lograr la eliminación rápida del contenido falso. En muchos casos, el material manipulado continúa circulando en internet, lo que prolonga el daño a la reputación, identidad o privacidad de la víctima, generando una forma de revictimización.	Definitivamente. La víctima de suplantación por IA no solo sufre el daño original, sino que debe enfrentar un sistema judicial que cuestiona la veracidad de su denuncia por "falta de pruebas tecnológicas". Al no haber protocolos de atención rápida para delitos cometidos con IA, la exposición del contenido dañino se prolonga, agravando el daño moral y psicológico.	Considero que la falta de una regulación específica genera un impacto en el contenido digital para poder perseguir este delito, dado que una nueva difusión rechazaría el daño y afectaría la reputación y estabilidad emocional, toda vez que, no cuenta con mecanismos de protección, por lo que la víctima sufre reiteradamente de estos hechos y delitos, debiendo establecerse mecanismos legales para eliminar de forma obligatoria su desindexación de los contenidos fraudulentos.	Creo que las leyes no deben modificarse planamente, ya que generan un impacto que repercute en la eficacia legal de las normas respecto a su aplicación en el ámbito en el que se desean abordar, por no ajustarse a la realidad actual y podría generar repercusión o confusión al revictimizar a las víctimas usando desproporcionalmente las entidades.

					proceso penal constituye una forma de revictimización sistémica que la norma no mitiga. La ley no contempla medidas cautelares específicas de retirada urgente de contenido generado por IA, ni reparaciones integrales diferenciadas para este tipo de daños. En consecuencia, existe una relación causal directa entre la insuficiencia regulatoria en materia de seguridad digital y la revictimización de los afectados.					
--	--	--	--	--	--	--	--	--	--	--

Tabla 4. Respuesta de entrevistados - Objetivo Específico 3

Entrevistados Preguntas	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	(E7)	(E8)	(E9)	(E10)
Pregunta 10: ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?	Puede afectar la correcta tipificación práctica cuando el delito se comete mediante inteligencia artificial.	La inoperancia incide en la falta de claridad respecto al elemento subjetivo del tipo, particularmente en la determinación del dolo cuando intervienen sistemas automatizados. La norma no precisa si basta la creación del contenido falso o si se requiere un propósito específico de daño. Esta ambigüedad afecta la seguridad jurídica y genera interpretaciones dispares. Ello repercute en la predictibilidad de la sanción penal.	La inoperancia normativa impacta porque diversas acciones de inteligencia artificial no se encuentran enmarcadas en sistemas típicos tradicionales en lo penal.	Nuestro Derecho Penal es básicamente probatorio, en tal sentido, el persecutor del delito debe llegar a la etapa de enjuiciamiento con suficientes elementos probatorios que puedan dotar de credibilidad su teoría del caso. No obstante, en el presente caso se tiene la gran dificultad de que los delitos de suplantación de identidad por Inteligencia de Identidad, deben ser encajados en tipos penales tradicionales, que, desde luego, dificultan en la acreditación de los elementos típicos del tipo penal en específico. Y, la dificultad por falta de protocolos, que permitan validar evidencias digitales provenientes de IA.	La inoperancia de la Ley N.º 32314 tiene impacto concreto en la tipificación penal del delito de suplantación de identidad mediado por IA. El esquema normativo actual construye el delito en dos capas: el tipo base del artículo 9 de la Ley N.º 30096 — que sanciona la suplantación mediante "tecnologías digitales" con penas de 3 a 5 años— y el agravante del artículo 11, numeral 5 de la misma ley, incorporado por la Ley 32314, que eleva la pena hasta en un tercio cuando se emplea IA. El problema de tipificación surge precisamente en la articulación entre ambas capas. Para aplicar el agravante, el fiscal debe acreditar que la suplantación fue realizada mediante	Afecta de manera directa, porque al no contemplar de forma expresa las modalidades de suplantación mediante inteligencia artificial, se generan vacíos en la tipificación. Esto obliga a forzar la subsunción en tipos penales tradicionales que no fueron diseñados para estas conductas, lo que debilita la imputación y puede afectar la solidez del caso en sede fiscal y judicial.	La inoperancia afecta la tipificación porque la ley no define de manera clara la conducta de suplantación mediante inteligencia artificial. Por ello, los fiscales suelen recurrir a tipos penales generales como: suplantación de identidad, informática, estafa, difamación, delitos contra la fe pública. Esto puede generar problemas de subsunción típica, ya que no siempre es fácil encajar estas nuevas conductas tecnológicas dentro de tipos tradicionales.	Genera atipicidad relativa o errores de subsunción. Al no existir una agravante específica o un tipo penal que describa el uso de "tecnologías de generación sintética", los fiscales fuerzan el Art. 9 de la Ley 30096. Esto permite que los abogados defensores aleguen vulneración al principio de taxatividad, logrando que muchas conductas queden sin sanción por no ajustarse exactamente al verbo rector tradicional.	Las nuevas formas o modalidades delictivas superan los esquemas clásicos del derecho penal en la normativa no logra abarcar estas conductas, limitando la persecución de este delito frente a la falta de capacitación que enfrentan los operadores al no lograr abarcar estas conductas, generando una carente eficacia al sistema, siendo necesario crear tipos penales específicos de delitos enfocados en IA.	La falta de regulación permite la persistencia de un daño generado en un entorno digital ante un contenido ilícito, exponiendo reiteradamente a las víctimas, ante una afectación prolongada en los casos donde el tipo penal no es claro con respecto a los agravantes por IA y suplantación de identidad.

					IA y no por otros medios digitales. Esto genera una distinción procesal que el sistema penal actual no está en condiciones de resolver técnicamente. Cuando no puede probarse el medio de comisión específico, el caso se procesa solo bajo el tipo base del artículo 9, sin el agravante, lo que subvalora jurídicamente la gravedad real de la conducta. Esta brecha entre la calificación jurídica posible y la calificación jurídica efectiva es en sí misma una manifestación de inoperancia, pues la norma prevé una respuesta diferenciada que la práctica no puede implementar.					
Pregunta 11: ¿Considera que el artículo 9 de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? ¿Explique, si existen vacíos normativos en la actual tipificación penal?	Considero que existe un vacío normativo respecto a la manipulación de datos biométricos, ya sea voz o imagen mediante el uso de algoritmos que sean avanzados, debido a que si no se sienten peritos y pruebas digitales idóneas, sería peligroso atribuirle un conducta delictiva a una persona y difícil demostrar la autoría o coautoría, en la actualidad la norma ha sido concebida dentro de un contexto tecnológico complejo y distinto a la realidad tecnológica de las unidades de investigación, sin prever la	El artículo 9 de la Ley N.º 30096 establece una tipificación orientada a la suplantación informática, pero no contempla expresamente la utilización de inteligencia artificial generativa. Aunque podría aplicarse por interpretación sistemática, su redacción no describe con precisión las nuevas modalidades tecnológicas. Esto genera dudas en la adecuación típica cuando se emplean herramientas automatizadas. Por tanto, la subsunción no siempre resulta clara ni uniforme.	Ley N.º 30096 pone a disposición una base normativa relevante; no obstante, el artículo 9 no determina en un ámbito totalitario los supuestos de suplantación mediante inteligencia artificial generativa. La dificultad estriba en que el tipo fue generado para la usurpación digital convencional, no para creación algorítmica de identidades. Por ejemplo, cuando existe clonación de voz, rostro o comportamiento digital, en estos casos la conducta excede los conceptos tradicionales de suplantación simple.	No, porque el artículo 207-A (derogado por la ley 30096), porque esta fue diseñada para conductas tradicionales de falsificación, mas no para técnicas como deepfakes, clonación de voz o identidades sintéticas. En tal sentido, como la suplantación es realizada por la IA, resulta inconsistente adecuarlo en los elementos del tipo penal.	El artículo 9 de la Ley N.º 30096, en su texto vigente modificado por el Decreto Legislativo 1591 de diciembre de 2023, sanciona al que "mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole," con penas de 3 a 5 años. El término "tecnologías digitales" es suficientemente amplio para cubrir el uso de sistemas de IA generativa, por lo que, en principio, existe base típica. Sin embargo, la subsunción no resulta clara cuando la suplantación se realiza mediante IA porque subsisten vacíos normativos	Considero que no permite una subsunción totalmente clara. El artículo 9º regula la suplantación de identidad en entornos digitales, pero no prevé específicamente el uso de inteligencia artificial como medio comisivo. Esto genera vacíos normativos, especialmente en supuestos donde no hay acceso indebido directo a sistemas, sino creación de identidades sintéticas o contenidos falsificados, lo que dificulta encuadrar la conducta de manera precisa, aunado a ello no existe circunstancias agravantes específicas como por ejemplo si los perpetradores son miembros de una banda u organización criminal.	El artículo 9º de la Ley N.º 30096 regula la suplantación de identidad en entornos informáticos, lo que permite sancionar a quien se hace pasar por otra persona utilizando medios digitales. Sin embargo, cuando la suplantación se realiza mediante herramientas avanzadas de inteligencia artificial, como deepfakes o clonación de voz, la subsunción no siempre resulta clara, porque la norma fue diseñada para formas más tradicionales de suplantación digital. Por ello, pueden presentarse vacíos normativos cuando la conducta implica manipulación audiovisual avanzada o generación	No es clara. El Art. 9º sanciona a quien "mediante el uso de tecnologías de la información... suplanta la identidad". Sin embargo, la IA permite crear identidades "híbridas" o "sintéticas" que no necesariamente pertenecen a una persona natural viva, o que distorsionan la voluntad de una persona real de formas que la ley no previó en 2013. Existe un vacío en la determinación de la lesividad cuando el daño es puramente algorítmico.	Considero que el tipo penal responde a escenarios tradicionales o comunes de la práctica y ejercicio de estos delitos, más no incorpora supuestos en casos de manipulación algorítmica, dificultando la subsunción típica para su identificación y agravantes, la normativa actual resulta siendo desactualiza ante los estándares tecnológicos para proteger integralmente a las víctimas y perseguir estos delitos, por lo cual se requiere una respuesta a la falta de protocolos y mecanismos, siendo relevante realizar una adecuación a la normativa que sea más específica, agregando supuestos de suplantación por medio del empleo de la IA.	La inoperancia legal genera un impacto en la adecuación típica referida a conductas, donde muchas veces las acciones no encajan al tipo penal común o antiguo, generando vacíos legales en la imputación penal por la existencia de inseguridad jurídica en lo que respecta a la nueva era digital.

	sofisticación en el marco de la realidad peruana, la cual es muy distinta a países como China, Alemania y España sobre los sistemas de simulación digital, ante la falta expresa de medios tecnológicos, generando graves controversias interpretativas, evidenciándose una latente necesidad de actualización legislativa pero equiparable a los sistemas tecnológicos y operativos.				relevantes. En primer lugar, el tipo exige que "resulte algún perjuicio", lo que plantea dificultades cuando el daño es difuso, latente o difícil de cuantificar en sus primeras manifestaciones. En segundo lugar, la IA como medio comisivo calificado solo aparece en el artículo 11, numeral 5, como agravante, no en el tipo base, lo que genera un problema dogmático: si el agravante exige probar el uso de la IA, pero el tipo base no lo requiere, la imputación puede descansar en el tipo más general, perdiendo la especificidad normativa que la Ley 32314 pretendía aportar. Esta doble estructura crea zonas de ambigüedad que impactan negativamente en la predictibilidad de la respuesta penal.		automática de identidades.			
Pregunta 12: Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?	Desde el enfoque de la dogmática, el principio de legalidad está habilitado, efectivamente el cuerpo normativo de la Ley 32314, si cumpliría este requisito, pues tipifica la utilización de inteligencia artificial como agravante en conductas delictivas como la suplantación de identidad, sin embargo, en la práctica los sistemas operativos, todavía no se encuentran actualizados y	Desde la dogmática penal, el principio de legalidad exige que la conducta prohibida esté descrita de manera clara y previa. Si la Ley N.º 32314 emplea conceptos abiertos o indeterminados respecto a tecnologías emergentes, podría vulnerar la exigencia de taxatividad. La falta de precisión semántica genera inseguridad jurídica. En consecuencia, el respeto al principio dependerá de la claridad de su redacción normativa.	Dogmáticamente, la ley constituye un progreso, pero mantiene confrontaciones con el principio de taxatividad penal. La inteligencia artificial es tipificada como medio agravante; sin embargo, en algunos casos no enmarcan conceptos de manera suficiente, motivo por el cual se generan una situación jurídica de incertidumbre al momento de la interpretación en torno a qué tecnología en específico, activa	Considero que aún no, dado que para que los operadores de justicia puedan hacer uso de los preceptos normativos, evidentemente, estos deben ser claro y precisos, La Ley en mención, no permite la consolidación del principio de legalidad, por la ausencia de sustento normativo que la contenga respecto a qué es precisamente lo que se está prohibiendo, y a quienes se les debe considerar como	Desde una perspectiva dogmática, la Ley N.º 32314 presenta tensiones con los principios de legalidad y taxatividad penal, aunque su análisis requiere matices. La norma introduce la expresión "inteligencia artificial o tecnologías similares" tanto en el artículo 46 del Código Penal como en el artículo 11 de la Ley 30096. Si bien esta formulación representa un avance frente a la omisión total previa, el término	Desde una perspectiva dogmática, su cumplimiento es parcial. Si bien la ley busca adecuarse a nuevas formas de criminalidad, presenta problemas de indeterminación en la descripción de conductas vinculadas a tecnologías emergentes como la inteligencia artificial. Esto puede generar interpretaciones amplias o ambiguas, lo que tensiona el principio de taxatividad y puede afectar la seguridad jurídica en la aplicación del derecho penal.	En términos generales, sí respeta el principio de legalidad, ya que no crea delitos indeterminados ni ambiguos, sino que incorpora el uso de inteligencia artificial como medio agravante en delitos ya existentes. No obstante, desde una perspectiva dogmática, puede cuestionarse su grado de taxatividad, porque la norma utiliza conceptos amplios como “inteligencia artificial o tecnologías similares”, lo que podría generar	La Ley 32314 es demasiado ambigua. El principio de taxatividad exige que la conducta prohibida esté descrita de forma precisa. Al ser una norma de carácter general sobre IA, su aplicación al ámbito penal es problemática porque delega mucha interpretación al juez, lo cual podría colisionar con el principio de legalidad si se intenta sancionar analogando comportamientos tecnológicos nuevos a tipos penales antiguos.	Desde el ámbito de la literatura, jurisprudencia y dogmática así como la doctrina, existe una falta de claridad limitada en la previsibilidad normativa para tratar jurídicamente estos delitos, al no establecer parámetros definidos al caso en concreto y la realidad jurídica peruana, afectando directamente la seguridad jurídica y digital para las personas ante la falta de protección y prevención normativa a estas nuevas tendencias en delitos tecnológicos, debilitando la	Desde una perspectiva dogmática la ley proporciona si bien una base normativa relevante, no obstante; no contempla adecuadamente la inteligencia artificial en sus modalidades, siendo su alcance limitado.

	modernizados para su calificación e interpretación por carecer de renovación, termina siendo obsoleto. Además, tener presente que contar con sistemas de alta tecnología tiene un costo elevado lo cual preciso dentro del presupuesto termina siendo escaso ante la falta de inversión pública. Por otro lado, la taxatividad exige que la conducta delictiva esté definida con precisión suficiente para que el ciudadano y el juez puedan reconocerla y aplicarla por lo cual desde mi opinión y experiencia terminaría siendo una ley inoperable “letra muerta” comúnmente denominado, existe en esencia la ley, pero no se puede ejecutar porque no se cuenta con lo básico y necesario.		la agravación penal.	responsables. Y de qué manera se puede determinar que un hecho debe responder penalmente. Por lo que, esta falta de especificad hace imposible la manifestación y del principio de taxatividad. Por lo que la Ley 32314 no garantiza estándares dogmáticos plenos de certeza, previsibilidad y restricción del ius puniendi en el ámbito de los delitos tecnológicos.	"tecnologías similares o análogas" carece de un contenido técnico-jurídico suficientemente preciso para satisfacer la exigencia de taxatividad que el principio de legalidad impone El operador jurídico se enfrenta a la pregunta: ¿qué tecnología es "análoga" a la inteligencia artificial a efectos penales? La norma no lo define, y el Poder Ejecutivo tampoco ha emitido hasta la fecha la reglamentación complementaria que la propia ley le encargó producir en sesenta días. Este déficit definitorio no solo afecta la seguridad jurídica del ciudadano, sino que coloca al juez en la posición de tener que realizar interpretaciones extensivas para aplicar el agravante, con el consiguiente riesgo de vulnerar la prohibición de analogía in malam partem. En ese sentido, si bien la ley cumple formalmente con mencionar a la IA, no satisface plenamente el mandato de determinación que el principio de taxatividad exige para los agravantes penales.		interpretaciones diversas en la aplicación práctica. Por ello, aunque la ley es válida desde el punto de vista del principio de legalidad, aún requiere mayor precisión normativa para enfrentar adecuadamente los delitos tecnológicos.		legalidad, siendo necesario desarrollar definiciones, protocolos y herramientas para el uso de la IA en el ámbito penal.	
--	--	--	-----------------------------	--	---	--	---	--	---	--

3.1. Análisis de resultados de entrevista

Tabla de análisis de los resultados relacionados al Objetivo General

Entrevistados Preguntas	Análisis e interpretación de las respuestas de los entrevistados (E1 – E10)
Pregunta 1: ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?	La inoperancia de la Ley desarrollada evidencia una brecha real entre la normativa y la práctica para aplicar la ley ante los delitos cometidos por intermedio de la inteligencia artificial. Los entrevistados coinciden en que la normativa no incorpora definiciones de carácter técnico específicos ni protocolos para la investigación de estos delitos, siendo dificultoso determinar el tipo penal y acreditar que el sujeto delictivo empleó el uso de la IA para la perpetración del delito, advirtiéndose una insuficiencia probatoria y falta de capacitación especializada tanto para la PNP como el Ministerio Público por carecer de laboratorios forenses digitales y herramientas tecnológicas optimizadas a estas nuevas modalidades, por lo que resulta formalmente limitada para el trabajo del cibercrimen o ciberdelincuencia. Al mismo tiempo, han coincidido que la normativa termina siendo inoperativa por la falta de actualización de los sistemas especializados para la persecución de estos delitos.
Pregunta 2: Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.	En esta interrogante, los especialistas reiteran y coinciden en que el cuerpo normativo vigente actualizado genera un avance para el uso de la IA, sin embargo, el elemento agravante para la configuración de estos delitos resulta complejo para combatir la criminalidad digital, las cuales adoptan un enfoque punitivo sin incorporar mecanismos o herramientas de carácter preventivo así como políticas de ciberseguridad mediante cooperación internacional en el ámbito tecnológico lo cual adolece de reforzamiento ante la ausencia de peritos competentes para estos delitos ser examinados y resulta de alguna forma siendo en la práctica ineficaz por no contar con sistemas operativos actualizados pero si un marco legal lo cual evidencia una falta de integración dentro de las estrategias tecnológicas por la falta de capacitación. En ese contexto, han desarrollado cada entrevistado que la ley responde axiológicamente a un problema, pero técnicamente no lo resuelve por las implicancias tecnológicas.
Pregunta 3: ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?	Los entrevistados indicaron según su análisis de las preguntas basándose en la Ley N.º 32314, la cual indica que no ha generado una mejora en la capacidad del sistema operativo dentro del marco del sistema penal para poder investigar y sancionar rigurosamente los tipos penales de estos delitos generados mediante los recursos tecnológicos como la IA, ante la falta de personal y recursos para aplicar supletoriamente el marco legal por la limitada posibilidad de evidenciar los orígenes algorítmicos en contenidos digitalizados por parte de los operadores de justicia para contrarrestar y prevenir estos casos en la preservación de la evidencia digital y mejora del sistema digital por lo cual resulta siendo un desafío tecnológico actual. Finalmente, como han indicado los entrevistado, si bien la ley mejora la estructura legal, no optimiza una modernización de la gestión pública para estos nuevos cambios tecnológicos y carece de falta de capacitación internacional,

Tabla de análisis de los resultados relacionados al Objetivo Especifico 1

Entrevistados Preguntas	Análisis e interpretación de las respuestas de los entrevistados (E1 – E10)
Pregunta 4: ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?	Para esta interrogante los entrevistados identificaron distintos aspectos que limitan la operatividad de la normativa en casos de la evidencia digital, donde uno de ellos es la ausencia de protocolos específicos para la obtención de la información en estos delitos por medio de entornos digitales como herramientas tecnológicas como la IA, lo cual debilita el ámbito probatorio y muchas veces influye en el análisis de los contenidos generados por lo que estas limitaciones generan determinada inseguridad y permiten que exista carencia de validez en la prueba digital. Para los entrevistados de manera general, la falta de una adecuación normativa a los agravantes y recursos tecnológicos sin implementar y modernizar limita la posibilidad de calidad de la atención de las entidades para combatir estos delitos.
Pregunta 5: ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?	Bajo esa misma directriz, los especialistas han coincidido en que una de las principales dificultades se traslada en la naturaleza volátil de la evidencia digital, ello genera que si no se detecta a tiempo puede ser eliminada o modificada lo cual podría replicarse en los ciberespacios rápidamente por distintos servidores, además podría ser manipulado por otros usuarios y al final sería complejo determinar si dicha huella digital algorítmica pertenece al sujeto principal o fue transferida otro desde su origen, lo cual las plataformas digitales muchas veces distribuyen los registros que se almacenan mediante cifrados de extremo a extremo siendo difícil identificar la información principal de la fuente primigenia, afectando y generando un obstáculo para garantizar la autenticidad y validez de dicha prueba en un proceso penal. Una de las dificultades resaltadas por todos los entrevistados es la falta de equipamientos, recursos y capacitación, así como la optimización y actualización de los sistemas operativos para tratar estos delitos informáticos.
Pregunta 6: Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?	Desde otra arista, los entrevistados manifestaron que la cadena de custodia digital actual no necesariamente garantiza plenamente la integridad o autenticidad de todos los contenidos generados por intermedio de la IA, al contrario, solo pueden evidenciar tradicionalmente los archivos digitales y no a grandes escalas como hoy en día suele aplicarse, y no se desplazan en deepfakes o clonaciones de voz y videos, por lo cual resultará complejo determinar el puerto principal de operatividad donde se distribuyó dicho contenido, no solo se requiere de un análisis técnico especializado sino de una identificación de metadatos algorítmicos propiamente de los modelos generativos, por lo que el sistema judicial peruano no cuenta con dichos recursos o motores de búsqueda, ni metodologías para revisar o reconocer su origen, siendo necesario actualizar los sistemas y recursos para poder custodiar digitalmente estos delitos. Como han mencionado los entrevistados de forma general, no existe un control del mercado negro y clandestino que distribuye la información y datos personales para empezar a sancionar e identificar a estos sujetos delictivos.

Tabla de análisis de los resultados relacionados al Objetivo Especifico 2

Entrevistados Preguntas	Análisis e interpretación de las respuestas de los entrevistados (E1 – E10)
Pregunta 7: ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?	En esta pregunta coincidieron los especialistas en que puede demostrarse por medio de un análisis comparativo los objetivos propuestos de la normativa y sus efectos en la inoperancia del cuerpo legal analizado, toda vez que, en la práctica judicial a pesar de la vigencia normativa, persisten dificultades para investigar y sancionar y determinar la suplantación de identidad por medio de la IA, lo cual implica una brecha entre protección normativa y efectividad para proteger el derecho a la autodeterminación informativa ante la falta de evaluaciones tecnológicas. En las respuestas de los entrevistados se puede probar la inoperancia a través de la autodeterminación informativa frente a una inseguridad digital por la falta de mapeo, rastreo y seguimientos a estas organizaciones criminales.
Pregunta 8: ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.	En esta pregunta los entrevistados consideraron que la protección que otorga la ley en la autodeterminación informativas muchas veces es limitada y reactiva, lo cual genera un daño a la investigación por su inoperatividad en la recolección de la información ante el uso indebido de datos personales, no regula expresamente estos aspectos mencionados, sin poder controlar la utilización de datos biométricos en sistemas de IA, por ende, resulta parcial. La constitución protege y garantiza estos derechos y busca una garantía, sin embargo, no se actualiza a los nuevos cambios o tendencias originadas en los entornos digitales.
Pregunta 9: ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?	En esta interrogante los entrevistados indicaron que ante la ausencia de una regulación insuficiente y específica respecto a la seguridad digital, puede implicar procesos de revictimización en personas afectadas por estos casos, por lo que no se establecen directrices para mejorar la normativa ante contenidos falsificados ni protocolos inmediatos para el uso de plataformas digitales, lo cual puede generar manipulación emocional hacia las víctimas y complejidad probatoria con manipulación algorítmica. Los entrevistados han considerado que la falta de una regulación específica impacta en la aplicación legal por no adecuarse a una realidad.

Tabla de análisis de los resultados relacionados al Objetivo Especifico 3

Entrevistados Preguntas	Análisis e interpretación de las respuestas de los entrevistados (E1 – E10)
Pregunta 10: ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?	En esta interrogante la inoperancia incide en la correcta tipificación penal de estos delitos por medio de la IA, toda vez que en la práctica, los hechos deben adecuarse en tipos penales que no fueron diseñados para altas tecnologías o avanzadas lo cual aplicar un agravante resulta siendo incongruente ante la introducción de esta normativa mediante el uso de la IA, por la falta de herramientas y peritos en los casos, ya que cuando esta acreditación no se logra los casos se procesan únicamente en relación al tipo base por lo que existe una limitación de carácter estructural. Los entrevistados coincidieron que ante una falta de claridad en el tipo penal es complejo imputar un delito y más cuando los agravantes no son precisos.
Pregunta 11: ¿Considera que el artículo 9 de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.	Bajo esa misma línea, los entrevistados consideraron que aunque el artículo 9º de la ley N.º 30096 contempla la suplantación mediante tecnologías digitales, su contexto no describe la forma especificada de modalidades derivadas de la IA, por lo cual esta falta de precisión impacta en la interpretación literal de la normativa al momento de adecuar el tipo de conducta o identidades dentro del tipo penal que se espera analizar o realizar la persecución del delito en estos casos, por consiguiente no existe plenitud cuantificable ante los vacíos emergentes actuales, los cuales afectan en la predictibilidad del tipo y respuesta penal. En esta pregunta también los entrevistados coincidieron que no, toda vez que el tipo penal no es específico sino fue abordado de forma general por lo que no es aplicable al caso.
Pregunta 12: Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?	Ahora bien, en esta interrogante los entrevistados consideraron que desde la perspectiva dogmática la normativa presenta deficiencias y tensiones en los principios de legalidad y taxatividad penal, lo que resulta ambiguo, ya que si bien incorpora a la IA como un agravante para determinados delitos, no termina de describir tecnologías similares o análogas, lo cual puede implicar conceptos amplios e interpretaciones carentes de validez jurídica ante la falta de precisión legal para delimitar con mayor claridad. Asimismo, la ausencia de una reglamentación complementaria y técnica agrava la incertidumbre tanto jurídica como interpretativa en la práctica y análisis de estos casos por parte de las instituciones, si bien la ley cumple con el principio de legalidad, empero no garantiza la taxatividad penal de delitos tecnológicos en entornos digitales. Finalmente, los entrevistados indicaron que la ley si cumple con la legalidad mas no con la taxatividad penal en los delitos tecnológicos.

3.2. Análisis de resultados de jurisprudencias

Tabla. Análisis jurisprudencial internacional y nacional del objetivo general

FUENTE DOCUMENTAL	Tribunal de Distrito de La Haya – Caso SyRI (Países Bajos, 2020) / Tribunal Constitucional del Perú – Exp. N.º 01116-2022-HD/TC
CONTENIDO	El presente caso inició en el 2018, mediante una demanda sobre privacidad dirigida a grupos de defensa de la privacidad y personas destacadas y el fallo se llevó a cabo el 20 de febrero de 2020 en una sentencia respecto al Sistema de Indicación de Riesgos. FUNDAMENTO INTERNACIONAL: Se fundamentó en el Convenio Europeo en Derechos Humanos al considerar el uso de tecnologías algorítmicas sin suficiencia en las garantías jurídicas vulneraba la protección de datos personales. Evidencia el desarrollo tecnológico para superar la capacidad de regular el derecho punitivo. La presente sentencia es un claro ejemplo pionero de la resistencia a todos aquellos sistemas digitalizados de carácter asistencial social al infringir derechos humanos. DECISION INTERNACIONAL: En el presente caso el Tribunal declaró incompatible el sistema automatizado SyRI vinculadas al derecho a la privacidad y la cooperación entre determinados grupos de derechos digitales y el bienestar para poder detener el fraude social y mejorar la eficiencia. El 05 de febrero de 2020 una sentencia sobre el Sistema de Indicación de Riesgos. FUNDAMENTO NACIONAL: En esta sentencia, tuvo su pronunciamiento en el control de los datos personales contribuyendo con los derechos fundamentales enfocado en entornos digitales. Asimismo, hizo hincapié a la suplantación de identidad mediante deepfakes o clonaciones evidenciando insuficiencia de instrumentos normativos actuales. DECISIÓN NACIONAL: El Tribunal Constitucional, declaró fundada la demanda por vulnerar el derecho a la autodeterminación informativa ordenando la entrega de dicho contenido con el rigor del tratamiento de datos personales.
ANÁLISIS CRÍTICO	INTERNACIONAL: Desde el análisis de la criminología digital se emplearon herramientas automatizadas en marcos normativos que delimitaron responsabilidades y mecanismos de persecución penal. Por consiguiente, la jurisprudencia comparada evidencia que cuando no se regula un derecho adecuadamente en el uso de tecnologías, genera un déficit en la tutela penal, por ello, impacta en la capacidad del sistema legal para tipificar y sancionar. NACIONAL: En ese contexto, la evolución tecnológica genera una discontinuidad normativa y tecnológica en el empleo de inteligencia artificial para la manipulación de identidades en el derecho penal peruano, por lo cual se planteó retos que permitan actualizar los mecanismos tradicionales para proteger jurídicamente a las personas.
CONCLUSIONES	En conclusión, la jurisprudencia internacional como nacional revelan la necesidad de fortalecer el marco legal enfrentado a los nuevos modelos de vulneraciones y desprotección digital en los ordenamientos jurídicos lo cual impacta riesgosamente en los delitos informáticos.

Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 1

FUENTE DOCUMENTAL	High Court of Bombay (India, 2024) – Caso Akshay Kumar vs. Deepfake Content. / Carpeta Fiscal No 294-2022.
CONTENIDO	FUNDAMENTO INTERNACIONAL: El caso fue presentado el 15 de octubre de 2025. Asimismo, el tribunal ordenó el retiro de todo contenido deepfake que era utilizado con la imagen y voz de un actor. El tribunal indicó que los deepfakes son una amenaza creciente ya que facilitan el generar contenidos extremos y realistas. Este presente precedente evidenció que los marcos tradicionales son insuficientes para combatir estos delitos tecnológicos debido a su complejidad para poder identificar autores y probar que se incurrió en falsificación tecnológica. DECISION INTERNACIONAL: El tribunal otorgó medida cautelar al demandante ordenando a los demandados se abstengan de violar sus derechos infringiendo o utilizando como apropiación indebida de sus derechos de personalidad y morales la explotación o manipulación de su información o nombres, voz, imagen y otros por ser un delito el cual acarreó denuncias por fraude contra el actor. FUNDAMENTO NACIONAL: El 5° Despacho de la Primera Fiscalía Corporativa Especializada en Delitos de Corrupción de funcionarios abordó la denuncia de la denunciada por la comisión de los delitos y se evidenció la prueba digital. Por su parte se identificó que la prueba puede darse por la veracidad objetiva, la Constitucionalidad de la actividad probatoria, la utilidad de la prueba y la Pertinencia de la prueba para acreditar la evidencia digital. DECISIÓN NACIONAL: La decisión final fue aperturar la investigación en base a los fundamentos expuestos que resaltaron la evidencia digital como parte de una prueba.
ANÁLISIS CRÍTICO	INTERNACIONAL: En el caso del ámbito comparado se pudo advertir el hecho probado por medio de la información recolectada generando un precedente para dicho delito. NACIONAL: Desde el ámbito jurídico nacional se evidenció la existencia de la prueba.
CONCLUSIONES	Se puede sintetizar que las distintas legislaciones todavía no cuentan con herramientas y leyes optimizadas para el tratamiento jurídico de estos delitos generando vacíos que repercuten en el análisis probatorio dentro del encuadre del derecho penal peruano.

Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 2

FUENTE DOCUMENTAL	Sentencia del Tribunal Constitucional 27/2020 / Exp. 03041-2021-PHD/TC
CONTENIDO	FUNDAMENTO INTERNACIONAL: En la presente sentencia el tribunal admitió la demanda de la demandante y ordenó el retiro inmediato debido a vulneraciones de datos personales partiendo del derecho a la intimidad el cual estableció el uso no consentido de la imagen en contextos ajenos por violar derechos fundamentales ante terceros no autorizados. DECISION INTERNACIONAL: Se ordenó el retiro de todos los motores de búsquedas de su información personal por implicar que se trasverse con otras conductas punibles. FUNDAMENTO NACIONAL: En el presente caso se llevó por medio de un proceso de Habeas data y se tuvo como objeto la protección de datos personales en derechos reconocidos, aplicando supletoriamente el derecho al olvido y garantizando la eliminación o supresión de información personal en sistemas informáticos para proteger derechos fundamentales y conexos en el caso (<i>caso Arévalo Ramírez</i>) ff. jj. 11-12]. DECISIÓN NACIONAL: La decisión fue declarar fundada la demanda por autodeterminación por haberse lesionado el derecho a la autodeterminación informativa en cuanto al derecho a la información.
ANÁLISIS CRÍTICO	INTERNACIONAL: El presente análisis del caso se basa en la vulneración de datos personales usados por sujetos inescrupulosos y solo se espera paz. NACIONAL: La sentencia relevante del derecho al olvido permite suprimir cualquier información personal de las víctimas y su distribución de datos personales en lugares de alta peligrosidad ilícitamente.
CONCLUSIONES	En ese mismo sentido ante la ausencia de credibilidad o carencia de jurisprudencia se puede generar un precedente para el tratamiento y mejor entendimiento de este delito generado.

Tabla. Análisis jurisprudencial internacional y nacional del objetivo específico 3

FUENTE DOCUMENTAL	Caso State v. Loomis (2016)
CONTENIDO	FUNDAMENTO INTERNACIONAL: En el presente caso, el Tribunal Supremo sostuvo que la sentencia de primera instancia sobre la evaluación del riesgo algorítmico en el marco de imposición de penal no habría vulnerado el debido proceso. DECISION INTERNACIONAL: La sala de apelaciones procedió a favor del sujeto delictivo al indicar que era complejo realizar evaluaciones de riesgo algorítmicas ya que estas son ambiguas, lo cual fue materia de análisis crítico.
ANÁLISIS CRÍTICO	INTERNACIONAL: En el presente caso no se pudo analizar como corresponde el tipo penal pese a acreditarse el delito, ya que no se podía establecer el origen de los algoritmos y el riesgo de estos, por lo cual fue una sentencia cuestionada en el ámbito de la tipificación penal.
CONCLUSIONES	En conclusión, es necesario contar con jurisprudencias que analicen el fondo de los algoritmos para delimitar conductas típicas y sancionar estos delitos realizados por altas tecnologías.

IV. DISCUSIÓN

4.1. Discusión del objetivo general

En concordancia con lo señalado por (Taboada, 2024) en España, se identificó que la identidad digital forma parte de la privacidad, la misma que se encuentra amenazada por las nuevas tecnologías. Desde esta perspectiva y en los hallazgos obtenidos en la presente investigación se evidencia un vacío normativo en este tipo de casos. Asimismo, en la investigación realizada por Santiago y Yesquen (2024) concluyen que la inteligencia artificial en los delitos de suplantación de identidad, afecta tanto al patrimonio como la moral de las víctimas.

En consecuencia, esto confirma la inoperancia de la normativa vigente ante la falta de adecuación para la prevención, investigación y sanción punitiva de estos delitos.

Desde un análisis de la jurisprudencia internacional indica que los avances en IA han llevado a crear escenarios inéditos donde vulneran derechos que el derecho penal todavía no ha culminado de regular de forma adecuada, como el caso presentado de Case of SyRI (2020), constato que los sistemas tecnológicos también pueden afectar y lesionar derechos fundamentales cuando no existen garantías específicas que controlen estos casos. A nivel Nacional, el Tribunal constitucional resalto la importancia de la autodeterminación informativa y la protección de los datos personales. No obstante, en nuestro ordenamiento jurídico aún no asegura de manera explícita la suplantación de

identidad mediante la IA; esto se evidencia en las limitaciones estructurales para la identificación de estas conductas en delitos tecnológicos y la regulación punitiva.

En base al análisis a nivel internacional y nacional, se observa que la normativa vigente resulta ineficiente frente a delitos tecnológicos. Si bien nuestra legislación reconoce la protección de datos y la identidad personal como parte de los derechos fundamentales, ello resulta insuficiente, debido que las nuevas modalidades delictivas requieren tipificaciones más precisas e instrumentos efectivos para poder sancionar y proteger la identidad en entornos digitales.

4.2. Discusión del objetivo específico 1

Los resultados muestran que los aspectos inoperantes incluyen limitaciones técnicas y jurídicas en el tratamiento jurídico de la evidencia digital, en el uso de tecnologías especializadas en el procedimiento penal, los hallazgos expuestos se ajustan a lo señalado por (Cieza et al., 2025) quien sostiene que la IA puede mejorar los procesos de autenticación, detección de *deepfakes* e identificación facial, sin embargo su mal uso puede generar limitaciones vinculadas a los datos y sesgos en algoritmos ante la ausencia o pérdida de evidencias, lo cual es necesario contar con instrumentos especializados para optimizar y garantizar su validez dentro de la evidencia digital.

Por otro lado, el autor Velásquez (2025), sostiene que los delitos de suplantación de identidad digital presentan falencias por los pocos recursos tecnológicos y equipos, así como el personal especializado. Con ello, se evidencia una brecha entre la norma y su aplicación.

Con la jurisprudencia obtenida a nivel internacional, como el precedente de *Akshay Kumar v. Deepfake Content (2024)* pone en énfasis los contenidos relacionados con *deepfakes*, que ponen en manifiesto una manipulación en entornos digitales como la

imagen o voz. Ello representa una amenaza que va en aumento debido que genera contenido realista, lo cual dificultaría reconocer lo autentico. En la jurisprudencia nacional adquirida, el Tribunal Constitucional ha revelado que se debe garantizar la protección de datos personales e individualidad de la identidad en el marco de disposiciones penales más específicas en casos de suplantación de identidad; sin embargo, la Ley N.º 32314 presenta limitaciones regulatorias enfrentándose a las nuevas modalidades delictivas como es la suplantación de identidad mediante IA.

Desde mi postura, considero que la normativa vigente resulta insuficiente para enfrentar delitos vinculados con IA, debido que nuestro derecho penal es tradicional y no fue diseñado para este tipo de comportamientos. Dado que estos hechos delictivos muestran un carácter trasnacional, automatizado y muy técnico ejecutado en el ciberespacio con soporte algorítmico, esto dificulta poder determinar la autoría y la imputación. Se requiere incorporar medidas más específicas en su tipificación.

4.3. Discusión del objetivo específico 2

Los resultados recopilados indicaron una capacidad limitada para garantizar la protección de la autodeterminación informativa y seguridad digital, señalando un problema a los algoritmos con capacidad de generar decisiones automatizadas y de esa manera puede vulnerar derechos fundamentales. La IA aún no cuenta con tratamiento para garantizar la sanción punitiva de manera integral en entornos digitales. Bajo esa línea, los hallazgos obtenidos en la investigación realizada por Gutiérrez (2024) demostró que el uso intensivo de datos personales por sistemas de inteligencia artificial genera afectaciones a la información ante la ausencia de garantías por medios como algoritmos masivos en la comisión de estos delitos por medio de estos canales.

En el análisis jurisprudencial a nivel internacional tenemos el (*Tribunal Constitucional de España*, 2020), evidencio uno de los retos más importantes para la persecución de delitos vinculados a la IA. Se abordó la problemática de los *deepfakes*, los cuales pueden comprometer la confiabilidad de las pruebas tanto audiovisuales como textuales en procesos determinados jurisdiccionalmente, dificultando la verificación de la autenticidad de evidencia digital. Por otro lado, a nivel Nacional el (*Tribunal Constitucional del Perú.*, 2021) ha manifestado que la autenticidad de la evidencia digital es ausente, pero reconocen constitucionalmente la autodeterminación informativa como derecho fundamental estrechamente vinculado al control de los datos personales, empero no establece protocolos especializados en identificación y verificación de datos o contenidos creados por la IA.

El derecho probatorio en estos casos enfrenta desafíos respecto a la autenticidad y confiabilidad de la evidencia digital, sin embargo, cuando no se cuenta con los recursos necesarios como es el contar con mecanismos técnicos verificables en peritajes digitales se ve vulnerado el proceso. Debido que las pruebas se pueden manipular, lo cual significa que en nuestra normativa requiere de una reglamentación que incorpore estándares de análisis forenses digitales para de esa manera pueda garantizar la eficacia del sistema operativo y de justicia en delitos tecnológicos.

4.4. Discusión del objetivo específico 3

Los resultados constataron que ante la poca claridad de una tipificación penal el delito carece de dificultades interpretativas, por su parte los investigadores Arredondo y Casique (2025) indicaron que existe ambigüedad respecto a la responsabilidad penal en los casos de suplantación de identidad, lo que afecta la eficacia del sistema penal. De esta manera, el autor Giuca (2023) abordó que el uso de inteligencia artificial plantea nuevos

desafíos en la determinación de la responsabilidad penal. En consecuencia, el marco legal peruano debe ser preciso y ajustarse a la realidad tecnológica actual.

Asimismo, se evidencia que la IA ha transformado la manera en que cometen estos hechos delictivos. En el derecho comparado, se muestra que los fraudes cometidos mediante *deepfakes* posee una tecnología que permite recrear identidades digitales con un realismo lo que supera las categorías tradicionales del derecho penal. Estas conductas no siempre se ajustan correctamente a tipos penales clásicos como falsedad documental o fraude informático.

En Perú, el (*Tribunal Constitucional del Perú*, 2022) reconoce que la identidad personal forma parte del núcleo esencial de los derechos fundamentales. Sin embargo, la legislación penal no regula explícitamente las nuevas formas de suplantación digital generadas por inteligencia artificial. Esto genera dificultades para encajar estas conductas en tipos penales existentes, evidenciando la inoperancia normativa frente a estas modalidades delictivas emergentes.

La tipificación penal es un pilar fundamental del principio de legalidad en materia penal. Cuando el ordenamiento jurídico no reconoce de manera expresa las nuevas formas de criminalidad tecnológica, surgen vacíos que limitan la actuación del Estado. La IA ha redefinido el concepto de identidad digital y amplía las posibilidades de manipulación fraudulenta de datos personales. En este contexto, resulta indispensable que el legislador actualice el marco penal incorporando figuras delictivas específicas relacionadas con *deepfakes*, clonación de voz e identidad sintética; de lo contrario, el sistema penal seguirá enfrentando dificultades para sancionar eficazmente estas conductas.

Figura 1. C1: Delito de Suplantación de Identidad y subcategorías / autores y discusión de los resultados

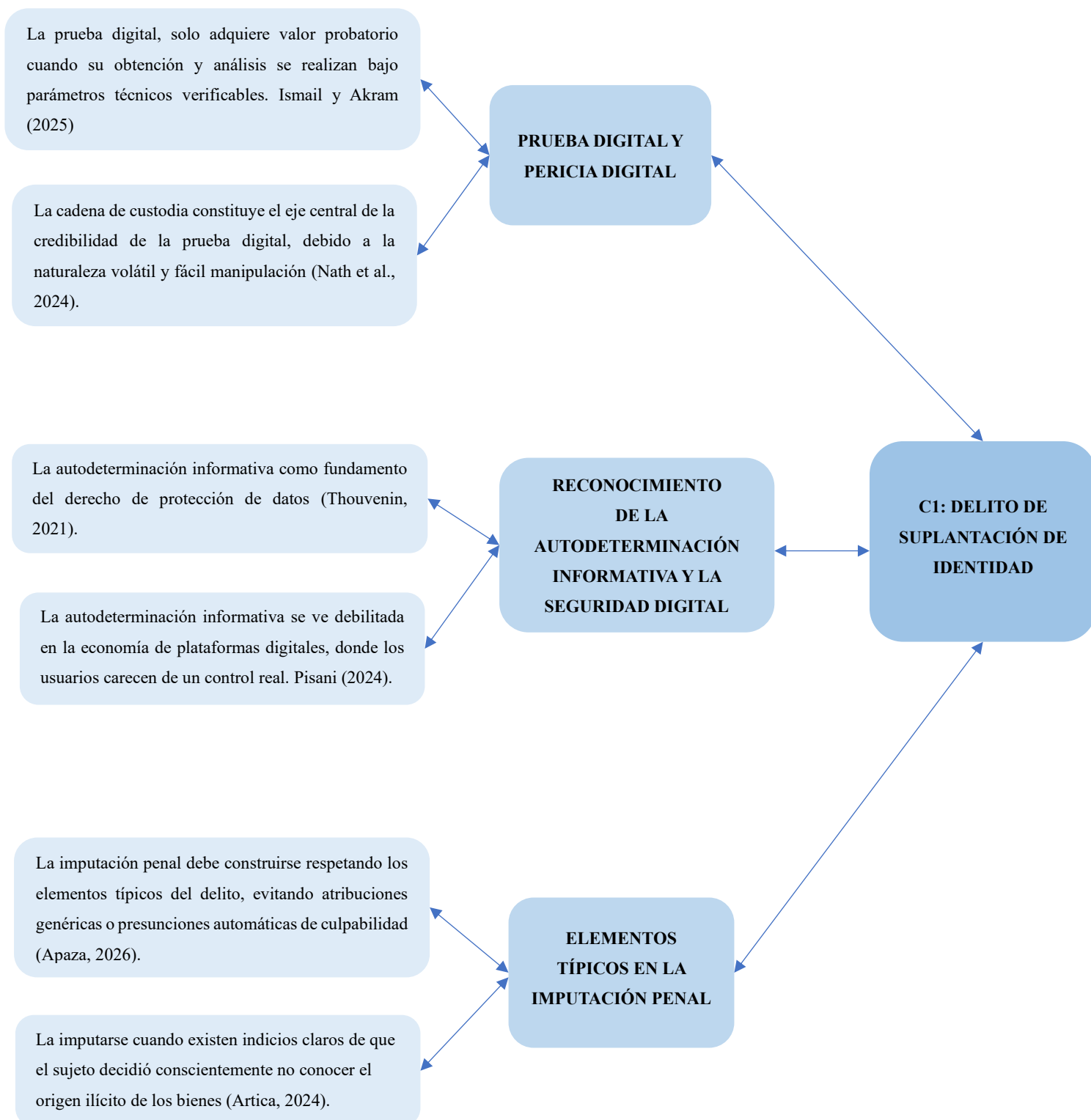
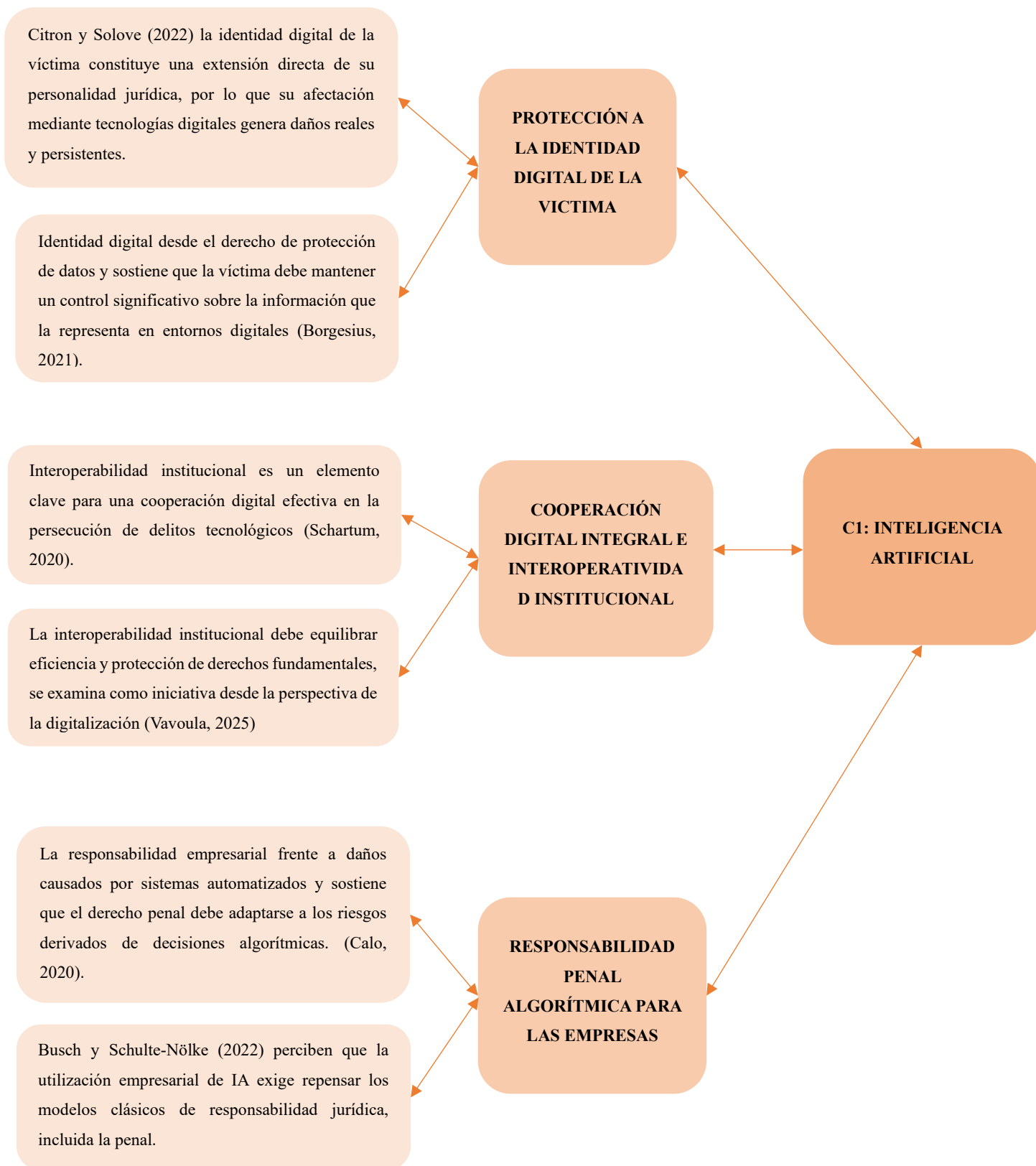


Figura 2. C2: Inteligencia Artificial y subcategorías / autores y discusión de los resultados



V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Primera: En conclusión, se analizó de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través de inteligencia artificial en Lima. Lo más relevante fue identificar que en el análisis de estos delitos pese a existir normativa, esta presenta limitaciones que se enfrentan a las nuevas modalidades en el ámbito de la criminalidad digital originadas en entornos digitales cuando se emplean tecnologías como la IA, vulnerando la identidad digital de las personas. En ese contexto, se evidenció que el marco jurídico actual no se encuentra plenamente adecuado a las nuevas formas de suplantación de identidad delictivas, por lo cual es necesario que el derecho penal y las políticas de persecución penal se adecuen a los avances tecnológicos creando mecanismos normativos con mayor precisión que permitan identificar, investigar y sancionar estas conductas en garantía de la protección de datos personales y seguridad digital. Lo que más contribuyó fue analizar el problema desde el ámbito jurídico de la criminología digital en el sistema peruano y su impacto internacional. Lo más difícil fue identificar la recopilación de la información especializada y jurisprudencias actuales en estos casos.

Segunda: En conclusión, se analizaron los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través de inteligencia artificial. Lo más relevante fue que del análisis se pudo advertir que la normativa

presenta vacíos y lagunas jurídicas en relación a la identificación de los medios tecnológicos empleados para la ejecución de estos delitos, así como determinar responsabilidades cuando intervienen sistemas automatizados o algoritmos con el uso de la IA, ello genera dificultades en la persecución penal de este delito, limitando la eficacia del sistema de justicia enfrentada a delitos informáticos por ser sofisticados conforme pasa el tiempo. En consecuencia, resulta necesario que el marco jurídico y su ordenamiento incorpore soluciones por medio de disposiciones más específicas en la regulación del uso indebido de tecnologías emergentes, fortaleciendo los instrumentos legales y procesales que permitan enfrentar la criminalidad digital. Lo que más coadyuvó fue el análisis doctrinario y jurisprudencia del derecho peruano y comparado para comprender este estudio. Lo más complejo fue la escasez de fuentes o precedentes judiciales nacionales vinculados a la IA, aplicada a suplantación de identidad.

Tercera: En conclusión, se evaluó como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial. El análisis permitió demostrar que ante la falta de mecanismos normativos claros en la protección de datos personales y la gestión recaudadora de evidencias digitales se ve dificultada la tutela efectiva del derecho a la autodeterminación informativa. Se identificó que, si bien existen avances tecnológicos que han superado la capacidad regulatoria del derecho punitivo, todavía existen vacíos en la protección jurídica enfrentados a la manipulación de datos, videos, imágenes, voz o identidades digitales en los distintos sistemas automatizados. En ese sentido, es necesario reforzar la normativa vinculada a datos personales y seguridad digital en casos de delitos informáticos con el propósito de brindar una mejor respuesta jurídica a las nuevas vulneraciones de derechos fundamentales. Lo que más ayudó fue el análisis relacionado al derecho

penal y constitucional, así como los nuevos modelos de criminalidad. Lo más complejo fue obtener estudios especializados que vinculen específicamente a la IA, con la afectación a la autodeterminación en el derecho peruano.

Cuarta: En conclusión, se analizó en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial. El presente estudio demostró que la legislación actual no contempla los nuevos modelos de suplantación de identidad en delitos generados por tecnologías avanzadas como algoritmos automáticos. Este hecho genera implicancias en la interpretación jurídica y dificulta contar con una tipificación óptima para el tratamiento jurídico de estos delitos en el marco penal existente. En ese contexto, es de suma importancia que el legislador pueda incorporar una regulación más exacta a las nuevas modalidades y que pueda contemplar el uso indebido de estas tecnologías modernas para su efectividad y vaya direccionado acorde a la evolución tecnológica actual. Lo que más colaboró fue el análisis de las normativas y las comparaciones con la jurisprudencia internacional. Lo más difícil fue la limitada existencia de normativas que seas especificadas en el uso de la IA, en el ámbito del marco peruano.

5.2. Recomendaciones

Primera: Se recomienda que el Estado peruano revise y actualice el contenido normativo de la Ley N.º 32314 con el propósito de adecuarla a los nuevos escenarios de criminalidad digital vinculados al uso de inteligencia artificial. Para ello, resulta necesario incorporar disposiciones específicas que permitan identificar y sancionar las nuevas modalidades de suplantación de identidad generadas mediante tecnologías emergentes, fortaleciendo así la eficacia del sistema de persecución penal.

Segunda: Se recomienda que el legislador incorpore en la normativa penal y en la legislación sobre delitos informáticos disposiciones que regulen de manera expresa el uso indebido de herramientas de inteligencia artificial en la comisión de delitos contra la identidad digital. Ello permitirá reducir los vacíos normativos existentes y facilitar el trabajo de las autoridades encargadas de la investigación y persecución de estos delitos.

Tercera: Se recomienda fortalecer los mecanismos institucionales de protección de la autodeterminación informativa y seguridad digital mediante la articulación entre las entidades responsables de la protección de datos personales, el sistema de justicia penal y los organismos especializados en ciberseguridad. Asimismo, se sugiere implementar protocolos de investigación digital que permitan recolectar y analizar adecuadamente las evidencias tecnológicas relacionadas con delitos cometidos mediante inteligencia artificial.

Cuarta: Se recomienda promover reformas legislativas orientadas a mejorar la tipificación penal del delito de suplantación de identidad cuando este sea cometido mediante inteligencia artificial, incorporando definiciones jurídicas claras sobre el uso de tecnologías automatizadas en la comisión de delitos. De esta manera, se contribuirá a fortalecer la seguridad jurídica, garantizar la protección del derecho a la identidad y brindar una respuesta penal adecuada frente a las nuevas formas de criminalidad digital.

5.3. Propuesta Normativa

Ley que modifica y complementa la Ley N° 32314 para fortalecer la persecución del delito de suplantación de identidad mediante inteligencia artificial

I. Exposición de motivos:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas sociales, económicas y comunicativas, generando beneficios indiscutibles, pero también nuevas formas de criminalidad altamente sofisticadas entre ellas la suplantación de identidad mediante tecnologías como Deepfakes, clonación de voz e identidades sintéticas representa una amenaza directa a derechos fundamentales como la identidad personal la autodeterminación informativa y la seguridad.

En el Perú, la promulgación de la Ley N.º 32314 constituyó un avance al incorporar la inteligencia artificial como circunstancia agravante en determinados delitos. Sin embargo, su diseño normativo ha evidenciado serias limitaciones en su aplicación práctica, pues no establece una tipificación autónoma del fenómeno, carece de criterios técnicos para la valoración de la prueba digital, no regula adecuadamente la atribución de responsabilidad en entornos automatizados ni garantiza una protección integral de la identidad digital como bien jurídico.

Esta insuficiencia normativa genera un escenario de inseguridad jurídica, dificultades en la labor fiscal y judicial, así como riesgos de impunidad frente a conductas que afectan gravemente a la ciudadanía. En tal contexto, resulta necesario adecuar el ordenamiento jurídico a la realidad tecnológica contemporánea, superando el enfoque reactivo y adoptando un modelo preventivo, integral y coherente con las políticas públicas de transformación digital, seguridad ciudadana y protección de datos personales.

El presente proyecto de ley se alinea con las políticas está orientadas a fortalecer el sistema de Justicia garantizar la seguridad jurídica y proteger derechos fundamentales en entornos digitales respondiendo a la necesidad de consolidar una política criminal moderna que permita al Estado de enfrentar eficazmente la ciudad delincuencia mediante la incorporación de estándares técnicos la especialización institucional y la regulación de nuevas formas de responsabilidad.

II. Propuesta Normativa

Artículo 1.- incorporación del delito de suplantación de identidad mediante inteligencia artificial

Incorpórese el artículo 154-C, al Código Penal en los siguiente:

“El que, mediante el uso de inteligencia artificial, tecnologías análogas o sistemas automatizados, cree, manipule o utilice datos personales, biométricos, imagen, voz o cualquier elemento de identificación digital de una persona con la finalidad de suplantarla, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años.”

La pena será no menor de 6 años y mayor de 10 años cuándo:

1. Se utilicen tecnologías de alta sofisticación como deepfakes o identidades sintéticas.
2. Se genere perjuicio económico, reputacional o afectación a la dignidad de la víctima.
3. La víctima sea menor de edad o persona en condición de vulnerabilidad.

Artículo 2. - Estándares de prueba digital

Incorpórese el artículo 158-A al Código Procesal Penal

“En la investigación y juzgamiento de delitos cometidos mediante Inteligencia artificial la evidencia digital deberá cumplir con criterios de autenticidad integridad trazabilidad y reproductividad técnica garantizando la cadena de Custodio y su validación mediante pericia especializada por un perito digital”.

Artículo 3.- Responsabilidad penal en entornos tecnológicos

Establézcase que: “Las personas naturales o jurídicas que diseñen, implementen, administren o utilicen sistemas de Inteligencia artificial serán responsables penalmente cuando por falta de control, supervisión faciliten la comisión de delitos”.

Artículo 4.- Protección de identidad digital

Reconocer la identidad digital como bien jurídico autónomo: “La identidad digital constituye una extensión de la personalidad y goza de protección penal Frente a cualquier forma de manipulación uso indebido o suplantación mediante tecnologías digitales.

Artículo 5.- Autodeterminación informativa y seguridad digital

Dispóngase que: “El tratamiento de datos personales mediante sistemas automatizados que vulnere la autodeterminación informativa o sea utilizado con fines ilícitos será sancionado conforme a ley, sin perjuicio de la responsabilidad penal correspondiente.”

Artículo 6.- Fortalecimiento institucional

“El Ministerio Público y la Policía Nacional del Perú implementarán unidades especializadas en investigación de delitos tecnológicos y peritaje digital, dotándolas de recursos técnicos y capacitación continua.”

Artículo 7.- Interoperabilidad y cooperación digital

“Las entidades del sistema de justicia deberán garantizar mecanismos de interoperabilidad para el intercambio seguro y eficiente de información en la investigación de delitos informáticos.”

III. Disposición Complementaria Final

El Poder Ejecutivo reglamentará la presente ley en un plazo no mayor de noventa (90) días, estableciendo estándares técnicos para la obtención, preservación y valoración de la evidencia digital, así como lineamientos de coordinación interinstitucional.

IV. Fundamentación Final

La presente propuesta normativa responde a la necesidad de cerrar los vacíos identificados en la legislación vigente, fortaleciendo la capacidad del Estado para prevenir, investigar y sancionar la suplantación de identidad mediante inteligencia artificial. Su enfoque integral articula política criminal, política pública digital y protección de derechos fundamentales, garantizando una respuesta jurídica coherente, proporcional y eficaz frente a los desafíos tecnológicos contemporáneos.

REFERENCIAS

LIBROS RECURRIDOS

BRENNER, W. (2010). *Cybercrime: criminal threats from cyberspace*. Bloomsbury Publishing USA.

<https://goo.su/6bmaNP1>

SUPO, J., y MARTÍNEZ ÁNGELES, J. (2025). *Niveles de Investigacion 2025*. Editorial Pacífico.

https://www.researchgate.net/publication/395943015_Niveles_de_Investigacion_2025pdf

Trejo, Z., MARTÍNEZ, C., SÁNCHEZ, O., y TÉLLEZ, A. (2025). *Estudios de derecho internacional y derecho interno*. Editorial Fontamara SA de CV.

<https://goo.su/S48re9>

REVISTAS Y ARTÍCULOS RECURRIDOS

ALVARADO, J. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Foro Jurídico*, (15), 26–41.

<https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19833>

AVALOS, A., BARRETO, A., SANCHEZ, G., TALANCHA, O., MARTINEZ, M., RODRIGUEZ, N., y LOPEZ, A. (2025). Abordaje, desafíos y evolución de la legislación sobre suplantación de identidad digital en Perú. *Sapientia & Iustitia*, (12), 5–36.

<https://sapientia.ucss.edu.pe/index.php/sei/article/view/155>

BHARATI, N., WONG, P., MOSTÉFAOUI, S. K., KBAIER, D., y COLLIE, J. (2025). *Explainable deepfake detection: A multi-model framework with human-interpretable rationales for legal investigation purposes*. *Machine Learning with Applications*, 23, 100819.

<https://www.sciencedirect.com/science/article/pii/S2666827025002026>

BRIONES, J., LOYAGA, Z., GRADOS, S., y VILCHEZ, C. (2024). El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el deepfake. *Vniversitas*, 73.

[https://revistas.javeriana.edu.co/files-articulos/VJ/73\(2024\)/6722660015/index.html](https://revistas.javeriana.edu.co/files-articulos/VJ/73(2024)/6722660015/index.html)

BUSCH, C., KAMPHORST, A., DE GRAAF, T., CARVALHO, J. M., GILLIES, E., PITTI, R., GOTTARDIS, L., RAJNERI, E., y BAGINSKA, E. (2019). Journal of European Consumer and Market Law. *Journal of European Consumer and Market Law*, 8(5).

https://heinonline.org/HOL/Page?handle=hein.kluwer/jeucml0008&div=45&g_sent=1&casa_token=

CALO, R. (2017). Artificial intelligence policy: a primer and roadmap. *UCDL Rev.*, 51, 399.

https://heinonline.org/HOL/Page?handle=hein.journals/davlr51&div=18&g_sent=1&casa_token=

CARTER, T., y MCNEALEY, L. (2025). Protection motivation and cybersecurity intentions: a visual conjoint experiment. *Journal of Experimental Criminology*, 1–28.

<https://link.springer.com/article/10.1007/s11292-025-09717-1>

CASH, P., ISAKSSON, O., MAIER, A., y SUMMERS, J. (2022). Sampling in design research: Eight key considerations. *Design Studies*, 78, 101077.

<https://www.sciencedirect.com/science/article/pii/S0142694X21000880>

CHAND, P. (2025). Methods of data collection in qualitative research: Interviews, focus groups, observations, and document analysis. *Advances in Educational Research and Evaluation*, 6(1), 303–317.

<https://www.syncsci.com/journal/AERE/article/view/AERE.2025.01.001>

CIEZA, P. BARANDIARÁN, V., y VASQUEZ, F. (2025). El uso de inteligencia artificial en el análisis forense de imágenes y videos en investigaciones criminales: una revisión sistemática. *Revista Escpogra PNP*, 5(1), 1–14.

<https://revistaescpograpnp.edu.pe/ojs/index.php/1/article/view/303>

CITRON, K., y SOLOVE, J. (2022). Privacy harms. *BUL Rev.*, 102, 793.

<https://www.bu.edu/bulawreview/files/2022/06/PRIVACY-HARMS.pdf>

D'ANNA, T., PUNTARELLO, M., CANNELLA, G., SCALZO, G., BUSCEMI, R., ZERBO, S., & ARGO, A. (2023). The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare*, 11(5), 634.

<https://www.mdpi.com/2227-9032/11/5/634>

DÍAZ, C., GRANADOS, L. A., y VELÁZQUEZ, D. (2024). Proceso de profesionalización para el desarrollo profesional docente en la escuela básica. *Varona. Revista Científico Metodológica*, (80).

http://scielo.sld.cu/scielo.php?pid=S1992-82382024000200020&script=sci_arttext&tlng=en

DÍAZ, J., MOLINA, L., y SERRADOR, E. (2023). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad*, 65(3), 81–95.

http://www.scielo.org.co/scielo.php?pid=S1794-31082023000300081&script=sci_arttext

- DUBEY, K., y CHOUBEY, K. (2024). Reliable detection of blast disease in rice plant using optimized artificial neural network. *Agronomy Journal*, 116(3), 1099–1111. <https://acsess.onlinelibrary.wiley.com/doi/abs/10.1002/agj2.21449>
- FLORIDI, L., COWLS, J., BELTRAMETTI, M., CHATILA, R., CHAZERAND, P., DIGNUM, V., LUETGE, C., MADELIN, R., PAGALLO, U., y ROSSI, F. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://link.springer.com/article/10.1007/S11023-018-9482-5>
- GALINDO, M. (2024). Suplantación de identidad digital: hacia una necesaria tutela penal. *Estudios de Deusto: Revista de Derecho Público*, 72(1), 199–228. <https://dialnet.unirioja.es/servlet/articulo?codigo=9598609>
- GIUCA, M. (2023). AI and criminal liability. Algorithmic error and human negligence in the context of the European regulation. *Diritto Penale Contemporaneo: Rivista Trimestrale*, (1), 46–69. <https://dialnet.unirioja.es/servlet/articulo?codigo=9608918>
- GUTIÉRREZ, B. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revista de La Facultad de Derecho de México*, 74(290), 125–148. <http://10.22201/fder.24488933e.2024.290.89719>
- HUAPAYA, S. (2024). Conflictos entre la autodeterminación informativa y la segmentación de perfiles a través de la publicidad programática online en el Perú. *Derecho & Sociedad*, (63), 285–298. <https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/29972>
- ISMAIL, M. , y A. M. (2025). (2025). Digital evidence and forensic standards. . . *Journal of Digital Forensics*, 19(1), 34–59. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0331683>
- JANUÁRIO, X. (2023). Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales. *Estudios Penales y Criminológicos*, 44(Ext.), 1–39. <https://revistas.usc.gal/index.php/epc/article/view/8902>
- KOOPS, B. (2022). Identity theft, identity fraud and/or identity-related crime. *Tilburg Law Review*, , 27(1), 1–25. https://www.researchgate.net/publication/257703479_Identity_theft_identity_fraud_andor_identity-related_crime

LIN, F. (2025). Organisational challenges in US law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws*, 14(4), 46.

<https://www.mdpi.com/2075-471X/14/4/46>

LOAIZA, D., SOTO, F., y HOYOS ESCALERAS, Á. M. (2024). Revolucionando la Justicia: El impacto de la Inteligencia Artificial en el Derecho Penal. *Estudios y Perspectivas Revista Científica y Académica*, 4(3), 2155–2174.

<https://doi.org/10.61384/r.c.a..v4i3.537>

MAMANI, A. (2026). La imputación penal con base en una delegación de funciones. *Derecho Penal y Criminología*, 47(122), 79–106.

<https://dialnet.unirioja.es/servlet/articulo?codigo=10525918>

MANTELERO, A. (2025). The AI Act: A realpolitik compromise and the need to look forward. *Digital Constitutionalism*, 311–344.

<https://www.inlibra.com/document/download/pdf/uuid/8944ad26-43a7-33fd-9711-51a29f76845d>

MARCHENA, Y. (2026). Garantías procesales y debido proceso: rol central de la imputación en el sistema penal peruano. *Revista InveCom*, 6(3).

https://ve.scielo.org/scielo.php?pid=S2739-00632026000302089&script=sci_arttext

MARTÍNEZ, G. (2024). Suplantación de identidad digital: Hacia una necesaria tutela penal. *Estudios de Deusto: Revista de Derecho Público*, 72(1), 199–228. <https://doi.org/10.18543/ed.3105>

MASSENO, D. (2022). La inteligencia artificial y la protección de datos: la “elaboración de perfiles” para la prevención de delitos graves y del terrorismo em las fuentes de la Unión Europea. *Revista Eletrônica Do Curso de Direito Da UFSM*, 17(2), e83679–e83679.

<https://doi.org/10.5902/1981369483679>

MITTELSTADT, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501–507.

<https://www.nature.com/articles/s42256-019-0114-4>

NATH, S., SUMMERS, K., BAEK, J., y AHN, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 11–20.

<https://ieeexplore.ieee.org/abstract/document/10835509/>

ORDOÑEZ-PACHECO, Á. F. (2025). Metodología de la Investigación Metodología académica con aplicación a las investigaciones sociales: enfoques, tipos, métodos y diseños. *Sociedad &*

Tecnología, 8(2), 335–357.

https://www.researchgate.net/publication/391268316_Metodologia_academica_con_aplicacion_a_las_investigaciones_sociales_enfoques_tipos_metodos_y_disenos

SION, L., VAN, D., DEWITTE, P., VALCKE, P., y JOOSEN, W. (2023). Demonstration of the DPMF for data protection analysis. *2023 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, 75–79. <https://ieeexplore.ieee.org/abstract/document/10350571/>

TABOADA, A. (2024). La ignorancia deliberada en la fórmula legislativa “debía presumir” en el delito de lavado de activos en el Perú. *THEMIS Revista de Derecho*, (86), 75–87. <https://revistas.pucp.edu.pe/index.php/themis/article/view/31015>

TAHERDOOST, H. (2021). Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. *International Journal of Academic Research in Management (IJARM)*, 10(1), 10–38. <https://hal.science/Hal-03741847/>

THOMAS, L., PITT, H., MCCARTHY, S., ARNOT, G., y HENNESSY, M. (2024). Methodological and practical guidance for designing and conducting online qualitative surveys in public health. *Health Promotion International*, 39(3), daae061–daae061. <https://goo.su/JdoA>

THOUVENIN, F. (2021). Informational self-determination: a convincing rationale for data protection law? *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 12, 246. https://heinonline.org/HOL/Page?handle=hein.journals/jipitec12&div=41&g_sent=1&casa_token=

VAVOULA, N. (2025). The Future of Digitalisation in EU Law Enforcement: Enhanced Exchanges of Personal Data, Privatisation and Algorithmisation. *Future*, 10(3), 709–719. https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2025_3_SS1_1_Niovi_Vavoula_00851.pdf

VLCKOVA, K., GONELLA, S., BAVELAAR, L., MITCHELL, G., Y SUSSMAN, T. (2024). Methodological and ethical challenges in designing and conducting research at the end of life: A systematic review of qualitative and textual evidence. *International Journal of Nursing Practice*, 30(5), e13224–e13224. https://www.researchgate.net/publication/376646560_Methodological_and_ethical_challenges_in

[designing_and_conducting_research_at_the_end_of_life_A_systematic_review_of_qualitative_and_textual_evidence](#)

YAZDANPANA, V., GERDING, H., STEIN, S., DASTANI, M., JONKER, M., NORMAN, J., y RAMCHURN, D. (2023). Reasoning about responsibility in autonomous systems: challenges and opportunities. *Ai & Society*, 38(4), 1453–1464. <https://link.springer.com/article/10.1007/s00146-022-01607-8>

ZAVALA, A. (2025). La Apropiación Fraudulenta por Medios Electrónicos y el Bien Jurídico Protegido. *Ciencia Latina: Revista Multidisciplinar*, 9(3), 11420–11437. <https://dialnet.unirioja.es/servlet/articulo?codigo=10375773>

ZUIDERVEEN, F., y POORT, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, 40(3), 347–366. <https://link.springer.com/article/10.1007/s10603-017-9354-z>

TESIS Y TRABAJOS DE INVESTIGACIÓN RECURRIDOS

ALAVA, P., y FLORES, A. (2024). *Análisis comparado de la inteligencia artificial y la suplantación de la identidad en el Perú 2023*. <https://hdl.handle.net/20.500.12692/158998>

ARREDONDO, X. y CASIQUE, D. (2025). *La responsabilidad penal de los operadores de telefonía en el delito de suplantación de identidad originada por la venta de chips en puntos no autorizados en el Perú*. https://alicia.concytec.gob.pe/vufind/Record/UTPD_b211d70dd21442e081361ae091816904

VELÁSQUEZ, L. (2025). *La figura jurídica de la suplantación de identidad frente a las barreras legales en las diligencias preliminares de investigación en el segundo despacho de la fiscalía de Miraflores - 2024*. <https://hdl.handle.net/20.500.12867/13889>

SANTIAGO, N., y YESQUEN, M. (2024). *Suplantación de identidad con el uso de la inteligencia artificial*. <https://hdl.handle.net/20.500.12692/159730> https://alicia.concytec.gob.pe/vufind/Record/UCVV_0f184e47e29de0a0d156d936433c682f

SCHARTUM, W. (2020). From legal sources to programming code. In *Cambridge Handbook of the Law of Algorithms* (pp. 301–336). Cambridge University Press.

[https://www.cambridge.org/core/books/abs/cambridge-handbook-of-the-law of algorithms/ from-legal-sources-to-programming-code/D6A122B2CF0DB96C628EDC8009A59497](https://www.cambridge.org/core/books/abs/cambridge-handbook-of-the-law-of-algorithms/from-legal-sources-to-programming-code/D6A122B2CF0DB96C628EDC8009A59497)

JURISPRUDENCIAS Y PRECEDENTES VINCULANTES RECURRIDOS

Akshay Kumar v. Deepfake Content. (2024). High Court of Bombay.

<https://indiankanoon.org/doc/>

Case of SyRI (System Risk Indication), ECLI:NL:RBDHA:2020:865 (Rechtbank Den Haag, 2020)

<https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:865>

Tribunal Constitucional de España. Sentencia 27/2020. (2020).

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3827

Tribunal Constitucional Del Perú. Expediente N.º 03041-2021-PHD/TC (2021).

<https://tc.gob.pe/jurisprudencia/2021/03041-2021-HD.pdf>

Tribunal Constitucional Del Perú. Expediente N.º 01116-2022-HD/TC (2022).

<https://tc.gob.pe/jurisprudencia/2022/01116-2022-HD.pdf>

RECURSOS ELECTRONICOS RECURRIDOS

DIRECCIÓN DE CIBERDELINCUENCIA PNP. (2025). *Comunicado N.º 14 - 2025 - Noticias - Policía Nacional del Perú - Plataforma del Estado Peruano.*

<https://www.gob.pe/institucion/pnp/noticias/1240629-comunicado-n-14-2025>

EBIZ NOTICIAS. (2025). *Mantenerse informado es clave para evitar ser víctima de delitos informáticos - eBIZ.*

<https://ebiz.pe/noticias/mantenerse-informado-es-clave-para-evitar-ser-victima-de-delitos-informaticos/>

FBI. (2025). *Centro de Denuncias de Delitos en Internet (IC3) | Altos funcionarios estadounidenses suplantados en una campaña de mensajes maliciosos.* <https://www.ic3.gov/PSA/2025/PSA250515>

INFOBAE. (2025). *Fraude digital en Perú: el 90% de limeños teme ser víctima mientras las estafas se vuelven más sofisticadas - Infobae.*

<https://www.infobae.com/peru/2025/03/24/fraude-digital-en-peru-el-90-de-limenos-teme-ser-victima-mientras-las-estafas-se-vuelven-mas-sofisticadas/>

OBSERVATORIO REGIONAL DE PIURA. (2025). *INCIDENCIA DELICTIVA PROVINCIAL (DENUNCIAS)* *Homicidios* *Robo* *Hurto* *Otros* *delitos.*

<https://www.policia.gob.pe/serviciospoliciales/denuncia.html>

Anexo 1: Matriz de categorización apriorística

“La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

PROBLEMA	OBJETIVOS	CATEGORÍAS	SUBCATEGORIAS	PREGUNTAS ORIENTADORAS	METODOLOGÍA
Problema General	Objetivo General	Categoría 1	Subcategorías 1		Enfoque de la investigación:
- ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?	- Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.	Delito de suplantación de Identidad	• Prueba digital y pericia digital • Reconocimiento de la autodeterminación informativa y la seguridad digital • Elementos típicos en la imputación penal	1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima? 2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente. 3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?	Cualitativo Método: Inductivo Diseño de la investigación: Descriptivo Tipo de investigación: Básica Diseño de la investigación: Estructura Metodológica No experimental /Teoría fundamentada Población participante: Profesionales del derecho: especializados en derecho penal e inteligencia artificial.
Problema Específico	Objetivo Específico	Categoría 2	Subcategoría 2		
- ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?	- Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.	Inteligencia Artificial	• Protección a la identidad digital de la víctima • Cooperación digital integral e interoperabilidad institucional. • Responsabilidad penal algorítmica para las empresas	4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial? 5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA? 6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de	Muestra: 10 abogados (litigantes, especializados en Procesal Penal y/o especialistas en IA) Técnica: Entrevista Instrumento: Guía de entrevista Escenario de estudio: Lima
- ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución	- Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en				

del delito de suplantación de identidad con inteligencia artificial?	la persecución del delito de suplantación de identidad con inteligencia artificial.	contenidos como deepfakes, clonaciones de voz o identidades sintéticas?
- ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?	- Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.	7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?
		8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.
		9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?
		10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?
		11. ¿Considera que el artículo 9 de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal
		12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Anexo 2. Instrumento de recolección de datos

Instrumento 1 – Guía de Entrevista



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:

Grupo/Sector:

Entrevistado:

Cargo:

Grado Académico:

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N°32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N°32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N°32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?
2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.
3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?
5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?
6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?
 8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.
 9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?
-

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?
11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal
12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:

Apellidos y nombres:

Cal:

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	23/02/2026
Grupo/Sector:	Dirección de Cibercrimen - Abogada
Entrevistado:	Mery Salas de Torres
Cargo:	Sub Oficial de la PNP/ Jefa del Área de la División de Investigación de Fraudes Informáticos y Contra la Fe Pública
Grado Académico:	Superior Universitaria

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N°32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N°32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N°32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

Se debe tomar en cuenta, que para la persecución de este tipo de delitos es necesario que tanto la Policía y como el Ministerio Público, deben llevar a cabo capacitaciones para el personal que la persecución de este delitos y todos los que conciernen a entornos digitales por medio de plataformas u otros análogos, que conforman de manera descentralizada, lo cual permitirá que se creen más Unidades Especializadas en Peritajes Digitales que puedan analizar evidencias que hayan sido generadas o usadas por medio tecnologías como la Inteligencia Artificial – IA. Aunado a ello, se debe contar con herramientas digitales óptimas y actualizadas a los nuevos modelos tecnológicos en el caso de la ciberdelincuencia en cibercrimen, los cuales deben estar a la altura de la modernidad ejercida por los delinquentes de este tipo, a fin de evitar que los casos remitidos al Ministerio Público queden en un simple archivamiento o sobreseimiento.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Desde mi experiencia como jefe y miembro de la PNP, se entiende jurídicamente este concepto en la práctica, tiene la intención de avanzar, sin embargo, la realidad es otra porque la criminalidad digital avanza y ello se demuestra con la elevada estadística respecto a las denuncias por ciberdelitos, se debe actualizar el código penal y la Ley especial de Delitos Informáticos, considero inclusive que todo debe ser dentro del Código Penal.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

Siempre se han preocupado en mejorar el marco legal para hacer frente a este tipo de delitos, sin embargo, como ya lo mencioné se necesita mayor capacitación al personal involucrado en este tipo de investigación y definitivamente descentralizar estas capacitaciones con la finalidad de contar con laboratorios forenses digitales en puntos críticos de nuestro país.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Uno de los principales aspectos en el ámbito de la evidencia digital, es resaltar que la misma requiere siempre de una preservación adecuada e inmediata, así como la extracción forense sin embargo eso no sucede en razón que en la práctica no se presenta las evidencias de manera adecuada en varias ocasiones inclusive se presentan como evidencias capturas de pantalla sin una validación adecuada, etc.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Una de las dificultades principales es que en la práctica se pierde información cuando no se realiza una preservación inmediata, como, por ejemplo; las direcciones IP, el registro de acceso, los perfiles falsos se pueden eliminar al instante, se debe tener en cuenta igualmente que los metadatos son importantes para determinar la autenticidad de la evidencia. Asimismo, para que la prueba sea válida debe de garantizarse la integridad, autenticidad, etc. en si no existe un protocolo para una evidencia generada por la IA.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

No garantiza plenamente la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas, aunque sí ofrece una base formal importante para su preservación; asimismo, la cadena de custodia puede garantizar que el archivo presentado en juicio es el mismo que fue recolectado, pero no garantiza por sí sola que su contenido sea autentico.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia puede probarse por medio de un análisis entre la finalidad declarativa de la norma y sus efectos son de carácter prácticos en casos concretos, pese a tener una normativa vigente como la Ley N.º 32314, existen dificultades al momento de sancionar de forma efectiva este tipo de conductas en casos como la suplantación de identidad mediante el uso de la inteligencia artificial siendo una brecha entre la regulación y realidad para que sea una ley eficiente. Asimismo, tengo que resaltar que ante la ausencia de herramientas técnicas obligatorias se demuestra insuficiencia probatoria. Por tal motivo, si el sistema no garantiza prevención, ni reparación, resulta siendo insuficiente y limitada para estos delitos.

-
8. **¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.**

Implica la protección efectiva de la identidad, datos y entornos digitales frente a accesos indebidos, manipulación o suplantación. La Ley 32314 modifica el Código Penal, pero no establece mecanismos preventivos de protección de datos, no desarrolla herramientas específicas para restitución de identidad digital, y contempla reparación integral especializada para víctimas de deepfake o clonación de voz.

9. **¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?**

La falta de una regulación específica y sistemática sobre seguridad digital si puede contribuir a la revictimización de las personas afectadas.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. **¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?**

Puede afectar la correcta tipificación práctica cuando el delito se comete mediante inteligencia artificial.

11. **¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.**

Considero que existe un vacío normativo respecto a la manipulación de datos biométricos, ya sea voz o imagen mediante el uso de algoritmos que sean avanzados, debido a que si no se sienten peritos y pruebas digitales idóneas, sería peligroso atribuirle un conducta delictiva a una persona y difícil demostrar la autoría o coautoría, en la actualidad la norma ha sido concebida dentro de un contexto tecnológico complejo y distinto a la realidad tecnológica de las unidades de investigación, sin prever la sofisticación en el marco de la realidad peruana, la cual es muy distinta a países como China, Alemania y España sobre los sistemas de simulación digital, ante la falta expresa de medios tecnológicos, generando graves controversias interpretativas, evidenciándose una latente necesidad de actualización legislativa pero equiparable a los sistemas tecnológicos y operativos.

12. **Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?**

Desde el enfoque de la dogmática, el principio de legalidad está habilitado, efectivamente el cuerpo normativo de la Ley 32314, si cumpliría este requisito, pues tipifica la utilización de inteligencia artificial como agravante en conductas delictivas

como la suplantación de identidad, sin embargo, en la práctica los sistemas operativos, todavía no se encuentran actualizados y modernizados para su calificación e interpretación por carecer de renovación, termina siendo obsoleto. Además, tener presente que contar con sistemas de alta tecnología tiene un costo elevado lo cual preciso dentro del presupuesto termina siendo escaso ante la falta de inversión pública. Por otro lado, la taxatividad exige que la conducta delictiva esté definida con precisión suficiente para que el ciudadano y el juez puedan reconocerla y aplicarla por lo cual desde mi opinión y experiencia terminaría siendo una ley inoperable “letra muerta” comúnmente denominado, existe en esencia la ley, pero no se puede ejecutar porque no se cuenta con lo básico y necesario.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Salas de Torres Mery

Cal: 77324



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	23/02/2026
Grupo/Sector:	Abogado
Entrevistado:	Roger Ureta Condor
Cargo:	Abogado Litigante
Grado Académico:	Superior Universitaria

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N.º 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N.º 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

La inoperancia se evidencia en la ausencia de una definición técnica clara sobre suplantación mediante sistemas de inteligencia artificial, especialmente frente a fenómenos como deepfakes o clonación de voz. La norma mantiene un enfoque tradicional del fraude informático sin incorporar las particularidades de la generación sintética de identidades. Ello dificulta la delimitación típica y genera interpretaciones extensivas que afectan la seguridad jurídica. En la práctica fiscal, se observa que los operadores recurren a tipos penales conexos por falta de precisión normativa. Esta deficiencia impacta en la formulación de imputaciones concretas. Además, la ley no contempla estándares probatorios diferenciados para entornos algorítmicos. Como consecuencia, la persecución penal se torna reactiva y no preventiva. Ello revela una brecha entre la evolución tecnológica y la respuesta legislativa.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Desde una perspectiva técnica, la ley resulta insuficiente frente a la sofisticación actual de la criminalidad digital. La inteligencia artificial permite crear identidades sintéticas con alto grado de verosimilitud. La norma no regula expresamente estas modalidades emergentes. Tampoco contempla criterios de prevención tecnológica. Su enfoque es esencialmente sancionador y no preventivo. Carece de articulación con políticas de ciberseguridad. Además, no integra estándares internacionales en materia de delitos tecnológicos. Por ello, su adecuación es parcial y limitada. Requiere actualización urgente.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

No se observa una mejora sustancial en la capacidad investigativa. La ley no ha venido acompañada de fortalecimiento institucional. Sin capacitación técnica, la norma pierde eficacia real. Los fiscales enfrentan limitaciones probatorias complejas. Además, la ausencia de peritos especializados dificulta la acreditación del ilícito. La tipificación continúa siendo genérica. Esto limita la precisión de la imputación. Por ende, la mejora es marginal. La brecha tecnológica persiste.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Es importante resaltar que los aspectos inoperantes de la normativa señalada radica en la falta de una regulación que identifique los tipos penales más específicamente sobre el ámbito probatorio respecto a los contenidos o delitos generados por el uso de la inteligencia artificial, toda vez que, la ley no explica los criterios técnicos ni los diferencia, ante la falta de recursos tecnológicos no se ajusta a la realidad de las nuevas modalidades en estos delitos ello genera una inseguridad jurídica, ya que los protocolos para establecer la materialidad de este delito es limitado cuando se aborda integralmente en el campo tecnológico de los entornos digitales por lo cual requiere de una adecuación o modificatoria más clara y taxativa de la normativa literalmente.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Desde el punto de vista técnico, otra de las complicaciones es la falta de intervención tecnológica en lo que comprende a la evidencia digital. Es menester mencionar que muchas veces los contenidos manipulados por medio de la IA pueden suprimirse, cambiar o tener replicas en múltiples servidores en pocos minutos. Por tal motivo, la obtención sería lenta para este compromete en la integridad probatoria. Asimismo, muchas plataformas realizan los denominados cifrados de extremo a extremo, lo cual termina dificultando la recuperación de los metadatos originales, por lo que muchas veces el avance digital supera la capacidad reactiva institucional.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

En términos generales, la cadena de custodia digital vigente no garantiza plenamente la autenticidad de contenidos generados por IA. Si bien existen protocolos para preservación de dispositivos y archivos electrónicos, estos fueron diseñados para evidencia digital convencional. Los deepfakes presentan alteraciones imperceptibles al análisis ordinario. La autenticidad requiere herramientas avanzadas de verificación algorítmica. Sin certificación técnica especializada, la integridad puede ser cuestionada en juicio. La defensa podría alegar manipulación posterior. Esto debilita la eficacia probatoria. Se necesita actualización metodológica urgente.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia puede probarse mediante un análisis comparativo entre la finalidad declarativa de la norma y sus efectos prácticos en casos concretos. Si, pese a la vigencia de la Ley N.º 32314, persisten dificultades para sancionar eficazmente conductas de suplantación con IA, se evidencia una brecha entre regulación y eficacia real. Asimismo, la ausencia de herramientas técnicas obligatorias para la protección de datos biométricos demuestra insuficiencia normativa. La autodeterminación informativa implica control sobre los propios datos. Si el sistema no garantiza prevención ni reparación efectiva, la ley resulta funcionalmente limitada. La prueba puede sustentarse en jurisprudencia incipiente y estadísticas fiscales. También en informes técnicos sobre limitaciones periciales. Todo ello revela ineficacia estructural.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

La Ley N.º 32314 protege la autodeterminación informativa de manera indirecta, al tipificar conductas relacionadas con la suplantación de identidad. No obstante, su enfoque es predominantemente penal y reactivo. La protección del dato personal frente a manipulación algorítmica exige mecanismos preventivos y técnicos que la norma no desarrolla expresamente. No se establecen obligaciones específicas sobre tratamiento automatizado de datos biométricos. Tampoco se regulan medidas de seguridad diferenciadas para entornos de IA generativa. Por tanto, la tutela resulta parcial. La norma sanciona el resultado, pero no regula adecuadamente el riesgo tecnológico previo. Existe un vacío en protección integral.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Sí, la ausencia de regulación específica en materia de seguridad digital puede generar revictimización. Cuando el ordenamiento no establece mecanismos de protección inmediata, la víctima permanece expuesta a la circulación continua del contenido manipulado. En casos de deepfakes o clonaciones de identidad, la difusión masiva amplifica el daño. La falta de protocolos claros de eliminación rápida prolonga la afectación. Además, la demora en investigaciones incrementa la incertidumbre jurídica. Esto impacta en la dignidad y reputación de la persona. La revictimización se produce por omisión normativa. La protección debe ser preventiva y no meramente reactiva.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

La inoperancia incide en la falta de claridad respecto al elemento subjetivo del tipo, particularmente en la determinación del dolo cuando intervienen sistemas automatizados. La norma no precisa si basta la creación del contenido falso o si se requiere un propósito específico de daño. Esta ambigüedad afecta la seguridad jurídica y genera interpretaciones dispares. Ello repercute en la predictibilidad de la sanción penal.

- 11. ¿Considera que el artículo 9° de la Ley N.° 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.**

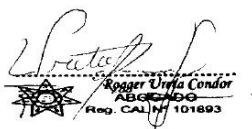
El artículo 9 de la Ley N.° 30096 establece una tipificación orientada a la suplantación informática, pero no contempla expresamente la utilización de inteligencia artificial generativa. Aunque podría aplicarse por interpretación sistemática, su redacción no describe con precisión las nuevas modalidades tecnológicas. Esto genera dudas en la adecuación típica cuando se emplean herramientas automatizadas. Por tanto, la subsunción no siempre resulta clara ni uniforme.

- 12. Desde una perspectiva dogmática, ¿la Ley N.° 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?**

Desde la dogmática penal, el principio de legalidad exige que la conducta prohibida esté descrita de manera clara y previa. Si la Ley N.° 32314 emplea conceptos abiertos o indeterminados respecto a tecnologías emergentes, podría vulnerar la exigencia de taxatividad. La falta de precisión semántica genera inseguridad jurídica. En consecuencia, el respeto al principio dependerá de la claridad de su redacción normativa.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Roger Ureta Condor
ABOGADO
Reg. CAL N° 101893

Apellidos y nombres: Ureta Condor Roger

Cal: 101893



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista: 22/02/2026

Grupo/Sector: Abogado Litigante

Entrevistado: Fernando Renzo Abanto Borgoño

Cargo: Fundador y Gerente del estudio Jurídico “ABANTO BORGÑO & BEDOYA-Abogados”

Grado Académico: Superior Universitaria

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N°32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N°32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N°32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

La ineficacia normativa de Ley N.º 32314 se define primordialmente en la brecha existente entre la previsión normativa y la realidad criminológica digital. Si bien esta norma integra el uso de inteligencia artificial, como agravante en delitos específicos y modifica el Código Penal y la Ley de Delitos Informáticos, su esquema responde a un modelo clásico de ciberdelincuencia, que no incorpora estructuralmente las nuevas modalidades de manipulación algorítmica de la identidad digital.

En el ámbito de política criminal, el problema se encuentra en la norma la cual, si bien es cierto que especifica la utilización de la inteligencia artificial como agravante, lo es también que no desarrolla completamente los supuestos fácticos específicos de suplantación de identidad utilizados con las mediante tecnologías de producción y generación de materiales digitales, tales como deepfakes, clonación de voz, identidades sintéticas o manipulación biométrica digital. Este punto de deficiencia crea complicaciones de subsunción típica en los operadores de justicia.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

En el ámbito jurídico-penal, la promulgación de Ley N.º 32314 constituye un progreso relevante en el interior del sistema penal peruano, al identificar claramente el uso de inteligencia artificial como instrumento potencial para la comisión de delitos y sus agravantes en las conductas ilícitas son realizadas con tecnologías basadas en inteligencia artificial o herramientas digitales análogas. No obstante, en lo dogmático y criminológico, el punto de vista del legislador podría definirse como parcial. La ley solo está limitada en el incremento de las penas o a insertar agravantes; sin embargo, no define una tipificación independiente de los delitos que son derivados de manipulación algorítmica de identidad digital, lo que disminuye su eficacia preventiva y represiva.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

El uso de inteligencia artificial como agravante penal es un importante avance en el sistema penal de nuestro país. No obstante, los avances en las técnicas de investigación utilizadas por el sistema penal, están enmarcadas tanto en la utilización

de las normas penales y la utilización de infraestructura institucional para efectivizar su campo de acción. En ese sentido, como parte de la investigación de delitos informáticos, es un desafío lograr estándares altos por las limitaciones estructurales y profesionales, básicamente con la escasez de peritos especializados en informática forense, análisis algorítmico y verificación de contenido digital.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

La falta de regulación detallada, sobre el procesamiento de la evidencia digital, generada mediante inteligencia artificial. La falta de establecer puntualmente los procesos específicos de investigación digital, hace difícil la generar una respuesta de criterios estandarizados en estos casos en sedes tanto fiscales como judiciales

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

La obtención de evidencia digital en este tipo de acciones punibles, evidencia varias complicaciones técnicas y jurídicas. Una de las principales es la volatilidad de la información digital, ya que muchos contenidos pueden eliminarse o modificarse rápidamente en entornos digitales. Por otro lado, los programas por ejemplo de anonimización y encriptación utilizados en internet hacen difícil identificar plenamente al autor material del este tipo de delitos, lo cual dificulta la atribución de responsabilidad penal individual.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

La cadena de custodia digital, en el ámbito penal, es un instrumento básico para reforzar la integridad, autenticidad de la evidencia electrónica; no obstante, ante contenidos generados por inteligencia artificial, como deepfakes, clonaciones de voz o identidades sintéticas, su eficacia es regular. La principal problemática está en que las formalidades tradicionales de cadena de custodia tuvieron como fin la evidencia digital convencional, estos son: archivos, correos electrónicos, registros de acceso y no para material algorítmicamente alterado, cuya falsedad puede no es fácilmente perceptible por la vista humana.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

Los defectos de Ley N.º 32314 logran evidenciar que pese a integrar la inteligencia artificial como factor de agravación en delitos específicos, no profundizan en técnicas suficientes de tutela efectiva ante la lesión del derecho fundamental, entendido como la facultad que tiene toda persona de controlar el uso, circulación y tratamiento de sus datos personales. Asimismo, la ley no instaura métodos inmediatos de neutralización tecnológica, como bloqueo urgente de contenidos, inmovilización digital, lo que revela una brecha entre sanción penal posterior y protección real del derecho afectado.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

La protección es actualmente parcial, toda vez que si bien identifica riesgo penal determinado por el uso de inteligencia artificial; no obstante, omite la incorporación de una tutela integral, direccionada puntualmente a controlar el dato personal distorsionado algorítmicamente.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Sí, porque en delitos cometidos mediante inteligencia artificial el daño no termina con la acción inicial, sino que se amplifica en cuanto el contenido permanezca accesible, replicable o redistribuible digitalmente. La revictimización sucede cuando continua la exposición de la víctima a nuevas reproducciones del contenido ilícito, comentarios en redes sociales, el menoscabo de la reputación, lo cual conlleva a la afectación emocional prolongada, inclusive durante el trámite judicial. En base a la teoría del daño penal, esta circunstancia constituye una lesión dinámica y expansiva, diferente al delito base de resultado instantáneo, toda vez que el perjuicio a la parte agraviada se reactualiza cada vez que el contenido vuelve a circular.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

La inoperancia normativa impacta porque diversas acciones de inteligencia artificial no se encuentran enmarcadas en sistemas típicos tradicionales en lo penal.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

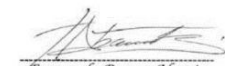
Ley N.º 30096 pone a disposición una base normativa relevante; no obstante, el artículo 9 no determina en un ámbito totalitario los supuestos de suplantación llevados a cabo mediante inteligencia artificial generativa. La dificultad estriba en que el tipo fue generado para la usurpación digital convencional, no para creación algorítmica de identidades. Por ejemplo, cuando existe clonación de voz, rostro o comportamiento digital, en estos casos la conducta excede los conceptos tradicionales de suplantación simple.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Dogmáticamente, la ley constituye un progreso, pero mantiene confrontaciones con el principio de taxatividad penal. La inteligencia artificial es tipificada como medio agravante; sin embargo, en algunos casos no enmarcan conceptos de manera suficiente, motivo por el cual se generan una situación jurídica de incertidumbre al momento de la interpretación en torno a qué tecnología en específico, activa la agravación penal.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Fernando Renzo Abanto
Borgoño
ABOGADO
C.A.L.: 98849

Apellidos y nombres: Abanto Borgoño Fernando Renzo

Cal: 98849



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: "La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025"

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	23/02/2026
Grupo/Sector:	Abogado del Sector Público
Entrevistado:	Klinton Abregu Gaspar
Cargo:	Analista Jurídico
Grado Académico:	Superior Universitaria

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N° 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N° 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N° 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

Sin duda, el avance tecnológico, no solo genera beneficios, sino nuevas problemáticas, que deben ser controlados. En tal sentido, la inoperancia de la Ley se manifiesta básicamente en el tema de especialización del personal del Ministerio Público, y en la implementación de Tecnología capaz de detectar estos ilícitos, y evidenciarlos en un proceso penal, así como en la obtención, validación, preservación y valoración de la evidencia digital.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Evidentemente no, sin embargo, es un avance, que debe ser perfeccionado. Me refiero que es un avance en el sentido que, en el ámbito penal ya se ha considerado como una problemática el uso de la Inteligencia Artificial, sin embargo, a mi consideración el fenómeno que está causando el uso de la Inteligencia Artificial, cada vez se hace inmensamente compleja. Toda vez, que, si es que lo vemos desde una perspectiva individualista, resulta complejo su detección. Ahora, si lo colocamos el uso ilícito de estas tecnologías, en manos de organizaciones criminales altamente complejas. Definitivamente, se requerirá de personas altamente especializada para su entendimiento y posterior sanción. Mientras tanto, la tranquilidad y paz pública seguirán siendo menoscabadas (sociedad con miedo a ser suplantados, estafados, chantajeados, etc.)

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

No ha logrado mejoras efectivas, pero es un comienzo. Podría considerar como mejora el hecho de que el sistema de justicia ya considera la posibilidad de que se hayan cometido la suplantación con ayuda de la Inteligencia Artificial, por lo que debe ser sancionados.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Como lo vengo sosteniendo, si bien es cierto, la referida ley tiene el mérito de evidenciar la problemática del uso ilícito de la inteligencia artificial, necesariamente, está por sí sola no podría sostenerse, puesto que no existen protocolos, directivas o lo que fuera necesario, para evidenciar en un proceso penal; quiero decir, para valorar contenido sintético y obligaciones para que plataformas o proveedores de IA entreguen registros que permitan identificar al auto. Además, no existen normativas sobre el tratamiento de este tipo de evidencias: cómo se debe seguir la cadena de custodia de evidencias digitales. Todas estas dificultades conllevan a que la defensa pueda cuestionarlos con facilidad y caiga en la impunidad. Dado que serán absueltos por duda razonable.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

En la demostración de su autenticidad, por su alta facilidad de manipulación, la no existencia de protocolos para el tratamiento de las pruebas indiciarias de índole digital (una correcta cadena de custodia), más que nada por su volatilidad y facilidad de manipulación. Otra dificultad es que estos ilícitos pueden ser cometidos desde el extranjero, por lo cual se dificulta aún más en la obtención de información e identificación de responsables. La insuficiente capacitación del personal del MP.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

No, puesto que, ante su gran facilidad de alteración de datos digitales, y la inexistencia de protocolos adecuados para su cadena de custodia respecto a Inteligencia Artificial, hacen que la información pueda ser cuestionado fácilmente.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia puede tener probanza por medio del análisis comparativo nacional e internacional, sin embargo, existen dificultades para sancionar eficazmente acciones que no pueden perseguirse por los avances tecnológicos ante la ausencia de herramientas tecnológicas de protección de datos por medio de la IA, lo cual ante el estudio estadístico podría dar un estimado del incremento de estos delitos perpetrados así como informes técnicos y capacitaciones internacionales para abordar como vienen combatiendo y trabajando otros países esta problemática.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

Básicamente que la regulación no es suficiente para proteger la autodeterminación informativa ni garantizar la seguridad digital, frente a ilícitos cometidos por IA, dado que la ley no especifica cuando se debe considerar que es un hecho ilícito. Además, no existen protocolos especializados de cadena de custodia que garanticen la autenticidad de los datos obtenidos que tienen el carácter de prueba. En conclusión, es insuficiente las herramientas con los que se cuenta para la persecución de este tipo de delitos.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Por supuesto que sí, dado que no se ejerce adecuadamente el derecho a la efectiva tutela jurisdiccional, que conllevan a la contravención de los derechos de la víctima, como es el derecho a saber la verdad y el derecho a la justicia.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

Nuestro Derecho Penal es básicamente probatorio, en tal sentido, el persecutor del delito debe llegar a la etapa de enjuiciamiento con suficientes elementos probatorios que puedan dotar de credibilidad su teoría del caso. No obstante, en el presente caso se tiene la gran dificultad de que los delitos de suplantación de identidad por Inteligencia de Identidad, deben ser encajados en tipos penales tradicionales, que, desde luego, dificultan en la acreditación de los elementos típicos del tipo penal en específico. Y, la dificultad por falta de protocolos, que permitan validar evidencias digitales provenientes de IA.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

No, porque el artículo 207-A (derogado por la ley 30096), porque esta fue diseñada para conductas tradicionales de falsificación, mas no para técnicas como deepfakes, clonación de voz o identidades sintéticas. En tal sentido, como la suplantación es realizada por la IA, resulta inconsistente adecuarlo en los elementos del tipo penal.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Considero que aún no, dado que para que los operadores de justicia puedan hacer uso de los preceptos normativos, evidentemente, estos deben ser claro y precisos, La Ley en mención, no permite la consolidación del principio de legalidad, por la ausencia de sustento normativo que la contenga respecto a qué es precisamente lo que se está prohibiendo, y a quienes se les debe considerar como responsables. Y de qué manera se puede determinar que un hecho debe responder penalmente. Por lo que, esta falta de especificidad hace imposible la manifestación y del principio de taxatividad. Por lo que la Ley 32314

no garantiza estándares dogmáticos plenos de certeza, previsibilidad y restricción del ius puniendi en el ámbito de los delitos tecnológicos.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Abregu Gaspar Klinton

Cal: 83417



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: "La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025"

Dirigida a abogados expertos en derecho penal

Fecha de entrevista: 09/03/2026

Grupo/Sector:

Entrevistado: Manuel Alvarado Rodríguez

Cargo: Consultor para la Administración Pública

Grado Académico: Magister

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N.º 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N.º 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

La inoperancia de la Ley N.º 32314 se manifiesta principalmente en la brecha entre su contenido formal y su eficacia práctica. Conviene precisar que esta ley no crea tipos penales autónomos de suplantación mediante IA, sino que modifica el Código Penal y la Ley N.º 30096 para incorporar la inteligencia artificial como circunstancia agravante. Así, el artículo 46, literal ñ del Código Penal y el artículo 11, numeral 5 de la Ley de Delitos Informáticos establecen que el uso de IA o tecnologías similares eleva la pena hasta en un tercio por encima del máximo legal. El problema no es, pues, la ausencia de mención normativa, sino la ausencia de una regulación procesal complementaria que permita operativizar estos agravantes. En la práctica limeña, los operadores de justicia carecen de protocolos técnicos para acreditar que un determinado contenido fue generado mediante IA y no por manipulación convencional, lo que hace inoperante el agravante. No existen peritos judiciales certificados en análisis forense de sistemas de IA generativa, ni estándares de cadena de custodia para contenidos sintéticos. En consecuencia, la norma existe formalmente pero no puede ser aplicada eficazmente, configurando una inoperancia de carácter fundamentalmente institucional y procesal.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Desde mi perspectiva profesional, la Ley N.º 32314 representa un avance normativo relevante, pues por primera vez en el Perú se incorpora explícitamente la inteligencia artificial como elemento de la reacción punitiva. La norma modifica el Código Penal y la Ley de Delitos Informáticos para tratar la IA como agravante en delitos como estafa (Art. 196-A, hasta 8 años), difamación mediante deepfakes (Art. 132, hasta 5 años), pornografía infantil con IA (Art. 129-M, entre 6 y 10 años), y los delitos informáticos en general vía el Art. 11 numeral 5 de la Ley 30096. En ese sentido, la norma no es ajena a la realidad tecnológica. Sin embargo, la ley resulta insuficiente para enfrentar los desafíos de la criminalidad digital vinculada a la IA porque adopta una lógica meramente punitiva-agravante, sin acompañarla de la infraestructura institucional necesaria. No establece protocolos de investigación digital específicos para casos de IA, no crea unidades especializadas en el Ministerio Público ni en la PNP, y no prevé obligaciones de colaboración para proveedores de tecnología. Una regulación eficaz requeriría no solo endurecer penas, sino construir la capacidad estatal para probarlas.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

La Ley N.º 32314 no ha logrado una mejora sustancial en la capacidad operativa del sistema penal para investigar, probar y sancionar la suplantación de identidad digital mediada por inteligencia artificial. Si bien la norma introduce herramientas punitivas concretas en particular el agravante del artículo 11, numeral 5 de la Ley 30096 y las modificaciones al artículo 46 del Código Penal estas no han venido acompañadas de reformas institucionales que permitan activarlas eficazmente en la práctica.

El núcleo del problema radica en que el legislador confió en que el marco normativo sería suficiente por sí solo. Sin embargo, la aplicación del agravante por uso de IA exige que la Fiscalía pueda acreditar técnicamente que el contenido fue generado mediante inteligencia artificial, lo que requiere peritos especializados, laboratorios forenses digitales y protocolos de cadena de custodia diferenciados para contenido sintético. Nada de esto fue implementado. La ley delegó al Poder Ejecutivo la emisión de normativa adicional en sesenta días, pero esa regulación complementaria ha avanzado de forma insuficiente, dejando al sistema penal en la misma posición de impotencia técnica que antes.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Los aspectos inoperantes más críticos de la Ley N.º 32314 en materia de evidencia digital son los siguientes. En primer lugar, si bien la norma reconoce el uso de IA como agravante incluyendo referencias explícitas a deepfakes y tecnologías de manipulación de voz e imagen no establece qué estándares técnicos deben cumplirse para acreditar ese agravante ante el órgano jurisdiccional. Esto genera un vacío probatorio determinante: el fiscal que quiere aplicar el agravante del artículo 11, numeral 5 de la Ley 30096 debe demostrar que el contenido fue creado con IA, pero no existe en el ordenamiento una regulación que defina cómo hacerlo. En segundo lugar, no se han establecido cadenas de custodia específicas para contenidos sintéticos generados por IA, cuya naturaleza difiere sustancialmente de la evidencia digital convencional. Los protocolos actuales no contemplan la preservación de los vectores de generación, los modelos utilizados ni los metadatos de creación propios de sistemas generativos. En tercer lugar, la ausencia de peritos judiciales certificados en análisis forense de IA generativa hace que incluso el material técnico recopilado sea difícil de valorar y sustentar en juicio, restando eficacia real a la norma.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Las dificultades son tanto de orden técnico como jurídico. En el plano técnico, destaca la volatilidad inherente de la evidencia digital: los archivos de audio o video generados mediante IA pueden ser manipulados o eliminados en fracciones de segundo, y los metadatos que permitirían identificar su origen algorítmico son fácilmente alterables. Más aún, los modelos de IA generativa actuales no siempre dejan trazas identificables que permitan vincular el contenido con un sistema, plataforma o usuario concreto, especialmente cuando se utilizan herramientas de acceso abierto sin registro de usuario.

En el ámbito jurídico, el principal obstáculo radica en la ausencia de un marco normativo que obligue a las plataformas tecnológicas a conservar y proporcionar a las autoridades los registros técnicos de generación de contenido. La Ley N.º 32314 introduce los agravantes, pero no regula estas obligaciones de colaboración. A ello se suma la falta de convenios internacionales operativos que permitan acceder expeditamente a servidores ubicados fuera del territorio peruano, donde frecuentemente residen los modelos y los datos más relevantes para la investigación.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

La cadena de custodia digital vigente en el Perú no garantiza, de manera adecuada, la autenticidad e integridad de contenidos sintéticos como deepfakes, clonaciones de voz o identidades generadas por IA. Los protocolos actuales fueron diseñados para evidencia digital convencional registros de acceso, capturas de pantalla, documentos electrónicos y no contemplan las particularidades técnicas de los contenidos generados algorítmicamente. En el caso de un deepfake, la cadena de custodia debería incluir no solo el archivo de video, sino el análisis forense del modelo de IA utilizado para su generación, los artefactos audiovisuales característicos del sistema generativo empleado y los metadatos de creación. La Ley N.º 32314 reconoce el deepfake como medio comisivo relevante, pero no establece protocolos específicos para su preservación e incorporación al proceso. En consecuencia, la evidencia de este tipo puede ser fácilmente impugnada en juicio, convirtiendo la cadena de custodia digital en uno de los eslabones más débiles del sistema penal frente a los delitos cometidos mediante IA.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa puede demostrarse a través de un análisis estructural de sus propias limitaciones normativas. La ley incorpora la IA como agravante en el artículo 46 del Código Penal y en el artículo 11 de la Ley 30096, pero no establece mecanismos sustantivos de protección del derecho a la

autodeterminación informativa cuando los datos biométricos de una persona son usados sin consentimiento para entrenar un modelo de suplantación. Este vacío es significativo y puede acreditarse a través del contraste entre el texto legal y la doctrina del Tribunal Constitucional peruano sobre autodeterminación informativa. Adicionalmente, la inoperancia se demuestra mediante el análisis estadístico de expedientes fiscales en Lima, que evidencia altas tasas de archivamiento en casos de suplantación digital por insuficiencia probatoria, precisamente porque el agravante del uso de IA no puede ser acreditado técnicamente. La norma declara proteger la autodeterminación informativa al sancionar la suplantación, pero carece de los instrumentos procesales y técnicos que harían esa protección efectiva frente a los sistemas de IA generativa.

8. **¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.**

La protección que brinda la Ley N.º 32314 al derecho a la autodeterminación informativa es muy limitada y parcial. La norma sanciona agravadamente la suplantación de identidad realizada mediante IA, pero no aborda el ciclo completo de la vulneración: no regula la recolección ni el uso no consentido de datos biométricos para el entrenamiento de modelos de IA destinados a la suplantación, ni establece la prohibición expresa de desarrollar, comercializar o distribuir sistemas de IA diseñados específicamente para suplantar identidades.

En materia de protección de datos personales en contextos de manipulación algorítmica, la ley tampoco incorpora mecanismos eficaces. No prevé el derecho a la eliminación de modelos entrenados con datos personales obtenidos ilícitamente, ni establece obligaciones de transparencia algorítmica para los proveedores de tecnología. En ese sentido, la norma se limita a sancionar el resultado delictivo la suplantación consumada, pero deja desprotegido el proceso previo de captura y procesamiento de datos personales que hace posible esa suplantación, que es precisamente donde reside la vulneración a la autodeterminación informativa.

9. **¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?**

La ausencia de regulación específica sobre seguridad digital en el contexto de la suplantación de identidad por IA genera un ciclo de revictimización que opera en múltiples niveles. A nivel normativo, aunque la Ley N.º 32314 sanciona la conducta, no establece vías expeditas para que la víctima solicite la eliminación inmediata del contenido sintético que la suplanta, ni obliga a los intermediarios digitales a actuar de forma preventiva. A nivel procesal, la víctima carga con la dificultad práctica de probar que el contenido fue generado mediante IA para activar el agravante, lo que supone una carga técnica desproporcionada. A nivel social, la prolongación del daño reputacional derivado de la circulación continua del contenido falso durante toda la duración del proceso penal constituye una forma de revictimización sistémica que la norma no mitiga. La ley no contempla medidas cautelares específicas de retirada urgente de contenido generado por IA, ni reparaciones

integrales diferenciadas para este tipo de daños. En consecuencia, existe una relación causal directa entre la insuficiencia regulatoria en materia de seguridad digital y la revictimización de los afectados.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

La inoperancia de la Ley N.º 32314 tiene impacto concreto en la tipificación penal del delito de suplantación de identidad mediado por IA. El esquema normativo actual construye el delito en dos capas: el tipo base del artículo 9 de la Ley N.º 30096 —que sanciona la suplantación mediante "tecnologías digitales" con penas de 3 a 5 años— y el agravante del artículo 11, numeral 5 de la misma ley, incorporado por la Ley 32314, que eleva la pena hasta en un tercio cuando se emplea IA. El problema de tipificación surge precisamente en la articulación entre ambas capas. Para aplicar el agravante, el fiscal debe acreditar que la suplantación fue realizada mediante IA y no por otros medios digitales. Esto genera una distinción procesal que el sistema penal actual no está en condiciones de resolver técnicamente. Cuando no puede probarse el medio de comisión específico, el caso se procesa solo bajo el tipo base del artículo 9, sin el agravante, lo que subvalora jurídicamente la gravedad real de la conducta. Esta brecha entre la calificación jurídica posible y la calificación jurídica efectiva es en sí misma una manifestación de inoperancia, pues la norma prevé una respuesta diferenciada que la práctica no puede implementar.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

El artículo 9 de la Ley N.º 30096, en su texto vigente modificado por el Decreto Legislativo 1591 de diciembre de 2023, sanciona al que "mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole," con penas de 3 a 5 años. El término "tecnologías digitales" es suficientemente amplio para cubrir el uso de sistemas de IA generativa, por lo que, en principio, existe base típica. Sin embargo, la subsunción no resulta clara cuando la suplantación se realiza mediante IA porque subsisten vacíos normativos relevantes. En primer lugar, el tipo exige que "resulte algún perjuicio", lo que plantea dificultades cuando el daño es difuso, latente o difícil de cuantificar en sus primeras manifestaciones. En segundo lugar, la IA como medio comisivo calificado solo aparece en el artículo 11, numeral 5, como agravante, no en el tipo base, lo que genera un problema dogmático: si el agravante exige probar el uso de la IA, pero el tipo base no lo requiere, la imputación puede descansar en el tipo más general, perdiendo la especificidad normativa que la Ley 32314 pretendía aportar. Esta doble estructura crea zonas de ambigüedad que impactan negativamente en la predictibilidad de la respuesta penal.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Desde una perspectiva dogmática, la Ley N.º 32314 presenta tensiones con los principios de legalidad y taxatividad penal, aunque su análisis requiere matices. La norma introduce la expresión "inteligencia artificial o tecnologías similares o análogas" tanto en el artículo 46 del Código Penal como en el artículo 11 de la Ley 30096. Si bien esta formulación representa un avance frente a la omisión total previa, el término "tecnologías similares o análogas" carece de un contenido técnico-jurídico suficientemente preciso para satisfacer la exigencia de taxatividad que el principio de legalidad impone. El operador jurídico se enfrenta a la pregunta: ¿qué tecnología es "análoga" a la inteligencia artificial a efectos penales? La norma no lo define, y el Poder Ejecutivo tampoco ha emitido hasta la fecha la reglamentación complementaria que la propia ley le encargó producir en sesenta días. Este déficit definitorio no solo afecta la seguridad jurídica del ciudadano, sino que coloca al juez en la posición de tener que realizar interpretaciones extensivas para aplicar el agravante, con el consiguiente riesgo de vulnerar la prohibición de analogía in malam partem. En ese sentido, si bien la ley cumple formalmente con mencionar a la IA, no satisface plenamente el mandato de determinación que el principio de taxatividad exige para los agravantes penales.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Alvarado Rodriguez Manuel



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista: 17 de marzo del 2026

Grupo/Sector: Derecho Penal

Entrevistado: Luis Salomon Felles Damian

Cargo: Abogado Junior

Grado Académico: Abogado

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N°32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N°32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N°32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

Desde mi experiencia, la inoperancia se manifiesta principalmente en la falta de adecuación normativa frente a las nuevas modalidades delictivas basadas en inteligencia artificial, como los deepfakes o la clonación de voz. La ley no define con precisión estas conductas ni establece mecanismos claros de investigación digital, lo que genera vacíos al momento de tipificar y sustentar los casos. En la práctica, esto se traduce en dificultades para encuadrar jurídicamente los hechos y para obtener pruebas idóneas.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Considero que no responde de manera adecuada. Si bien representa un avance, su enfoque aún es general y no aborda de forma específica el uso de inteligencia artificial en la comisión de delitos. La criminalidad digital evoluciona más rápido que la legislación, y actualmente no se cuenta con herramientas normativas suficientes para enfrentar fenómenos como la automatización del fraude o la manipulación de identidad digital mediante IA. Esto limita la eficacia del sistema penal.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

No de manera significativa. En la práctica fiscal, persisten serias dificultades para la obtención de evidencia digital, la trazabilidad de los autores y la validación técnica de los medios probatorios. La ley no ha venido acompañada de protocolos especializados ni de capacitación suficiente para operadores del sistema, por lo que su impacto real en la investigación y sanción de estos delitos aún es limitado.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Principalmente, la ley no desarrolla criterios claros sobre la obtención, validación y valoración de evidencia digital generada mediante inteligencia artificial. No regula, por ejemplo, cómo acreditar la autenticidad o manipulación de contenidos como deepfakes, ni establece estándares técnicos para su análisis pericial. Esto genera inseguridad jurídica y debilita la carga probatoria en estos casos.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Existen varias dificultades. A nivel técnico, la volatilidad de la evidencia digital y el uso de plataformas extranjeras dificultan su acceso y conservación. A nivel jurídico, hay limitaciones en los mecanismos de cooperación internacional y en la autorización oportuna de medidas como el levantamiento del secreto de las comunicaciones. Además, muchas veces no se cuenta con peritos especializados en inteligencia artificial, lo que afecta la calidad del análisis probatorio.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

Considero que no de manera suficiente. La cadena de custodia tradicional no está plenamente adaptada a la complejidad de la evidencia digital generada por IA. Si bien existen protocolos generales, estos no contemplan adecuadamente los riesgos de alteración, replicación o manipulación de este tipo de contenidos, lo que puede comprometer su valor probatorio en el proceso penal.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia puede evidenciarse a partir de casos concretos donde, pese a existir una afectación clara a la identidad digital de la víctima, no se logra una respuesta penal eficaz. Esto se observa en la dificultad para tipificar adecuadamente la conducta, la limitada protección de los datos personales y la ausencia de medidas oportunas para frenar la difusión del

contenido manipulado. En la práctica, la norma no garantiza una tutela efectiva del derecho a la autodeterminación informativa.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

La protección es aún limitada. Si bien la ley reconoce la relevancia de los datos personales, no incorpora mecanismos específicos para enfrentar escenarios de manipulación algorítmica, como el uso de IA para recrear identidades o alterar contenidos. Tampoco establece obligaciones claras para plataformas digitales ni protocolos de respuesta rápida frente a la vulneración de datos, por lo que la tutela del derecho a la autodeterminación informativa resulta insuficiente.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas? Sí, definitivamente. La falta de regulación específica permite que el contenido manipulado continúe circulando sin control, prolongando el daño a la víctima. Además, la ausencia de mecanismos rápidos de eliminación y de protección efectiva de su identidad genera una exposición constante, lo que agrava la afectación psicológica y social. En ese sentido, la deficiencia normativa contribuye directamente a la revictimización.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

Afecta de manera directa, porque al no contemplar de forma expresa las modalidades de suplantación mediante inteligencia artificial, se generan vacíos en la tipificación. Esto obliga a forzar la subsunción en tipos penales tradicionales que no fueron diseñados para estas conductas, lo que debilita la imputación y puede afectar la solidez del caso en sede fiscal y judicial.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

Considero que no permite una subsunción totalmente clara. El artículo 9º regula la suplantación de identidad en entornos digitales, pero no prevé específicamente el uso de inteligencia artificial como medio comisivo. Esto genera vacíos normativos, especialmente en supuestos donde no hay acceso indebido directo a sistemas, sino creación de identidades sintéticas o contenidos falsificados, lo que dificulta encuadrar la conducta de manera precisa, aunado a ello no existe circunstancias agravantes específicas como por ejemplo si los perpetradores son miembros de una banda u organización criminal.

-
12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Desde una perspectiva dogmática, su cumplimiento es parcial. Si bien la ley busca adecuarse a nuevas formas de criminalidad, presenta problemas de indeterminación en la descripción de conductas vinculadas a tecnologías emergentes como la inteligencia artificial. Esto puede generar interpretaciones amplias o ambiguas, lo que tensiona el principio de taxatividad y puede afectar la seguridad jurídica en la aplicación del derecho penal.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Luis Felles Damian
ABOGADO
CAL 103179

Apellidos y nombres:

Cal: 103179



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista: 17/03/2026

Grupo/Sector: Público

Entrevistado: Melissa Nadine Rodríguez Yarasca

Cargo: Asistente en Función Fiscal

Grado Académico:

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N.º 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N.º 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

La inoperancia de la Ley N.º 32314 se manifiesta principalmente en que la norma no crea un tipo penal autónomo para la suplantación de identidad mediante inteligencia artificial, sino que únicamente incorpora el uso de la inteligencia artificial como circunstancia agravante o medio de comisión del delito dentro del Código Penal y la Ley de Delitos Informáticos.

En la práctica, cuando se presentan casos de suplantación mediante deepfakes, clonación de voz o creación de identidades digitales falsas, los operadores jurídicos deben reconducir la conducta a tipos penales ya existentes, como estafa, difamación o suplantación informática. Esto genera dificultades en la tipificación y en la imputación penal, pues la norma no regula de manera específica estas nuevas modalidades tecnológicas.

Por ello, la persecución penal termina dependiendo de interpretaciones extensivas de tipos ya existentes, lo cual limita la eficacia del sistema penal frente a nuevas formas de criminalidad digital.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Desde una perspectiva práctica, la Ley N.º 32314 constituye un avance inicial, ya que reconoce que la inteligencia artificial puede ser utilizada como medio para cometer delitos y permite agravar las penas cuando se utilice esta tecnología.

Sin embargo, la norma resulta insuficiente frente a los desafíos actuales de la criminalidad digital, debido a que no regula de manera integral fenómenos como: la creación de identidades sintéticas, los deepfakes, la clonación de voz, la manipulación algorítmica de información personal. En ese sentido, la ley tiene un enfoque reactivo y no preventivo, ya que se limita a aumentar sanciones sin desarrollar mecanismos específicos para la investigación, prueba o identificación de estos delitos.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

No de manera significativa.

La Ley N.º 32314 incrementa la gravedad de la conducta cuando se utiliza inteligencia artificial, pero no introduce herramientas procesales ni técnicas para la investigación digital. En consecuencia, el sistema penal continúa enfrentando los

mismos problemas que ya existían en los delitos informáticos, como: dificultades para rastrear el origen de contenidos digitales, problemas de jurisdicción cuando los servidores están en el extranjero, limitaciones técnicas en la obtención de evidencia digital. Por ello, aunque la norma aumenta las penas, no mejora de forma real la capacidad investigativa del sistema penal.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Entre los principales aspectos inoperantes se pueden identificar: Ausencia de regulación específica sobre evidencia digital generada por IA. / Falta de criterios legales para determinar la autenticidad de contenidos manipulados, como deepfakes o audios sintéticos. / Falta de protocolos normativos para el análisis forense digital en casos de inteligencia artificial. / Dependencia de normas generales del proceso penal, que no fueron diseñadas para este tipo de tecnología. Esto provoca que, en muchos casos, la evidencia digital sea cuestionada en juicio por problemas de autenticidad o manipulación.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Las principales dificultades son: La volatilidad de la evidencia digital, ya que los contenidos pueden eliminarse o modificarse rápidamente. / La identificación del autor real del contenido, porque la inteligencia artificial permite generar material sin dejar rastros claros. / La ubicación internacional de los servidores o plataformas, lo que complica la cooperación judicial. / La falta de especialistas en informática forense dentro del sistema de justicia. Estas dificultades afectan la recolección, preservación y valoración de la prueba.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

Actualmente, la cadena de custodia digital no siempre garantiza plenamente la autenticidad de este tipo de contenidos, debido a que las herramientas de inteligencia artificial permiten alterar o generar información con gran realismo. Si bien el proceso penal exige asegurar la integridad de la evidencia, no existen protocolos especializados para contenidos generados por inteligencia artificial, lo que puede generar cuestionamientos sobre su origen o manipulación.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

La inoperancia puede demostrarse observando que la ley: no regula de manera específica la protección de la identidad digital, no establece mecanismos claros para la prevención de suplantaciones mediante IA, no desarrolla instrumentos para proteger la autodeterminación informativa de las personas.

Por ello, cuando se produce una suplantación digital, la respuesta penal suele llegar de forma tardía, cuando el daño a la identidad o reputación de la víctima ya se ha producido.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

La protección es limitada. La Ley N.º 32314 se centra principalmente en agravar las penas cuando se utiliza inteligencia artificial para cometer delitos, pero no desarrolla mecanismos específicos de protección de datos personales ni medidas preventivas frente a la manipulación algorítmica. En ese sentido, la protección del derecho a la autodeterminación informativa sigue dependiendo principalmente de otras normas, como la legislación sobre protección de datos personales.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Sí, la falta de regulación específica provoca que las víctimas enfrenten dificultades para: denunciar los hechos, demostrar la manipulación digital, lograr la eliminación rápida del contenido falso. En muchos casos, el material manipulado continúa circulando en internet, lo que prolonga el daño a la reputación, identidad o privacidad de la víctima, generando una forma de revictimización.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

La inoperancia afecta la tipificación porque la ley no define de manera clara la conducta de suplantación mediante inteligencia artificial. Por ello, los fiscales suelen recurrir a tipos penales generales como: suplantación de identidad informática, estafa, difamación, delitos contra la fe pública. Esto puede generar problemas de subsunción típica, ya que no siempre es fácil encajar estas nuevas conductas tecnológicas dentro de tipos tradicionales.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

El artículo 9° de la Ley N.° 30096 regula la suplantación de identidad en entornos informáticos, lo que permite sancionar a quien se hace pasar por otra persona utilizando medios digitales. Sin embargo, cuando la suplantación se realiza mediante herramientas avanzadas de inteligencia artificial, como deepfakes o clonación de voz, la subsunción no siempre resulta clara, porque la norma fue diseñada para formas más tradicionales de suplantación digital. Por ello, pueden presentarse vacíos normativos cuando la conducta implica manipulación audiovisual avanzada o generación automática de identidades.

12. Desde una perspectiva dogmática, ¿la Ley N.° 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

En términos generales, sí respeta el principio de legalidad, ya que no crea delitos indeterminados ni ambiguos, sino que incorpora el uso de inteligencia artificial como medio agravante en delitos ya existentes. No obstante, desde una perspectiva dogmática, puede cuestionarse su grado de taxatividad, porque la norma utiliza conceptos amplios como “inteligencia artificial o tecnologías similares”, lo que podría generar interpretaciones diversas en la aplicación práctica. Por ello, aunque la ley es válida desde el punto de vista del principio de legalidad, aún requiere mayor precisión normativa para enfrentar adecuadamente los delitos tecnológicos.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Rodríguez Yarasca Melissa Nadine

Cal: 95938



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	16/03/2026
Grupo/Sector:	Independiente
Entrevistado:	Alan José Rodríguez Díaz
Cargo:	Abogado Litigante
Grado Académico:	Superior Universitario

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N.º 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N.º 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

Esto se manifiesta principalmente a través de la impunidad técnica. La norma tiene un carácter declarativo, pero carece de herramientas coercitivas y procesales específicas para lograr la identificación de autores que utilizan redes o servidores en el extranjero. La inoperancia es visible cuando el Ministerio Público intenta aplicar tipos penales clásicos a conductas donde el "sujeto activo" es un algoritmo operado anónimamente, resultando en el archivo de denuncias por falta de individualización del presunto autor.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

No responde a ningún desafío, a pesar que se entiende que la ley es un esfuerzo loable pero insuficiente. Se queda en la superficie de la "regulación de uso" sin profundizar en la reforma procesal penal necesaria. Los desafíos de la IA requieren no solo una ley marco, sino protocolos de evidencia digital que la Ley 32314 no detalla, dejando a los operadores de justicia con una norma "letra muerta" ante ataques de material audiovisual falsos.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

No de manera efectiva. Si bien pone el tema en la agenda pública, la capacidad operativa (peritos especializados, software de detección de IA, cooperación internacional acelerada) no ha crecido al ritmo de la ley. Investigar una suplantación con IA en Lima sigue dependiendo de la Ley de Delitos Informáticos N°30096, la cual es previa al auge masivo de la Inteligencia Artificial.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

El principal aspecto es la omisión de estándares de validación para contenido sintético. La ley no establece cómo diferenciar legalmente una identidad real de una identidad sintética (*deepfake*) para efectos de imputación. Además, hay una inoperancia en la obligación de las plataformas tecnológicas de colaborar en tiempo real, lo que hace que la evidencia se pierda antes de que el fiscal emita la disposición de preservación.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

En las dificultades técnicas es la dificultad de rastrear el "prompts" original y la imposibilidad de realizar peritajes de autenticidad sobre archivos que han sido comprimidos por redes sociales (WhatsApp/Telegram), lo que altera los metadatos. Y en el caso de dificultades jurídicas: El conflicto con la privacidad de datos en el extranjero y la demora en las Cartas Rogatorias o asistencias judiciales internacionales, que no son compatibles con la volatilidad de la IA.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

No en su totalidad. La cadena de custodia tradicional (actas de visualización y lacrado) garantiza que el archivo no fue modificado después de su recojo, pero no puede certificar si el origen del archivo es humano o artificial. Se requieren pericias de análisis forense digital avanzado (detección de artefactos algorítmicos) que actualmente no forman parte del estándar básico de la cadena de custodia en las fiscalías corporativas de Lima.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

Se prueba mediante la tasa de reincidencia y victimización. Cuando un ciudadano ve su rostro o voz suplantados por IA y la autoridad no puede retirar dicho contenido de la red ni sancionar al responsable debido a vacíos en la Ley 32314, el derecho a controlar la propia información (autodeterminación) queda anulado. La inoperancia se refleja en la falta de "tutela correctiva" inmediata.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

La protección es nominal. La norma menciona el respeto a los derechos fundamentales, pero no incorpora mecanismos de "bloqueo preventivo" o "derecho al olvido" automatizado cuando se detecta una manipulación algorítmica. Sin una

articulación real con la Autoridad Nacional de Protección de Datos Personales (ANPD), la Ley 32314 es un saludo a la bandera en términos de protección de datos.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Definitivamente. La víctima de suplantación por IA no solo sufre el daño original, sino que debe enfrentar un sistema judicial que cuestiona la veracidad de su denuncia por "falta de pruebas tecnológicas". Al no haber protocolos de atención rápida para delitos cometidos con IA, la exposición del contenido dañino se prolonga, agravando el daño moral y psicológico.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

Genera atipicidad relativa o errores de subsunción. Al no existir una agravante específica o un tipo penal que describa el uso de "tecnologías de generación sintética", los fiscales fuerzan el Art. 9 de la Ley 30096. Esto permite que los abogados defensores aleguen vulneración al principio de taxatividad, logrando que muchas conductas queden sin sanción por no ajustarse exactamente al verbo rector tradicional.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

No es clara. El Art. 9º sanciona a quien "mediante el uso de tecnologías de la información... suplanta la identidad". Sin embargo, la IA permite crear identidades "híbridas" o "sintéticas" que no necesariamente pertenecen a una persona natural viva, o que distorsionan la voluntad de una persona real de formas que la ley no previó en 2013. Existe un vacío en la determinación de la lesividad cuando el daño es puramente algorítmico.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

La Ley 32314 es demasiado ambigua. El principio de taxatividad exige que la conducta prohibida esté descrita de forma precisa. Al ser una norma de carácter general sobre IA, su aplicación al ámbito penal es problemática porque delega mucha interpretación al juez, lo cual podría colisionar con el principio de legalidad si se intenta sancionar analogando comportamientos tecnológicos nuevos a tipos penales antiguos.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Rodríguez Díaz, Alan José

CAL: 101915



Universidad
Norbert Wiener

UNIVERSIDAD PRIVADA NORBERT WIENER

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	18/03/2025
Grupo/Sector:	Abogado
Entrevistado:	Yosseling Yahaira Morales Higinio
Cargo:	Abogada Independiente
Grado Académico:	Cursando Maestría en Derecho de la Empresa y Protección de Datos Personales

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N° 32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N° 32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N° 32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

La inoperancia enmarcada a la ley citada se evidencia en desconexión entre su formulación normativa aplicativa y la complejidad del incremento y avances por parte de las organizaciones criminales con respecto a los delitos realizados en entornos digitales. Si bien la normativa incorpora al delito cibernético el uso de la IA como agravante, no desarrolla de forma oportuna y real las nuevas formas de suplantación de identidad, siendo ello un factor limitante que imposibilita una adecuada subsumción jurídica de las conductas. Por todo lo expuesto, los operadores de justicia y las instituciones responsables de estos casos se enfrentan a vacíos interpretativos. En ese sentido, ello disminuye la posibilidad de una eficacia jurídica dentro del sistema penal, enfrentada a la evolución de las altas tecnologías. Como aporte puedo resaltar que es necesario diseñar una legislación tecnológica penal que incorpore una tipificación autónoma cuando se vea en conflicto los casos de suplantación de identidad por medio de la IA.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Considero desde mi experiencia realizando investigación sobre datos personales como investigadora que la ley representa un avance claro al reconocer el uso de la IA, empero la comisión de estos delitos tiene un alcance limitado al centrarse en agravantes, no se verifica tipos penales autónomos que aborden complicaciones de este fenómeno digital, por lo cual la normativa no puede cumplir su rol preventivo frente a los desafíos digitales actuales.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

Considero que la normativa introduce avances formales al reconocer el uso de la IA, no obstante, su impacto práctico es limitado debido a las dificultades estructurales ante la falta de peritos especializados, toda vez que afectaría las investigaciones ante la falta de infraestructura tecnológica por ser insuficiente, dificultando la obtención de pruebas.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Es primordial resaltar que, ante la falta de una regulación, clara, precisa y detallada respecto al tratamiento de la evidencia digital, todavía no contamos con mecanismos, ni protocolos claros para recolectar, analizar y conservar la inconsistencia en los procesos judiciales y penales, afectando significativamente la validez probatoria, ante la ausencia de un estándar que incrementa los riesgos de nulidades por la persecución de este delito nuevo empleándose las nuevas tecnologías. Por tal motivo, se deben incorporar protocolos para el tratamiento jurídico de la evidencia digital.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Una de las principales dificultades es la volatilidad información digital y los contenidos que constituyen un obstáculo relevante, referente a contenidos que requieren de una eliminación o modificación con proximidad. Esto implica que los contenidos recolectados tardarían en ser modificados o suprimidos del ciberespacio al comprometer su validez, dificultando su preservación y afectando la trazabilidad de dicha evidencia, siendo necesario fortalecer los mecanismos de cooperación y los sistemas de preservación que tengan inmediatez para la obtención de la evidencia digital.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

Desde mi punto de vista, bajo un criterio analítico es relevante indicar que los deepfakes y tecnologías similares desafían los métodos comunes para validarlos, dicha cadena de custodia no garantiza eficientemente la integridad de todos los contenidos en lo que respecta a la credibilidad del proceso, por lo que se necesita una actualización y gestión pública adecuada para modernizar esta cadena implementando tecnologías de verificación digital.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

En el caso de probar la inoperancia, se puede advertir que existe una gran brecha entre lo penal y la protección efectiva de los derechos fundamentales cuando se trata de uso de tecnologías ante la ausencia de contención. Es menester indicar que, la ley no puede cumplir con su funcionalidad protectora al no contar con mecanismos óptimos para su ejecución y aplicación con recursos que permitan garantizarlo, por lo que se debe adecuar medidas cautelares digitales de carácter inmediato, citando por ejemplo bloqueos, alertas y eliminación de contenidos delictivos generados por la IA.

-
8. **¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.**

Para esta interrogante es importante señalar que la medida en la normativa se manifiesta ante el derecho a la autodeterminación es escasa, toda vez que, no articula un enfoque de carácter garantista e integral, si bien es cierto no todas las normas pueden ser garantistas por las implicancias que se presentan en su interpretación, empero en los casos de protección de datos personales, no se cuentan con herramientas óptimas para ejercer un control del uso ilícito e indebido de estos datos, en donde no solo se afecta la seguridad digital sino también la integridad psicológica de las víctimas, resulta siendo limitada. Es necesario integrar a la normativa penal una regulación más protectora de datos personales.

9. **¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?**

Considero que la falta de una regulación específica genera un impacto en el contenido digital para poder perseguir este delito, dado que una nueva difusión rechazaría el daño y afectaría la reputación y estabilidad emocional, toda vez que, no cuenta con mecanismos de protección, por lo que la víctima sufre reiteradamente de estos hechos y delitos, debiendo establecerse mecanismos legales para eliminar de forma obligatoria su desindexación de los contenidos fraudulentos.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. **¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?**

Las nuevas formas o modalidades delictivas superan los esquemas clásicos del derecho penal en la normativa no logra abarcar estas conductas, limitando la persecución de este delito frente a la falta de capacitación que enfrentan los operadores al no lograr abarcar estas conductas, generando una carencia de eficacia al sistema, siendo necesario crear tipos penales específicos de delitos enfocados en IA.

11. **¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.**

Considero que el tipo penal responde a escenarios tradicionales o comunes de la práctica y ejercicio de estos delitos, más no incorpora supuestos en casos de manipulación algorítmica, dificultando la subsunción típica para su identificación y agravantes, la normativa actual resulta siendo desactualizada ante los estándares tecnológicos para proteger integralmente a las víctimas y perseguir estos delitos, por lo cual se requiere una respuesta a la falta de protocolos y mecanismos, siendo

relevante realizar una adecuación a la normativa que sea más específica, agregando supuestos de suplantación por medio del empleo de la IA.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Desde el ámbito de la literatura, jurisprudencia y dogmática así como la doctrina, existe una falta de claridad limitada en la previsibilidad normativa para tratar jurídicamente estos delitos, al no establecer parámetros definidos al caso en concreto y la realidad jurídica peruana, afectando directamente la seguridad jurídica y digital para las personas ante la falta de protección y prevención normativa a estas nuevas tendencias en delitos tecnológicos, debilitando la legalidad, siendo necesario desarrollar definiciones, protocolos y herramientas para el uso de la IA en el ámbito penal.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:


Yosseling Yahaira Morales
Higinio
 ABOGADA
C.A.L.: 101336

Apellidos y nombres: Morales Higinio Yosseling Yahaira

Cal: 101336

Para optar por el Título Profesional de Abogada

TESIS: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Dirigida a abogados expertos en derecho penal

Fecha de entrevista:	18/03/2026
Grupo/Sector:	Abogado
Entrevistado:	Mondaca Bejar Edgar Alcides
Cargo:	Abogado Litigante
Grado Académico:	Superior Universitario

Introducción:

El acelerado desarrollo de la inteligencia artificial ha transformado las dinámicas delictivas vinculadas a la suplantación de identidad, generando nuevas modalidades de afectación a derechos fundamentales como la identidad, la privacidad y la seguridad digital. En este contexto, el uso de tecnologías como la clonación de voz, la manipulación de imágenes y los sistemas automatizados de generación de contenido ha desbordado los esquemas tradicionales de persecución penal. Frente a ello, el ordenamiento jurídico peruano ha intentado responder mediante la Ley N°32314; sin embargo, su aplicación en la práctica evidencia serias limitaciones. Estas deficiencias normativas impactan directamente en la eficacia del sistema penal para enfrentar delitos tecnológicos complejos. Por ello, resulta necesario analizar críticamente su funcionamiento real.

Desde la perspectiva del problema general, la investigación se centra en determinar de qué manera se manifiesta la inoperancia de la Ley N°32314 en la persecución del delito de suplantación de identidad cometido mediante inteligencia artificial en Lima. Esta inoperancia se expresa en dificultades probatorias, vacíos normativos y una débil articulación entre el derecho penal sustantivo y la evidencia digital. Asimismo, los operadores de justicia enfrentan obstáculos técnicos y jurídicos para adaptar las herramientas tradicionales de investigación a entornos digitales avanzados. Estas limitaciones afectan la protección efectiva de las víctimas y la respuesta penal oportuna. En consecuencia, se evidencia una brecha entre la norma y la realidad tecnológica actual.

En relación con los problemas específicos, el estudio aborda, en primer lugar, los aspectos inoperantes de la Ley N°32314 vinculados al tratamiento de la evidencia digital en delitos de suplantación de identidad con inteligencia artificial. En segundo término, se analiza cómo dicha inoperancia incide en la protección de la autodeterminación informativa y la seguridad digital de las personas afectadas. Finalmente, se examina el impacto de estas deficiencias en la correcta tipificación penal del delito, lo que genera inseguridad jurídica y dificultades en la imputación penal. El análisis integral de estos aspectos permitirá evidenciar la necesidad de ajustes normativos y criterios interpretativos más acordes con los avances tecnológicos. De este modo, la investigación contribuye al debate jurídico sobre la adecuación del derecho penal frente a la inteligencia artificial.

OBJETIVO DEL INSTRUMENTO

Recoger información especializada para analizar críticamente la inoperancia de la Ley N.º 32314 en la persecución penal del delito de suplantación de identidad cometida mediante inteligencia artificial en Lima.

BLOQUE I – VALORACIÓN GENERAL DE LA LEY 32314

Objetivo General: Analizar de qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima.

1. ¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?

Considero que la inoperancia de esta normativa se traslada en la ausencia de agravantes específicos para materializar estos delitos por medio de las tecnologías modernas como la Inteligencia Artificial en la nueva era del derecho digital, y dentro de la esfera peruana, es de suma importancia operativizar y mejorar las instituciones a través de la transformación digital y gobierno digital para modernizar las instituciones del Estado que son partícipes de reducir estos delitos.

2. Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.

Desde mi experiencia como abogado penalista, he tenido clientes que han presentado denuncias por el empleo de la IA en delitos, sin embargo, su persecución es carente, debido a que no existen mecanismos de protección digital para las víctimas. En ese contexto, puedo indicar que existe un trabajo de parte del Estado y las instituciones para actualizarse a estas nuevas tendencias delictivas y lograr eficazmente sancionarlo.

3. ¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?

En el caso en particular, el sistema penal no cuenta con herramientas tecnológicas necesarias y básicas para proteger a las víctimas de manera integral, contamos con muchas leyes modernizadas, pero muchas veces no se ajustan al contexto peruano normativo y a la realidad problemática, por la falta de equipamientos, recursos y capacitación de las autoridades competentes.

OE1: Analizar los aspectos inoperantes de la Ley N.º 32314 que evidencia de manera digital en la persecución del delito de suplantación de identidad a través inteligencia artificial.

4. ¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través inteligencia artificial?

Uno de los aspectos más relevantes es que no contamos con herramientas que permitan recopilar y resguardar la evidencia digital, por lo cual se puede perder sino se logra reservar a tiempo con mecanismos tecnológicos. Por ejemplo, los

ciberdelinquentes se manifiestan por hackers crean bases de datos y luego las eliminan, perseguirlas es insuficiente y casi imposible sino se cuenta con un sistema mejor al que emplean para sus hechos delictivos.

5. ¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?

Una de las dificultades más relevantes que he identificado en mi experiencia, se basa en que existe un mercado negro que vende información personal y datos de las personas, vulnerando todos los sistemas como por ejemplo, entidades bancarias, RENIEC y demás entidades como ESSALUD y el SIS que todavía tienen acceso a datos personales, así como páginas clandestinas que una vez que detectan su origen desaparecen del ciberespacio, por lo cual el principal problema a tratar son webs, plataformas y sancionar programas o canales como telegram que filtran un banco de información de los usuarios que terminan siendo víctimas de estos sujetos delictivos que emplean la tecnología.

6. Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?

Esta pregunta es ambigua, dado que mientras exista gente que consuma estos mercados clandestinos, los delitos no cesarán y la integridad de las víctimas se verá cada vez más vulnerable ante la falta de protección y garantía estatal para perseguir estas organizaciones criminales.

OE2: Evaluar como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial.

7. ¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?

Para probar la inoperancia se puede evidenciar que la falta de mecanismos inmediatos y preventivos no prioriza la sanción ni persecución del delito posterior al hecho por la falta de herramientas tecnológicas y sistemas operativos que se adecuen a estas nuevas tendencias digitales como la IA, por lo cual se genera una desprotección y tutela insuficiente.

8. ¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.

Considero que no se garantiza ni protege el derecho a la autodeterminación informativa frente a estos delitos modernizados por la IA, debido a que la protección de datos personales es vulnerable en la actualidad y no se puede probar la conducta delictiva ante la ausencia de tecnologías optimizadas a estos nuevos delitos.

9. ¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?

Creo que las leyes no deben modificarse planamente, ya que generan un impacto que repercute en la eficacia legal de las normas respecto a su aplicación en el ámbito en el que se desean abordar, por no ajustarse a la realidad actual y podría generar repercusión o confusión al revictimizar a las víctimas usando desproporionalmente las entidades.

OE3: Analizar en qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial.

10. ¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?

La falta de regulación permite la persistencia de un daño generado en un entorno digital ante un contenido ilícito, exponiendo reiteradamente a las víctimas, ante una afectación prolongada en los casos donde el tipo penal no es claro con respecto a los agravantes por IA y suplantación de identidad.

11. ¿Considera que el artículo 9º de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.

La inoperancia legal genera un impacto en la adecuación típica referida a conductas, donde muchas veces las acciones no encajan al tipo penal común o antiguo, generando vacíos legales en la imputación penal por la existencia de inseguridad jurídica en lo que respecta a la nueva era digital.

12. Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?

Desde una perspectiva dogmática la ley proporciona si bien una base normativa relevante, no obstante; no contempla adecuadamente la inteligencia artificial en sus modalidades, siendo su alcance limitado.

Agradezco su tiempo y aporte. Se le informa que el contenido de la presente entrevista será utilizado exclusivamente para fines académicos lo cual contribuirá al fortalecimiento del campo del derecho.

Al final se le solicita respetuosamente pueda firmar y dejar constancia de su participación:



Apellidos y nombres: Mondaca Bejar Edgar Alcides

Cal: 96257

Anexo 3: Evaluación de Rigurosidad del Instrumento

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 1/ DELITO DE SUPlantACIÓN DE IDENTIDAD							
1	¿De qué manera se manifiesta la inoperancia de la Ley N.º 32314 en la persecución del delito de suplantación de identidad a través inteligencia artificial en Lima?	x		x		x		
2	Desde su experiencia profesional, ¿considera que la Ley N.º 32314 responde adecuadamente a los desafíos actuales de la criminalidad digital vinculada a la inteligencia artificial? Fundamente.	x		x		x		
3	¿Cree usted que la Ley N.º 32314 ha logrado mejorar efectivamente la capacidad del sistema penal para investigar, probar y sancionar la suplantación de identidad digital?	x		x		x		
	DIMENSIÓN 2/ INTELIGENCIA ARTIFICIAL	Si	No	Si	No	Si	No	
4	¿Cuáles son los aspectos inoperantes de la Ley N.º 32314 que se dan mediante la evidencia digital en la persecución del delito de suplantación de identidad a través de la inteligencia artificial?	x		x		x		
5	¿Qué dificultades técnicas o jurídicas identifica en la obtención y preservación de evidencia digital cuando se investiga una suplantación de identidad basada en IA?	x		x		x		
6	Desde su criterio, ¿la cadena de custodia digital actualmente garantiza la autenticidad e integridad de contenidos como deepfakes, clonaciones de voz o identidades sintéticas?	x		x		x		
7	¿Como probar la inoperancia de la Ley N.º 32314 frente a la autodeterminación informativa y seguridad digital en la persecución del delito de suplantación de identidad con inteligencia artificial?	x		x		x		
8	¿En qué medida la Ley N.º 32314 protege el derecho a la autodeterminación informativa, frente al uso ilícito de sistemas de inteligencia artificial? Explique, si la norma incorpora mecanismos eficaces para la protección de datos personales en contextos de manipulación algorítmica.	x		x		x		

9	¿Cree que la falta de regulación específica sobre seguridad digital contribuye a la revictimización de las personas afectadas?	x		x		x		
10	¿En qué medida la inoperancia de la Ley N.º 32314 afecta una correcta tipificación penal del delito de suplantación de identidad que se da a través de inteligencia artificial?	x		x		x		
11	¿Considera que el artículo 9 de la Ley N.º 30096 permite una subsunción típica clara cuando la suplantación se realiza mediante inteligencia artificial? Explique, si existen vacíos normativos en la actual tipificación penal.	x		x		x		
12	Desde una perspectiva dogmática, ¿la Ley N.º 32314 respeta el principio de legalidad y taxatividad penal en delitos tecnológicos?	x		x		x		

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Observaciones (precisar si hay suficiencia): Correcto

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador: Gino Raúl Romero Curioso

DNI: 07425522 / CAL: 22604 / Grado: Magister en Derecho Penal e Constitucional



Mg. Gino Raúl Romero Curioso

Anexo 4: Consentimiento informado

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEL-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 23-02-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO:	VERSION: 01
	UPNW-EES-FOR-068	FECHA: 23-02-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio. Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Mery Salas De Torres
DNI: 449927695
Fecha: 23/02/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 23/02/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 23-02-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01 FECHA: 23-02-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

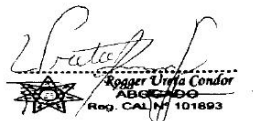
Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Rogger Ureta Córdor
ABOGADO
Reg. CAJ. N° 101893

Participante: Rogger Ureta Córdor
DNI: 72553139
Fecha: 23/02/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 23/02/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 22-02-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 22/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema relativo “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 22-02-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasiona ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comité.etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Fernando Renzo Abanto
Borgoño
ABOGADO
C.A.L. 98849

Participante: Fernando Renzo Abanto Borgoño
DNI: 25787877
Fecha: 22/02/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 22/02/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 23-02-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema relativo “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 23-02-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comité.etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Klinton Abregu Gaspar
DNI: 47646286
Fecha: 23/02/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 23/02/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 09-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 09/03/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema relativo “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO:	VERSION: 01
	UPNW-EES-FOR-068	REVISION: 01

FECHA: 10-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comité.etica@uwienner.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Manuel Alvarado Rodriguez
DNI: 05282279
Fecha: 09/03/2026



Investigador (a): María Jesús Díaz Aldaz
DNI: 72169470
Fecha: 09//03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 17-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01 FECHA: 17-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.


Luis Felles Damian
 ABOGADO
 CAL 103179

Participante: Luis Felles Damian
DNI: 74450244
Fecha: 17/03/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 17/03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 17-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 17-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Melissa Nadine Rodríguez Yarasca
DNI: 72531727
Fecha: 17/03/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 17/03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 16-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 16-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Alan Rodríguez Díaz
DNI: 45072994
Fecha: 16/03/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 16/03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 18-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 18-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comité.etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.


 Yosseling Yahaira Morales
 Higinio
 ABOGADA
 C.A.L.: 101336



Participante: Yosseling Morales Higinio
DNI: 47493577
Fecha: 18/03/2026

Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 18/03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

	FORMULACION DE CONSENTIMIENTO INFORMADO(DCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI		
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01	FECHA: 18-03-2026

Título de proyecto de investigación: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”

Investigadores : Jesús María Díaz Aldaz

Institución(es) : Universidad Norbert Wiener

Estamos invitando a usted a participar en un estudio de investigación titulado: “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. de fecha 23/02/2026 y versión. 01. Este es un estudio desarrollado por investigadores de la Universidad Privada Norbert Wiener (UPNW)

I. INFORMACIÓN

Duración del estudio (meses): 6 meses

Nº esperados de participantes: 10

Criterios de inclusión y exclusión: Expedientes de Protección de datos / Abogados Penalistas.

Procedimientos del estudio: si Usted decide participar en este estudio se le realizara los siguientes procesos:

- Se realizará una entrevista.
- Serán un numero de preguntas que deberá contestar.
- Puede durar 45 min. Aproximadamente.

La entrevista/encuesta puede demorar unos 45 minutos con la finalidad de conocer sus puntos de vista como especialista en el tema “La persecución del delito de suplantación de identidad mediante inteligencia artificial y la inoperancia de la Ley N.º 32314, Lima 2025”. Los resultados se le entregarán a usted de forma individual y se almacenarán respetando la confidencialidad de su anonimato.

Riesgos: Su participación en el estudio no presenta ningún riesgo ya que tendremos que acomodarnos al tiempo y horario del participante.

Beneficio: Usted se beneficiará del presente proyecto colaborado con brindar información relevante de ello nos servirá y permitirá conocer para aportar conocimiento que posteriormente será utilizado por las entidades especializadas en el tema relativo a casos de Delitos Informáticos en la modalidad del empleo del uso de la Inteligencia Artificial.

	FORMULACION DE CONSENTIMIENTO INFORMADO(FCI) EN UN ESTUDIO DE INVESTIGACION DEL CIEI-VRI	
	CÓDIGO: UPNW-EES-FOR-068	VERSION: 01 REVISION: 01

FECHA: 18-03-2026

Costos e incentivos: Usted no pagará ningún costo monetario por su participación en la presente investigación. Así mismo, no recibirá ningún incentivo económico ni medicamentos a cambio de su participación.

Confidencialidad: Nosotros guardaremos la información recolectada con códigos para resguardar su identidad. Si los resultados de estudio son publicados, no se mostrará ninguna información que permita su identificación. Los archivos no serán mostrados a ninguna persona ajena al equipo de estudio.

Derechos de los profesionales de los abogados penalistas: la participación en el presente estudio es voluntaria. Si usted lo decide puede negarse a participar en el estudio o retirarse de ese en cualquier momento, sin que esto ocasione ninguna penalización o pérdida de los beneficios y derechos que tiene como individuo, coma si tampoco modificaciones o restricciones al derecho penal sino un análisis.

Preguntas/contacto: puede comunicarse con el investigador Principal (Detallar el nombre, número de teléfono y correo electrónico del investigador principal).

Así mismo puede comunicarse con el Comité de Ética que validó el presente estudio.

Contacto del Comité de Ética: Dra. Yenny M. Bellido Fuentes, presidenta del Comité de Ética de la Universidad Norbert Wiener, para la investigación de la Universidad Norbert Wiener, Email: comite_etica@uwiener.edu.pe

II. DECLARACIÓN DEL CONSENTIMIENTO

He leído la hoja de información de Formulación de Consentimiento informado (FCI), y declaro haber recibido una explicación satisfactoria sobre los objetivos, procedimientos y finalidades del estudio.

Se han respondido todas mis dudas y preguntas. Comprendo que mi decisión de participar es voluntaria y conozco mi derecho a retirar mi consentimiento en cualquier momento, sin que esto me perjudique de ninguna manera. Recibiré una copia firmada de este consentimiento.



Participante: Edgar Alcides Mondaca Bejar
DNI: 43715666
Fecha: 18/03/2026



Investigador (a): Jesús María Díaz Aldaz
DNI: 72169470
Fecha: 18/03/2026

Nota: La firma del testigo o representante legal es obligatoria solo cuanto el participante tiene alguna discapacidad que impida firmar o imprimir su huella, o en el caso de no saber leer o escribir.

Anexo 5: Carta de aprobación de la institución para investigación

Anexo 6: Aprobación del comité de ética

Anexo 7: Informe de turnitin

15% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

- 9%  Fuentes de Internet
- 4%  Publicaciones
- 12%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

- 9% Fuentes de Internet
- 4% Publicaciones
- 12% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Internet		
hdl.handle.net			<1%
2	Trabajos entregados		
Universidad Wiener on 2025-07-02			<1%
3	Internet		
www.coursehero.com			<1%
4	Trabajos entregados		
Universidad Wiener on 2025-05-31			<1%
5	Trabajos entregados		
Universidad Cesar Vallejo on 2023-03-02			<1%
6	Trabajos entregados		
Universidad Tecnologica del Peru on 2025-12-22			<1%
7	Trabajos entregados		
Universidad Cesar Vallejo on 2025-12-01			<1%
8	Trabajos entregados		
Universidad Tecnologica del Peru on 2025-12-09			<1%
9	Trabajos entregados		
Universidad Privada Antenor Orrego 2025 on 2025-09-29			<1%
10	Trabajos entregados		
Universidad Wiener on 2025-06-22			<1%
11	Internet		
repositorio.udh.edu.pe			<1%