Revista Sapientia & Iustitia
FDCP • Universidad Católica Sedes Sapientiae
e-ISSN 2709-1228 Año 6 N. 12

ABORDAJE, DESAFÍOS Y EVOLUCIÓN DE LA LEGISLACIÓN SOBRE SUPLANTACIÓN DE IDENTIDAD DIGITAL EN PERÚ

Guisella Ivonne Azcona Avalos[*]
Universidad Católica Sedes Sapientiae
gazcona@ucss.edu.pe
https://orcid.org/0000-0002-5476-6699

Angie Antonella Alama Barreto[**]
Universidad Católica Sedes Sapientiae
2022100226@ucss.pe
https://orcid.org/0009-0007-7205-0727

Pamela Ariana Gonzales Sanchez[***]
Universidad Católica Sedes Sapientiae
2022100094@ucss.pe
https://orcid.org/0009-0001-4833-841X

Abigail Ore Talancha[****]
Universidad Católica Sedes Sapientiae
2021201044@ucss.pe
https://orcid.org/0009-0001-4435-3014

Anna Camila Medrano Martinez[*****]
Universidad Católica Sedes Sapientiae
2020200527@ucss.pe
https://orcid.org/0009-0006-4299-7250

[*] Doctora en Educación. Docente de Metodología de la Investigación y de Investigación Jurídica 1 y 2 de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

[**] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

[***] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

[****] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

[*****] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Gustavo Rogelio Noroña Rodriguez[******]
Universidad Católica Sedes Sapientiae
2022100480@ucss.pe
https://orcid.org/0009-0001-3912-6474

Luis Gerardo Alarcon Lopez[******]
Universidad Católica Sedes Sapientiae
2022102029@ucss.pe

Resumen: Este estudio analiza el abordaje, la evolución y los retos de la legislación peruana sobre la suplantación de identidad digital, enfocándose en la urgente necesidad de actualización legislativa frente a los avances tecnológicos y las nuevas modalidades de ciberdelitos. A través de un enfoque cualitativo y análisis documental, se examina la legislación vigente, destacando la Ley 30096 y su modificación, así como la adhesión de Perú al Convenio de Budapest. Se identifican brechas legislativas, desafíos prácticos en la aplicación de la normativa y se compara con tendencias internacionales para proponer mejoras legislativas. El estudio subraya la importancia de la cooperación internacional y la innovación legal para proteger los derechos digitales y personales en un contexto globalizado y digitalmente avanzado.
Palabras clave: suplantación de identidad digital, legislación peruana, ciberdelitos, Ley 30096, Convenio de Budapest.

APPROACH, CHALLENGES, AND EVOLUTION OF LEGISLATION ON DIGITAL IDENTITY IMPERSONATION IN PERU

Abstract: This study analyzes the approach, evolution, and challenges of Peruvian legislation on digital identity impersonation, emphasizing the urgent need for legal updates in response to technological advances and emerging forms of cybercrime. Using a qualitative approach and documentary análisis, it examines current regulations, highlighting Law No. 30096 and its amendment, as well as Peru's accession to the Budapest Convention. Legislative gaps, practical challenges in the enforcements. The study underscores the importance of international cooperation and legal innovation to safeguard digital and personal rights in a globalized and technologically advance context.

[******] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

[*******] Estudiante del quinto ciclo de estudios de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Sedes Sapientiae.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Keywords: Digital Identity Theft, Peruvian Legislation, Cybercrime, Law 30096, Budapest Convention.

1. Introducción

El presente estudio aborda una problemática contemporánea y de creciente preocupación en el ámbito jurídico y tecnológico: la suplantación de identidad digital en Perú, un fenómeno que ha encontrado en el avance tecnológico un vehículo propicio para su proliferación. Este ciberdelito, caracterizado por la usurpación o suplantación de la identidad de una persona en el ámbito digital, compromete seriamente el prestigio, honor y, en numerosas ocasiones, el patrimonio económico de las víctimas. La gravedad y complejidad de este delito plantean interrogantes fundamentales sobre la preparación y capacidad del marco jurídico y legislativo actual para abordar y regular adecuadamente estas conductas delictivas, con el objetivo de salvaguardar el derecho a la identidad y al honor de los individuos.

La revisión de la literatura y estudios previos revela un panorama variado y multifacético en cuanto a la legislación y el abordaje de la suplantación de identidad digital a nivel internacional. Investigaciones como las de Solís (2018) y Hernández (2019) ofrecen un análisis comparativo de las respuestas legislativas ante los ciberdelitos en diferentes jurisdicciones, subrayando la importancia de una comprensión integral y actualizada de este fenómeno a escala global. De igual forma, el estudio de Mejía et al. (2023) destaca la relevancia del Convenio de Budapest como marco de referencia internacional para la armonización legislativa en materia de ciberdelincuencia, proporcionando un valioso contexto para la discusión y análisis de las políticas y estrategias de prevención y sanción de la suplantación de identidad digital.

En el contexto peruano, la legislación vigente presenta diversas limitaciones. Primeramente, se observa la subjetividad de la ley peruana respecto a la definición de suplantación de identidad dentro de su normativa, ya que esta no se encuentra redactada en la medida que evite vacíos e interpretaciones negativas, lo que lleva a un aumento de la acción delictiva. En segundo lugar, como otra limitación recurrente en la ley, está la falta de investigación jurídica del delito de la suplantación de identidad, investigación que vaya acorde a los nuevos alcances que la tecnología tiene en él, provocando así un estancamiento del derecho en este caso. La Ley 30096, promulgada en 2013, y su posterior modificación mediante la Ley 30171 en 2014, constituyen los principales instrumentos legislativos en la materia, aunque su alcance y profundidad resultan insuficientes ante la evolución y complejidad de los ciberdelitos, debido al avance y diversificación de la tecnología en esta época. Dicha tecnología se caracteriza por presentar numerosas actualizaciones

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

sin restricciones para la sociedad, permitiendo con ello la mala manipulación de los medios digitales; lo que significa la existencia de nuevos precedentes, y en respuesta a ello la falta de bases actualizadas para su resolución. La adhesión de Perú al Convenio de Budapest sobre la ciberdelincuencia representa un paso adelante en el compromiso del país con la cooperación internacional y el fortalecimiento del marco jurídico contra la ciberdelincuencia. Sin embargo, persisten desafíos significativos en la implementación efectiva y la adaptación de las disposiciones del Convenio a la realidad nacional. Entre estos retos figura la aplicación del modelo al contexto social y legal del Perú, ya que, al introducirnos en un acuerdo internacional, se necesita conocer y estudiar el avance y trascendencia de ese delito en la sociedad peruana, debido a que en cada país es diferente. En esa línea, se tiene que buscar la manera de desarrollarla en la justicia peruana e idear la capacitación de los organismos públicos encargados de ello. Respecto a esto, se plantea el siguiente desafío: la concientización sobre los nuevos alcances de ese tipo de delito, enfocado en impartir el conocimiento de ello en las autoridades respectivas, y que se garantice su continuidad y evolución a lo largo de los años.

La falta de protección de datos personales, la insuficiente concienciación sobre los riesgos asociados a la suplantación de identidad y la escasez de recursos especializados en la investigación y persecución de este tipo de delitos son factores que agravan la situación. Estos factores, unidos a la limitada capacidad de respuesta del sistema jurídico y de seguridad, facilitan la impunidad de los ciberdelincuentes y perpetúan la vulnerabilidad de los ciudadanos ante estos ataques.

Frente a tal escenario, se plantea la necesidad de adoptar un enfoque multidimensional y coordinado, en el cual se trate la dimensión de análisis y seguimiento, la dimensión estratégica, y por último una dimensión empírica que involucra la practicidad del objetivo planteado. Dentro de ello, se maneja la actualización legislativa, la especialización y formación de los operadores de justicia, y la promoción de campañas de concientización dirigidas a la población. Solo mediante una estrategia integral que contemple la prevención, detección, persecución y sanción de la suplantación de identidad digital, será posible contrarrestar eficazmente este ciberdelito y proteger los derechos fundamentales de los individuos en el entorno digital.

Esta investigación se propone contribuir al debate y la reflexión sobre el abordaje y la evolución de la legislación sobre suplantación de identidad digital en Perú, con el fin de identificar vías de mejora y fortalecimiento del marco jurídico y las políticas públicas en este ámbito. A través del análisis de antecedentes nacionales e internacionales, así como de la normativa jurídica vigente, se busca aportar elementos de juicio y propuestas concretas

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

que permitan avanzar hacia una respuesta más efectiva y ajustada a las necesidades de la sociedad peruana frente a la creciente amenaza de la ciberdelincuencia.

1.1. Problema general

¿Cómo se ha abordado y evolucionado la regulación jurídica de la suplantación de identidad a través de medios digitales en Perú y qué desafíos y oportunidades presenta esta legislación en el contexto de los avances tecnológicos y cambios sociales actuales?

1.2. Problemas específicos

- ¿Cuáles son las características y limitaciones de la legislación peruana actual en el contexto de los ciberdelitos, con especial énfasis en la suplantación de identidad?
- ¿Cuáles son los desafíos prácticos y teóricos en la aplicación de la legislación existente sobre suplantación de identidad en medios digitales?
- ¿Cómo se comparan las tendencias internacionales con la situación en Perú para entender el posicionamiento del país en el contexto global?

1.3. Objetivo general

Analizar el abordaje, la evolución y los desafíos de la normativa jurídica peruana en relación con la suplantación de identidad digital, determinando oportunidades para fortalecer la legislación y mejorar la protección de los derechos de los individuos en el entorno digital.

1.4. Objetivos específicos

- Examinar las características y limitaciones de la legislación peruana actual en el contexto de los ciberdelitos, con especial énfasis en la suplantación de identidad digital.
- Analizar los desafíos prácticos y teóricos en la aplicación de la legislación existente sobre suplantación de identidad digital en medios digitales.
- Comparar las tendencias internacionales con la situación en Perú para entender el posicionamiento del país en el contexto global.

2. Metodología

Este estudio adopta un enfoque cualitativo (Hernández-Sampieri & Mendoza, 2018), centrándose en el análisis documental para examinar y criticar la regulación

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

jurídica de la suplantación de identidad a través de medios digitales en Perú. El análisis se enfoca en una revisión exhaustiva de documentos legales y literatura académica relevante. Este método permite una comprensión profunda y crítica de las implicaciones legales y sociales del fenómeno, así como de las respuestas legislativas a los desafíos presentados por la suplantación de identidad en la era digital.

La recopilación de datos incluye la búsqueda y revisión de fuentes primarias y secundarias. Las fuentes primarias abordan legislación y decretos, mientras que las secundarias incluyen estudios académicos, análisis de políticas y artículos de expertos en el campo. Esta aproximación garantiza una visión integral y actualizada de la situación en Perú, permitiendo la identificación de tendencias, vacíos y potenciales áreas de mejora en la legislación existente.

La técnica de análisis documental se emplea para sintetizar y evaluar críticamente la información recabada, identificando patrones, temas y discrepancias en el corpus documental. Este enfoque permite no solo comprender la situación actual, sino también proponer recomendaciones informadas y basadas en evidencia para el fortalecimiento del marco legal peruano en lo que respecta a la suplantación de identidad digital.

3. Marco teórico normativo

Para abordar de manera efectiva la suplantación de identidad digital, este marco teórico normativo inicia con una conceptualización detallada del fenómeno, incluyendo su evolución y los retos legales que presenta. Se examina el Convenio de Budapest y su influencia en Perú, contrastando con legislaciones de otros países para subrayar deficiencias y necesidades de reforma. Posteriormente, se analiza la legislación peruana sobre ciberdelincuencia, destacando la Ley 30096 y sus limitaciones. Se enfatiza la importancia de la cooperación internacional y la adaptación legislativa frente a avances tecnológicos, proponiendo actualizaciones para proteger contra la suplantación de identidad en el ámbito digital.

3.1. Conceptualización de la suplantación de identidad

3.1.1. *Definición y naturaleza de la suplantación de identidad en el entorno digital*

La suplantación de identidad digital es un delito informático enfocado en obtener información privada mediante engaños para conseguir algún beneficio a costa de dañar a una persona. Según Belisario (2014), el *phishing* es un ataque de ingeniería social que utilizan los delincuentes para la obtención de datos, para luego suplantar a la persona.

Por consiguiente, se está dando una amenaza creciente con la evolución tecnológica, enfatizando su objetivo de causar daños patrimoniales y extrapatrimoniales (Leguizamón, 2015). Los ciberdelincuentes, aprovechando las herramientas de inteligencia artificial, buscan vulnerar la seguridad personal y financiera de los usuarios, lo que subraya la importancia de estar informados sobre las características, etapas y modalidades de este ciberdelito para prevenirlo eficazmente.

3.1.2. *Evolución histórica de las técnicas para la suplantación de identidad en el contexto de los avances tecnológicos*

Las técnicas para la suplantación de identidad digital han evolucionado a través de varios periodos clave. En la década de 1990, los ciberdelincuentes comenzaron a utilizar correos electrónicos fraudulentos para obtener información personal. A mediados de la década de 2000, surgieron técnicas más avanzadas, como la creación de sitios web falsificados y el uso de malware para capturar datos. Desde 2010, la inteligencia artificial ha permitido a los delincuentes desarrollar ataques más sofisticados y personalizados, elevando el perfeccionamiento y eficacia de las técnicas de suplantación de identidad (García, 2017).

Otro factor relevante es la automatización, definida como la aplicación tecnológica que asigna a las máquinas tareas anteriormente realizadas por humanos, reduciendo así la carga de trabajo. Este avance ha llevado a una ciberdependencia significativa en la sociedad moderna, que considera indispensable la tecnología para una vida cotidiana satisfactoria (Martínez, 2020).

Por tanto, la introducción de nuevas tecnologías, como la Inteligencia Artificial (IA), representa un cambio significativo para la sociedad peruana y su marco legal. Actualmente, la legislación no ha sido modificada para incluir la IA entre los métodos de suplantación de identidad, abriendo así nuevos retos y posibilidades que aún no se han explorado completamente. Este avance tecnológico plantea incertidumbres sobre sus futuras implicaciones legales y el potencial uso malintencionado por parte de ciberdelincuentes que se adaptan rápidamente a las nuevas tendencias digitales.

3.2. Marco Jurídico Internacional

3.2.1. *Convenio de Budapest sobre Ciberdelincuencia: implicaciones e incorporación por parte de Perú*

El Convenio de Budapest sobre la ciberdelincuencia, promovido por el Consejo de Europa desde 2001, es un acuerdo internacional creado para abordar el aumento de

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

los delitos informáticos impulsados por la digitalización y globalización. Este tratado fomenta la cooperación global para combatir delitos como la interceptación de datos, el fraude y la suplantación de identidad, estableciendo leyes y técnicas de investigación para proteger los derechos fundamentales y facilitar una acción penal efectiva contra la ciberdelincuencia (Martins, 2020). Perú se adhirió a este convenio en marzo de 2019 mediante el Decreto Supremo 010-2019-RE, publicado en el Diario Oficial *El Peruano* el 22 de septiembre de ese año, complementando su legislación nacional sobre delitos informáticos, vigente desde 2013 con la Ley 30096 y su posterior modificatoria en 2014 con la Ley 30071, la cual tuvo una última reforma en sus artículos 5 y 9 con el Decreto Legislativo 1591 en diciembre de 2023.

3.2.1. *Comparación con legislaciones de otros países y su tratamiento de la suplantación de identidad*

En su análisis comparativo sobre legislaciones de delitos informáticos, Mejía et al. (2023) examinaron las normas de Perú, Chile, Colombia, España y Alemania. Destacaron que las leyes colombianas, particularmente las 1273 y 2009, presentan deficiencias en proteger los derechos fundamentales frente a los ciberdelitos. Este estudio subraya la importancia de adaptar y fortalecer las legislaciones nacionales en consonancia con estándares internacionales como el Convenio de Budapest para una protección efectiva contra la ciberdelincuencia.

Por su parte, Montaperto (2018), en su tesis titulada *Suplantación de identidad. Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino*, examina la ley modificada 26.388 de delitos informáticos de Argentina, destacando su omisión de la suplantación de identidad como delito específico. Argumenta que esta omisión podría contravenir el principio de legalidad, esencial para el debido proceso, dado que la ley penal no admite interpretación por analogía. Además, realiza un análisis comparativo de la legislación sobre suplantación de identidad entre Argentina y otros países como Brasil, Paraguay, Colombia, Perú y España, evidenciando el desarrollo legislativo y las diferencias en la tipificación del delito en estas jurisdicciones.

3.3. Legislación peruana sobre ciberdelincuencia

3.3.1. *Análisis de la Ley 30096, Ley de Delitos Informáticos: alcance y limitaciones*

La Ley 30096 (2013) de Delitos Informáticos en Perú regula la suplantación de identidad y otros ciberdelitos. En su artículo 9, se especifica la ilegalidad de suplantar identidades a través de medios tecnológicos, imponiendo penas de 3 a 5 años. Esta

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

legislación hasta el momento no ha tomado más énfasis en la evolución de la suplantación de identidad con el uso de la inteligencia artificial, por lo tanto, se ve una desprotección a la seguridad digital de los peruanos.

Asimismo, la Ley 30171 modificó la Ley 30096, introduciendo actualizaciones en los artículos 2, 3, 4, 7, 8 y 10, ampliando los supuestos y formas de comisión de delitos informáticos. Esta reforma incluyó la penalización de una gama más amplia de ciberdelitos como el acceso ilícito, interceptación ilegal, alteración, robo, difusión de datos falsificados, fraude, extorsión, daños informáticos y sabotaje, estableciendo penas de prisión que varían desde un año hasta más de dieciocho años, según la gravedad del delito cometido (Congreso de la República del Perú, 2014).

Por su parte, el Decreto Legislativo 1591 modifica la anterior ley en los artículos 5, el cual sanciona a los sujetos que realizan proposiciones con fines sexuales a los menores de edad a través de los medios tecnológicos, y el artículo 9, sobre suplantación de identidad, el cual agregó un segundo párrafo incluyendo una pena privativa de libertad no menor de 6 ni mayor a 9 años contra quienes suplanten la identidad de los menores de 18 años que causen perjuicios de cualquier índole (Congreso de la República del Perú, 2023).

Por tanto, la Ley de Delitos Informáticos de Perú proporciona al marco jurídico herramientas esenciales para enfrentar los desafíos digitales, aumentando la seguridad y estableciendo penalidades específicas. Sin embargo, las modificaciones posteriores han generado incertidumbre sobre la protección de los derechos ciudadanos, debido a su generalidad y la necesidad de especificaciones más detalladas, especialmente en lo que respecta a la suplantación de identidad. Por ello, es necesaria una revisión del artículo 9 para mejorar la legislación y su aplicabilidad en casos de suplantación de identidad, que incluya protección a los ciudadanos contra quienes usen de manera maliciosa las tecnologías digitales para perjudicar a otros.

3.4. Desafíos y limitaciones de la legislación actual

3.4.1. *Brechas en la legislación actual y su efectividad en la lucha contra la suplantación de identidad digital*

La legislación actual enfrenta desafíos significativos en la lucha contra la suplantación de identidad digital. Existe una necesidad urgente de fortalecer el marco legal para mejorar la detección, interpretación y tipificación de estos delitos, que han aumentado con el avance tecnológico. Las brechas en la normativa no solo dificultan la efectividad en el combate a la ciberdelincuencia sino que exigen la actualización y

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

adaptación de las leyes a las realidades digitales contemporáneas, garantizando así una protección efectiva de la identidad en el ámbito digital.

La legislación vigente sobre delitos informáticos, incluyendo la suplantación de identidad digital, enfrenta críticas por su insuficiencia y falta de precisión. Zorrilla (2018) argumenta que las leyes actuales no están adecuadamente equipadas para manejar todos los procedimientos relacionados con delitos informáticos, ya que no incluyen protección contra los avances tecnológicos que se están dando a gran escala en los medios digitales, tal como la IA, que ahora es usada por lo delincuentes para poder suplantar la identidad y de esta forma cometer actos delictivos con el fin de obtener beneficios económicos. Esta deficiencia legislativa conlleva a un ámbito de acción legal imprecisa y posibles sobrepenalizaciones.

La carencia evidente en la legislación, especialmente en el artículo 9 de la Ley 30096, limita significativamente su eficacia en el manejo de casos de suplantación de identidad digital, dejando a la sociedad insatisfecha con su capacidad regulatoria. Esta situación se agrava por la ausencia de un organismo especializado que realice las investigaciones necesarias, aprovechando tanto referencias nacionales como internacionales para formular una respuesta efectiva contra este tipo de ciberdelito.

3.5. Impacto social y económico de la suplantación de identidad

3.5.1. *Consecuencias sociales de la suplantación de identidad: afectación a individuos y entidades*

Las consecuencias sociales de la suplantación de identidad impactan tanto a individuos como a entidades, evidenciando una interdependencia significativa. Esta situación se agrava con el auge de la comunicación electrónica, que facilita la interacción global pero también expone a riesgos de privacidad y seguridad (Martínez, 2020). La suplantación, definida como la usurpación no autorizada de la identidad de otra persona a través de medios digitales, compromete seriamente los derechos fundamentales, subrayando la necesidad de un control más estricto en el uso de las tecnologías.

La proliferación de la comunicación electrónica sin el adecuado control ha situado a la suplantación de identidad como una consecuencia directa de esta expansión, afectando a individuos y entidades. Numerosos casos evidencian la vulneración de derechos fundamentales debido a la gestión inadecuada de tecnologías como redes sociales, páginas web y aplicaciones. Esta situación resalta la crítica necesidad de implementar medidas preventivas y promover un uso consciente de estos medios para comunicarnos globalmente.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

3.5.1. *3.5.2. Impacto económico y retos para las empresas en la era digital*

La era digital presenta desafíos económicos significativos para las empresas, especialmente en contextos donde el acceso a internet es limitado, como se destaca en estudios del Instituto Nacional de Estadística y Censos (INEC, 2017) en Ecuador. Esta situación resalta la brecha digital existente y cómo afecta a las empresas en su capacidad para alcanzar a toda la población. Además, la digitalización ha incrementado la vulnerabilidad de los grupos más susceptibles, especialmente los niños, a delitos en línea, incluida la pornografía infantil y la piratería, que atentan contra los derechos de autor y la privacidad.

Las empresas enfrentan retos adicionales en proteger la información confidencial y operaciones bancarias de ataques cibernéticos. La suplantación de identidad, facilitada por la amplia disponibilidad de herramientas digitales, representa un riesgo significativo tanto para individuos como para entidades corporativas, evidenciando la necesidad de robustecer las medidas de seguridad en línea.

En consecuencia, la evolución tecnológica exige una actualización constante de las estrategias de protección de datos personales y empresariales. La sociedad debe equiparse con herramientas adecuadas para salvaguardar su información en el ciberespacio, adaptándose a los cambios y desafíos que presenta la era digital y, de ese modo, proteger tanto a individuos como a empresas de las amenazas cibernéticas emergentes.

3.6. Tendencias y futuro de la legislación en el contexto digital

3.6.1. *Avances tecnológicos y su impacto en la legislación futura*

Los avances tecnológicos, como la inteligencia artificial y la biotecnología, requieren de una legislación que se adapte a nuevos desafíos y oportunidades, transformando sectores como la salud y la seguridad. Según Hernández (2019), es fundamental desarrollar leyes flexibles, proactivas, y colaborar internacionalmente para asegurar que la tecnología beneficie a la humanidad. La participación de actores sociales variados en la creación de leyes es clave para enfrentar la incertidumbre tecnológica y garantizar la protección de los derechos individuales en un futuro digital.

La rápida evolución de la tecnología informática ha introducido nuevos desafíos legales debido a la aparición de los delitos informáticos, los cuales pueden ser cometidos mediante el uso de la tecnología o tener como objetivo la tecnología misma. Zorrilla (2018) destaca que estas circunstancias demandan una revisión constante del Derecho

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

para asegurar la protección de los derechos individuales y mantener la justicia en un contexto cada vez más dominado por la tecnología.

3.6.2. *Propuestas para la mejora de la legislación y adaptación a los nuevos desafíos digitales*

El estudio de Quispe y Quispe (2023) revela la insuficiencia de la Ley 30096 para afrontar la suplantación de identidad en transacciones comerciales digitales. Mediante entrevistas a 10 abogados y análisis legislativo y literario, identifica la necesidad de regulaciones específicas para el comercio electrónico, así como para contrarrestar el *phishing* y el *vishing*. Sugiere actualizaciones legislativas que incluyan la definición precisa de suplantación de identidad digital, mecanismos de prevención y detección de fraudes, y fomento de la educación digital. Destaca la importancia de considerar los datos digitales y contraseñas como bienes jurídicos protegidos, proponiendo sanciones penales para violaciones de privacidad.

3.7. Conclusión del marco teórico normativo

La regulación jurídica de la suplantación de identidad digital en Perú se halla en un punto crítico, demandando actualizaciones legislativas urgentes para abordar las complejidades emergentes en un mundo interconectado. La investigación destaca la imperiosa necesidad de una legislación integral que contemple la protección de la información personal y promueva la cooperación internacional, facilitando de ese modo combatir el uso de la inteligencia artificial en los delitos de suplantación de identidad. Este marco normativo debe ser dinámico, capaz de adaptarse a las rápidas transformaciones tecnológicas y a las nuevas modalidades de delitos informáticos, incluida la suplantación de identidad, que desafían la efectividad de las leyes actuales. El mal uso que le dan los seres humanos a la inteligencia artificial subraya la urgencia de reformas legales que protejan adecuadamente los derechos individuales en el espacio digital, asegurando una cultura de seguridad y prevención. La colaboración internacional emerge como un pilar esencial para fortalecer las capacidades nacionales en la lucha contra la ciberdelincuencia, garantizando la protección de los derechos fundamentales en el entorno digital. Este análisis subraya la importancia de ajustes legislativos proactivos y conscientes de la evolución digital, para proteger a la sociedad de los riesgos inherentes a la suplantación de identidad y otros ciberdelitos.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

4. Resultados

A continuación, se describe cómo se logró obtener los resultados a través del análisis documental de los textos. Para ello, se empleó una metodología detallada que comenzó con la selección y revisión de 23 fuentes de información, incluyendo leyes, libros, artículos científicos y tesis. Este proceso se estructuró en dos fases clave: inicialmente, se utilizó un sistema de fichaje para registrar detalles esenciales de cada fuente, como el Título, Autor, Año, Descriptores o palabras claves, Tipo de fuente y URL. Esta primera matriz facilitó un análisis crítico individualizado de cada documento. Posteriormente, se aplicó una Matriz de triangulación de la información, donde se realizó la interpretación de los datos recogidos en función de los objetivos específicos de la investigación. Esta etapa permitió relacionar las fuentes con las categorías, subcategorías e indicadores pertinentes, asegurando que el análisis estuviera alineado con las preguntas de investigación planteadas. Este enfoque metódico garantizó una comprensión profunda de la temática y contribuyó significativamente a los hallazgos de la investigación.

4.1. Análisis e interpretación de los hallazgos

El análisis de los resultados de la investigación se presenta en relación a la triangulación de las fuentes de información analizadas, la cual sirvió para la construcción de la matriz de triangulación, cuyos resultados generales interpretados se exponen en este subapartado.

De acuerdo con el objetivo específico 1, Examinar las características y limitaciones de la legislación peruana actual en el contexto de los ciberdelitos, con especial énfasis en la suplantación de identidad digital, se interpretó lo siguiente:

- En base a la categoría evolución legislativa, subcategoría cambios en la legislación e indicador modificaciones legales, se argumenta que actualmente la legislación peruana encamina un importante avance hacia la actualización del marco legal en el país. Se plantea la existencia de cuestiones sobre la suficiencia y la capacidad de adaptación de la ley frente a la progresiva evolución de las tecnologías digitales. La revisión y adaptación legislativa se realiza constantemente para garantizar la protección integral de los derechos digitales de los ciudadanos, destacándose los avances logrados y las áreas que necesitan mayor interés y observación. Los delitos informáticos y la evaluación constante de su adecuación a los desafíos digitales emergentes son aspectos clave para asegurar una respuesta efectiva y actualizada ante la ciberdelincuencia. El Congreso de la república del Perú (2014), en su

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Ley 30096 y modificatoria Ley 30171, que ha sido reforzada y actualizada, con la más reciente modificatoria del Decreto Legislativo 1591, incorpora nuevos cambios y evidencia su adhesión al tratado internacional sobre la ciberdelincuencia (como el Convenio de Budapest) en los artículos que establecen bases fundamentales para la acción legal, específicamente, contra la suplantación de identidad.

- En base a la categoría evolución legislativa, subcategoría tratados internacionales e indicador ratificación de tratados, se argumenta el compromiso por parte de Perú sobre la ciberdelincuencia en la ratificación del convenio, asumiendo los estándares internacionales para combatir este tipo de delitos y alineando sus políticas nacionales con las prácticas globales. El objetivo es buscar la acción, facilitando la cooperación entre países extranjeros en la persecución de crímenes digitales, relacionada a la suplantación de identidad. Se reconoce el impacto de la implementación efectiva de las disposiciones del convenio a nivel nacional siendo decisivo más allá de la ratificación inicial. Se destacan los ajustes a la legislación y los mecanismos de aplicación para cumplir con las obligaciones y aprovechar las oportunidades que el convenio internacional ofrece y que garantiza una protección adecuada y eficaz contra la ciberdelincuencia. La ratificación de acuerdos internacionales establece una guía en acciones concretas dentro de su propio marco legal y de aplicación para la legislación interna.
- En base a la categoría desafíos jurídicos, subcategoría brechas y limitaciones e indicador lagunas legales en la legislación actual, se argumenta en base a lo dicho por Zorrilla (2018) en relación a que en la realidad jurídica peruana existen varias lagunas y vacíos legales que se encuentran en la legislación actual, y dentro de este cuadro también se encuentran ambigüedades e inconsistencias como lo hubo dentro de la Ley 30096 y la actual Ley 30171 que entró en vigencia en el año 2014, más específicamente el artículo 36 dentro de los numerales 1, 2 y 4 que limitan la aplicación correcta de las leyes relacionadas con delitos informáticos. Por ello, dificulta su aplicación efectiva para garantizar la protección de la información de los ciudadanos en la era digital. Lo que en realidad quiere lograr ese escrito es resaltar la importancia de la claridad y precisión de las leyes. En correlación con lo expresado, Montaperto (2018) en su investigación también se aprecian brechas y limitaciones debido a la falta de un marco jurídico regulatorio para los delitos informáticos contra la suplantación de identidad en el derecho penal argentino. Al aplicarse este marco, se evidencia una inmensa laguna

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

legal que puede afectar uno de los principios fundamentales del derecho penal: la legalidad. Incluso se observa una ausencia de regulación jurídica clara.

- A ello se suma la necesidad de analizar la suplantación de identidad desde un punto de vista teórico, considerando su configuración como delito y la manera en que puede ser aceptada como conducta delictiva, para recién luego ser normativamente definida por la ley penal.
- En ese sentido, se realiza una observación sobre la legislación peruana vigente, en comparación con el derecho argentino, resaltando la necesidad de aplicar el derecho comparado como herramienta analítica para fortalecer las normativas nacionales.
- En base a la categoría desafíos jurídicos, subcategoría brechas y limitaciones e indicador identificación de vacíos legales, se argumenta que Quispe y Quispe (2023), con el fin de poder identificar dicho vacío legal, estuvieron envueltos en una investigación cualitativa con la intención de centrar dicho estudio en las acciones de la persona humana y de la vida social teniendo dentro de su objetivo principal el artículo 9 de la Ley 30096 en relación al delito de suplantación de identidad de la ley de delitos informáticos. Es decir, donde se describe las transacciones y compras por medio de la vía digital dentro del internet por medio de tecnologías de la comunicación e información. Dicha norma no especifica en ninguna de sus líneas la transferencia financiera que cometen los delincuentes cibernéticos para sustraer toda la información personal de las víctimas para, posteriormente, cometer la suplantación de identidad además de otros delitos. Es aquello que produce vacíos legales, que de boca del mismo Marcial Rubio es aquel suceso sin una norma jurídica aplicable por lo cual no puede aplicarse ninguna norma en específico, por lo cual en medio de esto entra lo estipulado en nuestra Carta Magna en su artículo 2, inciso 24, literal A, el cual señala que nadie está obligado a hacer lo que la ley no manda ni prohibido de hacer lo que esta no prohíbe. Lo cual da una ventaja para aquellos delincuentes y de esta forma evadir la justicia. En vista de ello, se recomienda regularizar la ley 30096 por medio de una iniciativa legislativa, esta falta de regulación es la principal causa por la que existen varios casos de suplantación por los medios digitales como clonación de tarjetas, transferencias de dinero, transferencia de datos, etc.

Por ende, las fuentes de información analizadas manifiestan que la legislación actual no se encuentra actualizada con diversas y amplias especificaciones en la redacción de

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

su artículo, las cuales requieren ser descritas y estudiadas a detalle en lo que respecta a las nuevas modalidades de suplantación de identidad. No hacerlo podría dejar impune tal delito, ya que no se ha realizado hasta el momento una modificatoria, por lo tanto, los ciberdelincuentes se encuentran tranquilos al cometer ese crimen. Además, tenemos que estar a la vanguardia de los demás países aledaños para no atrasarnos en la protección de derechos de los ciudadanos. Si bien en la actualidad nos encontramos en el Convenio de Budapest que trata sobre los ciberdelitos, estos convenios se deben de ratificar, impulsando el implemento de las modalidades tecnológicas en el delito de suplantación de identidad, entre ellos, el más común se relaciona con la IA (Inteligencia Artificial) cuando es usada por lo suplantadores en las diversas redes sociales, páginas web, incluso incurriendo en cuentas bancarias, para robar financieramente.

De acuerdo al objetivo específico 2, Analizar los desafíos prácticos y teóricos en la aplicación de la legislación existente sobre suplantación de identidad digital en medios digitales, se interpretó lo siguiente:

- En base a la categoría Desafíos Jurídicos, subcategoría Aplicación y Eficacia e indicador Dificultades en la implementación de la ley, se argumenta que la eficacia de las legislaciones normativas actuales en favor a la protección de los derechos digitales es un tema de carácter bastante controversial. Núñez (2016) señala que existen muchas complejidades en la implementación de legislaciones oportunas que protejan la identidad digital de los individuos en un entorno virtual, lo que se manifiesta en las leyes existentes, las cuales no logran satisfacer la necesidad de seguridad y privacidad en línea. Debido a ello, enfatiza la importancia de actualizar y mejorar el marco normativo en temas relacionados a las tecnologías emergentes y los nuevos desafíos digitales. Asimismo, sugiere la urgencia de optar por un enfoque más integral que logre garantizar la protección de la identidad digital como un derecho más, así como también asegurar la privacidad de los usuarios en el amplio mundo del internet. La investigación aporta una perspectiva esencial para comprender las dificultades que existen en cuanto a la eficacia de la aplicación normativa de las leyes que buscan proteger la identidad digital; por ello, se proponen soluciones legislativas y políticas para reforzar la seguridad y la credibilidad en los procesos digitales.
- En base a la categoría Desafíos Jurídicos, subcategoría Aplicación y Eficacia e indicador Retos en la aplicación efectiva de la nor-

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

mativa, se argumenta que el desarrollo de los delitos cibernéticos en el entorno social está indudablemente relacionado con la figura normativa. Vega y Arévalo (2022) detallan cómo los avances de los ciberdelitos originaron obligatoriamente una evolución en el marco jurídico nacional e internacional. En el caso de Perú, se manifestó en la creación y promulgación de la Ley 30096, Ley de Delitos Informáticos, la que posteriormente fue modificada en la actual Ley 30171. Asimismo, se evidenció en su adhesión al tratado internacional sobre la ciberdelincuencia, llamado también Convenio de Budapest, en 2019. Las normas vigentes enfatizan el problema que resultan ser los delitos cibernéticos, al igual que el aumento de sus modalidades delictivas, lo que conlleva a la obligación de garantizar y condicionar acción legal por parte de las autoridades competentes. El libro de Vega y Arévalo expone que, a pesar del intento de mitigar los delitos en el medio digital, las leyes con las cuales se rige el Perú en esta área son bastante limitadas y su eficacia no resulta satisfactoria para los mismos usuarios vulnerados, por tanto, se insta que se gestione el problema de manera adecuada por parte de las autoridades y la promulgación normativa.

En consecuencia, las fuentes de información analizadas manifiestan que la eficacia de la legislación peruana frente a los ciberdelitos y la protección de la identidad digital enfrenta desafíos considerables. Se señala la necesidad urgente de actualizar y reforzar el marco normativo para abordar adecuadamente las tecnologías emergentes y los nuevos riesgos digitales. La legislación actual, incluyendo la Ley 30096 y su modificatoria, así como la adhesión al Convenio de Budapest, aún no satisface completamente las demandas de seguridad y privacidad *online*, lo que subraya la importancia de adoptar un enfoque más integral en la protección legal de la identidad digital.

De acuerdo con el objetivo específico 3, Comparar las tendencias internacionales con la situación en Perú para entender el posicionamiento del país en el contexto global, se interpretó lo siguiente:

- En base a la categoría impacto social, subcategoría impacto en las víctimas e indicador consecuencias emocionales y psicológicas, se argumenta, recurriendo a la investigación de Aguilar (2019), que la suplantación de identidad conlleva otros delitos que van contra la dignidad del ser humano.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Entre ellos se puede mencionar la trata de personas, donde muchas de las víctimas son raptadas, contactándolas a través de redes sociales, suplantan su identidad, y luego las secuestran para así explotarlas sexualmente y laboralmente, incurriendo en violencia física y psicológica. La mayoría de las víctimas son niños, los cuales son separados de sus familias, adquiriendo con ello traumas desgarradores. La suplantación de identidad tiene un vínculo muy fuerte con la pornografía. En este caso, los pervertidos delincuentes no tienen límites con tal de hacer daño a las personas; su método radica en utilizar perfiles falsos con las fotos de sus víctimas y pasar a colgarlas en páginas ilegales. A través de esto, chantajean a los menores de edad con información valiosa y así obtener fotos subidas de tono, lo que ocasiona a las víctimas sentimientos de angustia y temor, por lo que intentan buscar ayuda de sus amistades o de personas que no conocen del tema; poniéndolos en ocasiones bajo un mayor riesgo. Aquellos ciberdelincuentes captan a las personas que son más vulnerables, utilizando distintos tipos de amenazas, entre ellas, varias que involucran el daño del círculo familiar de la víctima.

- En base a la categoría impacto social, subcategoría impacto en las víctimas e indicador daños económicos, se argumenta que la investigación de Hernández (2019), situada en Ecuador, nos menciona las distintas modalidades de robos de suplantación de identidad. Una de las más comunes es el robo a mano armada, donde se llevan las tarjetas de crédito y débito, DNI, entre otros documentos de gran relevancia; lo cual provoca que los delincuentes utilicen lo robado para realizar todo tipo de compras, llegando incluso a pedir préstamos en distintas entidades bancarias. Asimismo, otra de las modalidades de los ciberdelincuentes es utilizar las redes sociales para robar datos personales, con el propósito de venderlo por páginas web del mercado negro, donde es comprado por personas sin escrúpulos, incurriendo posteriormente en otros delitos como la trata de personas y pornografía. Por otra parte, el artículo de Vinelli (2021) aborda la ineficacia de la legislatura actual en relación con el robo financiero, recalcando que la suplantación de identidad es un delito que se comete teniendo fines económicos, perjudicando de ese modo la situación financiera de la víctima. Por las razones antes mencionadas es que se debe modificar la ley, en vista de tener métodos preventivos más convenientes para evitar este tipo de actos delictivos. Adicionalmente, es preciso que se estudie las nuevas modalidades digitales, aquello establecerá un equilibrio entre el aspecto legislativo y las actualizaciones de los ciberdelitos.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

- En base a la categoría impacto social, subcategoría percepción pública e indicador nivel de conocimiento sobre la legislación, se argumenta, de acuerdo con el trabajo de Fernández (1997), la importante necesidad de conocer sobre la identidad personal dentro de nuestro marco jurídico, el cual permitirá que los ciudadanos tengan conocimiento sobre su derecho fundamental y de ese modo tener un criterio acerca de ello y de su relevancia. Según el estudio, es necesario comprender cómo los peruanos perciben lo que implica dañar la identidad de la persona, destacando la brecha entre el conocimiento minuciosamente legal y la conciencia pública sobre la protección de la identidad. Fernández comparte la idea del requerimiento de educación respecto de los derechos y protecciones legales, sobre todo para sensibilizar a los peruanos acerca del derecho a la identidad; puesto que en nuestra realidad muchas personas omiten e incluso muestran indiferencia sobre la identidad personal o simplemente no saben de la existencia de leyes que protejan dicha identidad. Por otro lado, una minoría lo considera solo como aquello que identifica al ser humano de manera única. Sin embargo, Fernández subraya la importancia de fortalecer la educación sobre la legislación peruana actual para prevenir daños a esta cualidad del ser humano y responder adecuadamente ante el atentado de su identidad personal.
- En base a la categoría impacto social, subcategoría percepción pública e indicador campañas de concienciación, se argumenta, con apoyo de la investigación de Pedrero (2021), que en un entorno tan conocido actualmente como lo es el internet, un lugar al que se puede acceder libremente, desde cualquier punto de ubicación, es un espacio en el cual se debe tener sumo cuidado, porque no se está consciente de que intenciones tengan ciertas personas dentro de la red. Estas pueden incurrir en delitos de robo de información personal y ello puede progresar hasta cometer otro tipo de acto delictivo como la suplantación de identidad y el robo de esta misma. De esta manera, es que se procura poner énfasis en la importancia de la identidad como factor necesario dentro de la sociedad y en las relaciones sociales. A partir de ello, se observa que varios usuarios al utilizar las redes, en la mayoría de los casos no toman precauciones a la hora de navegar y así terminan siendo víctimas de los delincuentes cibernéticos. Debido a ello, se subraya la importante necesidad de saber identificar con quién estamos en las redes sociales y sobre mantener nuestra identidad bajo nuestra protección. Sobre todo, se recomienda poseer una adecuada seguridad de los sistemas informáticos, además de tener en cuenta las diversas modalidades que los

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

delincuentes pueden realizar para violar la seguridad de la identidad de los usuarios. Por ende, se crean situaciones relativas con la intención de prevenir y concientizar a los ciudadanos sobre la suplantación de identidad al estar relacionada con los delitos de los bienes jurídicos y delitos contra el honor.

- En base a la categoría comparación internacional, subcategoría legislaciones extranjeras e indicador estudio comparativo, adaptación legal, tratados internacionales, se argumenta con el aporte de Solís (2018) la importancia de comprender la historia, las condiciones sociopolíticas y económicas, así como la tradición jurídica de cada país. Este enfoque permite la identificación de puntos de convergencia y la generación de soluciones creativas para abordar un problema complejo, internacional y de larga data. La identidad digital, como faceta crucial de la identidad humana, es altamente vulnerable a la delincuencia, lo que subraya la imperiosa necesidad de protegerla. El estudio se centra en las legislaciones de tres países: México, Estados Unidos y Francia, con el objetivo de entender cómo reconocen, regulan y garantizan el derecho humano a la identidad, especialmente la digital. Se busca identificar estrategias legales de protección y defensa que no dependan exclusivamente de procesos legislativos lentos e ineficaces. La identidad digital abarca múltiples aspectos más allá de lo evidente, constituyendo nuestra auténtica huella virtual; es esencial comprender que cada interacción en el entorno digital deja una marca que refleja nuestra personalidad, preferencias y temores, exponiendo nuestra intimidad de manera sin precedentes. Por ende, debemos ser extremadamente cautelosos con lo que compartimos en línea. El delito de usurpación de identidad no es un acto aislado, sino que puede ser un medio preparatorio para otros ilícitos, lo que dificulta su detección y persecución, por lo que es crucial abordar este delito como parte de un conjunto de actividades delictivas, considerando tanto sus orígenes como sus posibles consecuencias futuras.
- En base a la categoría cooperación internacional, subcategoría estrategias de prevención e indicador medidas preventivas, educación digital, cooperación internacional, se argumenta que el phishing, un tipo de ataque de ingeniería social que tiene más de dos décadas de existencia, sigue representando una amenaza significativa en el panorama digital. En esa línea, el análisis exhaustivo de Belisario (2014) no solo busca comprender las características y la evolución del phishing, sino también resaltar las responsabilidades tanto de las organizaciones como de los usuarios en la prevención de este delito. Las corporaciones, priorizando la operatividad sobre la seguridad, a menudo

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

dejan puertas abiertas a los ataques de phishing. Estas vulnerabilidades pueden surgir en cualquier nivel del sistema, desde fallas en el diseño del hardware hasta configuraciones básicas en la seguridad informática, y a menudo no se solucionan inmediatamente, lo que deja a las organizaciones expuestas por períodos prolongados. El acceso fácil a la información a través de redes sociales también ha facilitado a los phishers la obtención de datos para perpetrar ataques, como el whaling, spear phishing y VoIP. Además, los phishers pueden valerse de herramientas de almacenamiento de información y recursos de bajo costo para crear páginas web falsas, lo que complica aún más la detección de los ataques. El constante avance en la sofisticación de los ataques de phishing, dirigidos a víctimas específicas, hace que la suplantación de identidad sea cada vez más difícil de detectar (Leguizamón, 2015). Esto se agrava por la falta de atención de los usuarios debido al ritmo acelerado de la vida moderna, lo que convierte al phishing en una amenaza latente que persiste en el tiempo.

- En base a la categoría oportunidades de mejora, subcategoría innovación legal e indicador propuesta de reforma, se argumenta que existe una discrepancia significativa entre la legislación peruana actual sobre ciberdelitos, particularmente en lo que respecta a la suplantación de identidad, y las prácticas globales recomendadas, como se ejemplifica en las propuestas de reforma de Alberca (2017). Este estudio subraya la ineficacia del artículo 9 de la Ley 30096, apuntando a una urgente necesidad de actualización para abordar nuevas modalidades de delito. La falta de modificación de esta ley pone en riesgo la protección jurídica de los ciudadanos peruanos frente a los desafíos emergentes en el ámbito digital, contrastando con los países vecinos que han adaptado sus legislaciones para combatir efectivamente estos delitos. La investigación sugiere una colaboración interdisciplinaria para el fortalecimiento legal, destacando la importancia de una tipificación que proteja integralmente la identidad y la integridad personal y familiar, resaltando el desfase entre las normativas nacionales y las tendencias internacionales en la regulación de ciberdelitos.
- En base a la categoría oportunidades de mejora, subcategoría innovación legal e indicador actualización legal, se argumenta que la investigación de Zorrilla (2018) destaca la imperante necesidad de actualizar la legislación peruana sobre delitos informáticos, específicamente la Ley 30096 y su modificatoria, la Ley 30171, para abordar de manera efectiva las nuevas modalidades de ciberdelincuencia y ampliar la protección legal. Resalta la confusión entre

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

legisladores para adecuar las normas a la evolución tecnológica, evidenciando la importancia de adaptar las leyes para proteger adecuadamente a las víctimas de estos crímenes. La adhesión de Perú al Convenio de Budapest se señala como un paso adelante en la regulación de estos delitos, aunque se subraya la necesidad de que cualquier legislación en este ámbito respete plenamente las libertades y derechos constitucionales, garantizando leyes proporcionadas, efectivas y alineadas con principios fundamentales. Este análisis crítico subraya la urgencia de reformas legales que permitan una protección más robusta ante el constante avance de la tecnología y las formas emergentes de criminalidad digital.

- En base a la categoría oportunidades de mejora, subcategoría fortalecimiento institucional e indicador mejora en la aplicación de la ley, se argumenta que Martínez (2020) explica en el respectivo artículo la importancia de que exista una colaboración entre las entidades del Estado, aquello con el propósito de dar respuesta a los numerosos avances de ciberataques en la actualidad. Asimismo, expone los antecedentes que se han investigado previamente a la redacción del artículo, los cuales se caracterizan principalmente por la necesidad de un sistema de ciberseguridad y de fortalecimiento legislativo. En efecto, ciertas deficiencias se encuentran en numerosas normativas tanto nacionales como internacionales. Por ello, como parte del contenido del artículo, es primordial destacar su estimulación sobre una colaboración y cooperación entre reglamentos, que ayuden a evolucionar los conceptos de ciberdelincuencia y ciberseguridad, conceptos que poco a poco se han convertido en parte de la cotidianidad de la población. En respuesta a lo que se conoce como ciberdependencia, se piensa en la creación de leyes que estén a la par de los avances cibernéticos que se presentan, garantizando un balance estable entre ambos y, a su vez, evitar permanecer bajo un sistema primitivo que no se adapte a los requerimientos del presente. En consecuencia, se establece el papel que tiene el Estado en este tipo de necesidades jurisdiccionales, en la cual su intervención no solo resulta satisfactoria para la población en general, sino para los organismos estatales, los cuales también podrán verse resguardados por los cambios normativos sobre ciberseguridad, ya que hoy por hoy no solo se ven casos de ciberdelincuencia externamente, sino también de manera intrínseca, como los hackeos a los sistemas del Estado, etc. Por ese motivo, el apoyo, coordinación y organización para la creación de un medio que se aplique a los casos producidos en el ciberespacio, resulta vital y necesario a nivel nacional como internacional.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

- En base a la categoría oportunidades de mejora, subcategoría fortalecimiento institucional e indicador propuestas de capacitación, se argumenta que el libro de Vega y Arévalo (2022), expone el campo de los ciberdelitos, desde sus inicios y su desenvolvimiento en la sociedad, lo que se puede traducir como un aumento de la ciberdependencia, así como también de la evolución de los métodos que se pueden utilizar tanto para beneficio como para delinquir. De este modo es que nace la inquietud por la urgencia de una legislación sobre ciberdelitos más adecuada en Perú, por lo que se observa la presencia de análisis a la legislación nacional, donde la anterior Ley 30096, y su modificatoria con la Ley 30171, son importantes para seguir avanzando en la creación de una normativa legislativa que sea más factible en todos sus aspectos: interpretación, precisión y alcance. La investigación que se percibe en el libro resulta predominante en lo que se entiende por relación internacional, la mención de organismos internacionales como la ONU, la OEA, así como también la existencia del Convenio de Budapest, realzan lo trascendental que tiene la actuación de estos como factor referente en la mejora de la legislación peruana. Por ende, el compendio permite la comprensión de los delitos cibernéticos, desde una visión jurídica del tema, ya que es de esa manera como persuade a que se tome en serio el problema de la ciberdelincuencia, en su aspecto legal, dadas las diversas materias que incluye el área penal, procesal y constitucional.

Por ende, las fuentes de información analizadas manifiestan que con el propósito de conseguir una base legal más adaptada y precisa en el contexto de la ciberdelincuencia, resulta necesario no solo un estudio de casos a nivel nacional sino también reivindica la importancia de los antecedentes internacionales en la elaboración de un sistema legal que cumpla con los diversos criterios que hoy por hoy se piden y para lo cual serán utilizados. Asimismo, ya que el proceso de estudio de las legislaciones extranjeras es un tema reciente, pero que sin embargo ha sido un medio utilizado para múltiples modificaciones legales, contribuye a no pasar desapercibido el tema de los ciberdelitos. De ahí que actuando no solo en vista del presente es que se plantea y propone una iniciativa de modificación, y que ello sirva a las generaciones futuras como un precedente legal al momento de presentarse distintas modalidades y/o casos poco frecuentes en el ámbito procesal, penal y constitucional. Cabe recalcar que actualmente, al formar parte del Convenio de Budapest, y tener como ejemplos la Ley 30171, permite tener conocimiento de la ciberdelincuencia, aunque algo limitada en contexto de los avances de la cibertecnología. En efecto, el estudio de la legislación peruana en conjunto con la extranjera genera un acercamiento

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

más profundo entre el Estado y la sociedad, esto debido a la evolución de las modalidades de ciberdelitos y su peligrosa acción sobre los derechos fundamentales de las personas y de su seguridad personal, financiera y colectiva.

Finalmente, en cuanto al objetivo general analizar el abordaje, evolución y los desafíos de la normativa jurídica peruana relacionada con la suplantación de identidad a través de medios digitales, identificando oportunidades para fortalecer la legislación y proteger mejor los derechos de los individuos en el entorno digital; las fuentes de información analizadas sugieren una necesidad crítica de actualización y adaptación de las leyes peruanas. Resaltan la urgencia de incorporar nuevas modalidades de ciberdelitos, especialmente la suplantación de identidad, en el marco legal existente, alineando las prácticas nacionales con estándares y tratados internacionales como el Convenio de Budapest. Esto implica no solo la modificación de leyes existentes sino también la creación de nuevas regulaciones que respondan eficazmente a los avances tecnológicos y las cambiantes dinámicas de la ciberdelincuencia, enfatizando la importancia de la cooperación internacional y la innovación legal para garantizar una protección integral en el espacio digital.

5. Discusión

La presente investigación tiene como objetivo principal el de analizar el abordaje, la evolución y los desafíos de la normativa jurídica peruana relacionada con la suplantación de identidad a través de medios digitales. Se identifica oportunidades para fortalecer la legislación y proteger de mejor manera los derechos de los individuos en el entorno digital, argumentando que el desarrollo tecnológico a lo largo de los años ha agravado los ciberdelitos, con impactos económicos y morales en la sociedad peruana. Por ello, se examinó la evolución de la normativa jurídica vigente en relación a la suplantación de identidad, evaluando su eficacia en la protección y restitución de los derechos vulnerados, tanto patrimoniales como extrapatrimoniales, con el propósito de formular una propuesta de mejora normativa que satisfaga las necesidades de seguridad de la población.

Esto concuerda con Vega y Arévalo (2022), quienes afirman que los avances de los ciberdelitos originaron una obligatoria evolución en el marco jurídico nacional, manifestándose en la creación y promulgación de la Ley 30096, Ley de Delitos Informáticos, la que posteriormente fue modificada en la actual Ley 30171. Asimismo, se evidenció en su adhesión al Convenio de Budapest. Sin embargo, a pesar del intento de mitigar los delitos en el medio digital, las leyes con las cuales se rige Perú en esta área es bastante limitada y su eficacia no resulta satisfactoria para los mismos usuarios

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

vulnerados. Por tanto, se insta que se gestione el problema de manera adecuada por parte de las autoridades y la promulgación normativa.

Por otro lado, Zorrilla (2018) sí considera la existencia de ambigüedades en el artículo 9 de la Ley de Delitos Informáticos, pero no precisamente porque esta no desarrolle bienes jurídicos tutelados o especificaciones de las modalidades delictivas, sino porque estima que existe una superposición del tipo penal, ya que el artículo 438 del Código Penal peruano desarrolla el delito de la Falsedad Genérica, la cual sanciona a quien cometa falsedad suponiendo, simulando y alterando la verdad *en cualquier medio* de forma intencional en agravio de terceros, lo que es equivalente a la suplantación de identidad como delito informático también, puesto que el propio artículo del CP enfatiza el uso de cualquier medio para cometerlo. Como resultado, los legisladores de la Ley 30096 y su modificatoria Ley 30171 están errando al pretender legislar el medio a través del cual se comete el delito en lugar de conductas, las cuales ya están previamente tipificadas en el Código Penal.

Por tanto, los argumentos presentados evidencian la evolución legislativa nacional en relación a la suplantación de identidad a través de los medios digitales, así como los desafíos que presenta en su eficacia y aplicación. Dicha información ha sido examinada con el fin de mejorar y reforzar la normativa jurídica en busca de proteger los derechos de los ciudadanos en las plataformas digitales.

De acuerdo con el objetivo específico 1, en la cual invita a examinar las características y limitaciones de la legislación peruana actual en el contexto de los ciberdelitos, con especial énfasis en la suplantación de identidad digital, en donde se argumenta que, pese a los avances normativos que ha logrado Perú en el tema de delitos cibernéticos, no logra ser suficiente para satisfacer las necesidades de seguridad que requiere la sociedad peruana, ya que las leyes que abordan la suplantación de identidad como delito informático no han logrado profundizar en el desarrollo de este, dejando muchas lagunas jurídicas.

Esto concuerda con Quispe y Quispe (2023), quienes afirman que el artículo 9 que trata sobre la suplantación de identidad de la Ley 30096 no especifica en ninguna de sus líneas la suplantación de identidad en las transacciones comerciales, como la compra y venta por internet, y las transferencias bancarias, lo que deja un amplio vacío legal. Por lo cual, se enfatiza la importancia de la actualización del artículo 9 de la Ley 30096, conforme lo dispuesto por el Decreto Legislativo 1591, en los siguientes términos:

> Artículo 9. Suplantación de identidad: El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

> conducta resulte algún perjuicio, material, moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole.

Se suma a ello la necesidad de considerar como bienes jurídicos protegidos tanto los datos como las contraseñas digitales.

Por su parte, Alberca (2017), si bien reconoce la necesidad de una modificación del artículo 9 de la Ley de Delitos Informáticos, no la considera como única solución para la eficacia de esta norma contra el delito de suplantación de identidad, sino que plantea la implementación de talleres de aprendizaje sobre la tipificación y desarrollo de delitos informáticos por parte del Poder Judicial y el Ministerio Público con el fin de mejorar la administración y control de justicia, así como garantizar la seguridad en las redes sociales para los usuarios. Además, considera de suma relevancia que la División de Investigación de Delitos de Alta Tecnología, parte de la Policía Nacional del Perú, organice eventos que promuevan el uso de las tecnologías en busca de la mejora y reforzamiento en la tipificación de los delitos digitales.

Por tanto, dichos argumentos exponen, luego de ser examinada, una crítica en su mayoría negativa hacia la actual regulación normativa sobre el delito de suplantación de identidad en los medios digitales, tipificado en el artículo 9 de la modificada Ley 30171, ya que sus vacíos legales así como sus ambigüedades imposibilitan su correcta aplicación y, por consiguiente, eficacia.

De acuerdo con el objetivo específico 2, en la cual invita a analizar los desafíos prácticos y teóricos en la aplicación de la legislación existente sobre suplantación de identidad digital en medios digitales, se argumenta que la existencia de ineficacia de la Ley 30096 incide significativamente en diversos delitos por medios informáticos que el agraviado desconoce sobre la respectiva diligencia que debe de seguir al captar que la información privada y personal ha sido vulnerada, utilizando diferentes técnicas con fines ilícitos. En consecuencia, el delito de suplantación de identidad por medios informáticos no incluye en su tipificación una redacción específica adecuada, lo que hace que en la mayoría de los casos no se sancione debidamente.

Quispe y Quispe (2023) destacan que el *phishing* y el *vishing* son técnicas que utilizan los ciberdelincuentes en situaciones cotidianas para obtener información personal de la víctima mediante correos maliciosos que aparentan ser fehacientes o mensajes de

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

texto. Por ello, todo lo contrastado está relacionado con los diferentes métodos para cometer los ciberdelitos. Además de que se ha podido verificar que quienes cometen delitos informáticos son expertos en tecnología informática, como también pueden ser novatos interesados en la tecnología.

Por su parte, Núñez (2016) admite que, mientras no exista la trascendencia del respeto y protección del derecho de identidad digital en Internet para brindar la protección de datos personales, bajo el marco de un sistema funcional eficiente, con la finalidad de lograr la confianza necesaria a nivel internacional y permitir que un ciudadano peruano pueda tener acceso a servicios públicos en línea en otros Estados internacionales, no se generaría próximamente un progreso en los diversos desafíos que posee la legislación peruana.

Por tanto, dichos argumentos señalan que existe ineficacia en Ley 30096 que incide significativamente en diversos delitos por medios informáticos, como la suplantación de identidad, debido a una falta de redacción específica adecuada en su tipificación. Además, se destaca el desarrollo de diversas técnicas como el *phishing* y el *vishing* utilizadas por ciberdelincuentes para obtener información personal de las víctimas, en la cual, los perpetradores de estos delitos pueden ser tanto expertos en tecnología informática como novatos. Esto se refiere a la importancia de garantizar el respeto y protección del derecho de identidad digital en Internet para proteger los datos personales. Al respecto, la presente investigación invita a buscar soluciones y mejorar el desarrollo de los casos sobre ciberdelitos originados en los medios digitales para lograr reforzar las normas jurídicas de la legislación peruana.

De acuerdo con el objetivo específico 3, en la cual invita a comparar las tendencias internacionales con la situación en Perú para entender el posicionamiento del país en el contexto global, en donde se argumenta que desde el progresivo avance de desarrollo de la legislación le ha dado a los delitos informáticos una progresiva y coherente codificación en el artículo 207 del Código Penal, en la Ley 30096 y las modificaciones realizadas por Ley 30171, permitió un avance a una legislación ordenada y codificada de los tipos de ciberpunibles mencionados en el convenio de Budapest, aunque se declare la existencia de inconsistencias o la necesidad de mejora actualmente.

Esto concuerda con lo que Mejía et al. (2023) destacan sobre la relevancia del funcionamiento del Estado y la regulación en el ámbito de la información y la implementación de políticas de seguridad informática, ofreciendo una perspectiva integral y mejorada sobre los comportamientos en línea y su importancia en el contexto legal. Así, se consideró el marco normativo nacional y las conductas tipificadas como

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

ciberdelitos según la Ley 1273 de 2009, prestando especial atención al manejo de datos y sistemas informáticos, lo cual implica directamente la prevención y persecución de delitos cibernéticos, especialmente en los grupos uno y dos de ciberdelitos agrupados en el Convenio de Budapest. Asimismo, se menciona que el desarrollo legislativo de Perú ha sido progresivo y rápido a diferencia de Colombia que no aparejan el mismo alcance de la legislación peruana, la cual, rebasa la codificación de punibles sobre la información y los datos.

Por otro lado, Alberca (2017) resalta la obligación y urgencia de modificar la legislación para mejorar la tipificación del artículo 9 sobre suplantación de identidad en los delitos informáticos, demostrando la importancia de la necesidad de modificaciones legislativas que respondan a los cambios constantes de uso de la tecnología con finalidades ilícitas causadas por la ciberdelincuencia.

Por tanto, dichos argumentos señalan que existe el avance progresivo en la codificación de los delitos informáticos en el Código Penal, pero se reconoce la existencia de inconsistencias. Además, se enfatiza la importancia del funcionamiento del Estado y la regulación informativa y la implementación de políticas de seguridad informática, y la urgencia de modificar la legislación que debe adaptarse a los cambios constantes en el uso de la tecnología con fines ilícitos. El progreso de la legislación peruana en sus normas jurídicas ha demostrado un avance favorable, manteniéndose nivelada a los requerimientos del Convenio de Budapest y los acuerdos internacionales según sus lineamientos, pero con la obligación de desarrollar y modificar leyes idóneas.

6. Conclusiones

1. Este estudio analiza el abordaje, la evolución y desafíos de la normativa jurídica peruana sobre suplantación de identidad digital, destacando la importancia crucial de la colaboración interinstitucional para una efectiva actualización legislativa y protección en el ámbito digital. La necesidad de alinear la legislación nacional con estándares internacionales, como el Convenio de Budapest, es enfatizada por expertos como Martínez (2020) y Pedrero (2021), quienes resaltan la urgencia de adaptar la legislación frente a la rapidez de la evolución tecnológica y la emergencia de nuevas modalidades de ciberdelitos.
2. Se reconoce un progreso legislativo con la actualización de leyes como la 30096 y la 30171, aunque se critica la persistencia de deficiencias en su capacidad para abordar la suplantación de identidad en transacciones digitales.

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Expertos como Zorrilla (2018) y Quispe y Quispe (2023) sugieren una legislación más específica y detallada para mejorar la protección digital efectiva.

3. Se destacan los desafíos prácticos en la implementación de la ley, donde la actual Ley 30096 se muestra inadecuada para defender contra la suplantación digital eficazmente, permitiendo a los delincuentes explotar vulnerabilidades a través de técnicas como el *phishing* y el *vishing*. La comparación con tendencias globales muestra que, si bien Perú ha progresado, aún requiere mejoras sustanciales para fortalecer su marco legal en comparación con estándares internacionales y responder adecuadamente a las amenazas emergentes.
4. Es imperativo una revisión y adaptación continua de la normativa jurídica peruana para proteger los derechos digitales de los individuos y mantenerse al paso con las dinámicas de ciberdelincuencia global. La cooperación internacional y una visión legislativa innovadora y proactiva serán clave para asegurar que la tecnología beneficie a la humanidad sin comprometer la seguridad y la privacidad individual.

Referencias

Aguilar, E. (2019). *Suplantación de la identidad digital con fines de trata de personas en Facebook* [Tesis de maestría, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. Repositorio de INFOTEC. https://infotec.repositorioinstitucional.mx/jspui/handle/1027/363

Alberca, H. (2017). *Importancia de proponer la modificatoria del art. 9 de la Ley 30096 a fin de tipificar una mejor conducta delictiva en una materia de suplantación de identidad en los delitos informáticos, Perú. 2017* [Tesis para Título Profesional, Universidad Alas Peruanas]. Repositorio de la Universidad Alas Peruanas. https://repositorio.uap.edu.pe/handle/20.500.12990/4908

Belisario, A. (2014). *Análisis de métodos de ataques de phishing* [Trabajo Final de Posgrado, Universidad de Buenos Aires]. Biblioteca Prof. Emérito Alfredo L. Palacios. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0840_BelisarioMendezAN.pdf

Congreso de la República del Perú. (2013, 27 de septiembre). Ley 30096. Ley de Delitos informáticos. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Congreso de la República del Perú. (2014, 10 de marzo). Ley 30171. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. Diario Oficial El Peruano 12780.

https://www.mef.gob.pe/contenidos/servicios_web/conectamef_quechua/pdf/normas_legales_2012/NL20140310.pdf

Congreso de la República del Perú. (2019, 13 de febrero). *Convenio sobre la ciberdelincuencia.* Diario Oficial El Peruano. https://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2292019/22-09-2019_CONVENIO.pdf

Congreso de la República del Perú. (2023, 13 de diciembre). Decreto Legislativo 1591. Decreto Legislativo que modifica la Ley 30096, Ley de Delitos Informáticos, para promover el uso seguro y responsable de las tecnologías digitales por niñas, niños y adolescentes. Diario Oficial El Peruano. https://www.gob.pe/institucion/mpfn/informes-publicaciones/5258286-decreto-legislativo-n-1591

Fernández, C. (1997). Daño a la identidad personal. *THEMIS Revista de Derecho*, (36), 245-272. https://revistas.pucp.edu.pe/index.php/themis/article/view/11743

García, R. A. (2017). *Seguridad Informática y el malware* [Tesis de licenciatura, Universidad Piloto de Colombia]. Repositorio de la Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/2641

Hernández, D. A. (2019). *La suplantación de identidad cibernética en el Ecuador* [Tesis de maestría, Universidad Externado de Colombia]. Repositorio de la Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/entities/publication/e4c9884a-ad38-4350-a324-fc732276eb93

Hernández-Sampieri, R. & Mendoza, C (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. Editorial Mc Graw Hill Education.

Instituto Nacional de Estadística y Censos. (2017). *Programa Nacional de Estadística 2017-2021*. Instituto Nacional de Estadística y Censos, Quito-Ecuador. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Normativas%20Estadisticas/Planificacion%20Estadistica/Programa_Nacional_de_Estadistica-2017.pdf

Leguizamón, M. S. (2015). *El phishing* [Tesis de licenciatura, Universitat Jaume I]. Repositorio de la Universitat Jaume I. https://repositori.uji.es/xmlui/handle/10234/127507

Martínez, F. (2020). Ciberseguridad y Estado autonómico. *ICADE. Revista de la Facultad De Derecho,* (109), 1–19. https://doi.org/10.14422/icade.i109.y2020.001

Martins, S. (2020). *Convenio de Budapest sobre la ciberdelincuencia en América Latina*. IDRC Canadá. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Mejía, M., Hurtado, S. V. y Grisales, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, *29*(2), 356-372. https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

Montaperto. J. V. (2018) *Trabajo final de graduación. Suplantación de identidad. Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino* [Tesis de licenciatura, Universidad Siglo 21]. Repositorio de la Universidad Siglo 21. https://repositorio.uesiglo21.edu.ar/handle/ues21/15652

Núñez, J. (2016). *Derecho de identidad digital en internet* [Tesis de doctorado, Universidad Nacional Mayor de San Marcos]. Repositorio institucional Cybertesis UNMSM. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/6252/N%C3%BAnez_pj.pdf?sequence=2&isAllowed=y

Pedrero, Z. J. (2021). *Suplantación de identidad* [Tesis para título profesional, Universidad Miguel Hernández de Elche]. Repositorio de core. https://core.ac.uk/works/129118814

Quispe, V. F. y Quispe, L. S. (2023). *Análisis jurídico de la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.* [Tesis de licenciatura, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/110772/Quispe_AVF-Quispe_SLS-SD.pdf?sequence=8&isAllowed=y

Solís, C. (2018). *Usurpación de identidad digital: un estudio comparativo de soluciones francesas, mexicanas y norteamericanas* [Tesis de doctorado, Universidad Paris Saclay y Université panaméricaine]. Repositorio de HAL open science. https://theses.hal.science/tel-01797447/document

Vega, J. A. y Arévalo, M. (2022). *Ciberdelitos: Análisis en el sistema penal*. Editorial Iustitia. https://drive.google.com/file/d/1DZEk_8nJuKr6qDEliowWFHMiWynwqdQQ/view?usp=drive_link

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis, 53*(053), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zorrilla, K. (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento* [Tesis de licenciatura, Universidad Nacional de Ancash Santiago Antúnez de Mayolo]. Repositorio de la Universidad Nacional de Ancash

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228

Santiago Antúnez de Mayolo. https://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowed=y

Revista Sapientia & Iustitia, N. 12, 2025, pp. 5-36 e-ISSN 2709-1228