UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

ROL DE LOS INTERMEDIARIOS DE INTERNET EN LA LUCHA CONTRA EL DELITO DE SUPLANTACIÓN DE IDENTIDAD EN PERÚ, 2020

TESIS

PRESENTADA POR:

YESENIA LUPACA QUISPE

PARA OPTAR AL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2024

Reporte de similitud

NOMBRE DEL TRABAJO

ROL DE LOS INTERMEDIARIOS DE INTER NET EN LA LUCHA CONTRA EL DELITO D E SUPLANTACIÓN DE IDENTIDAD EN

AUTOR

YESENIA LUPACA QUISPE

RECUENTO DE PALABRAS

22489 Words

RECUENTO DE CARACTERES

127761 Characters

RECUENTO DE PÁGINAS

94 Pages

TAMAÑO DEL ARCHIVO

1.9MB

FECHA DE ENTREGA

Apr 22, 2024 10:12 AM GMT-5

FECHA DEL INFORME

Apr 22, 2024 10:20 AM GMT-5

5% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 5% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 3% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 12 palabras)

JULIO JESUS CUENTAS CUENTAS

ASESOR DE TESIS

UNIVERSIDAD NACIONAL DEL ALTIPLANO
Facultad de Ciencias Jurídicas y Políticas

Abg. Eva Marina Centeno Zavala
DIRECTORA DE LA UNIDAD DE INVESTIGACIÓN

Resumen

DEDICATORIA

Dedico este trabajo a todas las personas que han sido parte fundamental en mi camino de aprendizaje y crecimiento. A mi madre, Elena Quispe Vda. de Lupaca, por su amor incondicional, apoyo constante y sacrificios que han hecho posible mi educación. A mis seres queridos, por su aliento y compañía en cada paso de este camino. Con gratitud, dedico este trabajo a todos ustedes.

Yesenia Lupaca Quispe

AGRADECIMIENTO

Mi más sincero agradecimiento a todas las personas que han contribuido sustancialmente a este trabajo.

En primer lugar, a Dios por las fuerzas que me ha dado para seguir adelante en medio de las dificultades. Mi fe y su amor me dieron coraje para no rendirme y afrontar los momentos más desafiantes.

En segundo lugar, a la Universidad Nacional del Altiplano, Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho por su formación profesional.

Agradecer a mi asesor de tesis, Maestro Julio Jesús Cuentas Cuentas, por su orientación, paciencia y apoyo constante a lo largo de todo el proceso de investigación. Sus valiosas sugerencias y comentarios han sido fundamentales para lograr los objetivos propuestos.

No puedo pasar por alto agradecer a todas las fuentes académicas y referencias que he usado en mi investigación, así como a los profesionales por su colaboración en la realización de entrevistas, lo que ha permitido obtener datos valiosos para el desarrollo de esta investigación.

Yesenia Lupaca Quispe

ÍNDICE GENERAL

Pág.

CAPÍTULO III

MATERIALES Y MÉTODOS

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

ÁREA: Ciencias Sociales

LÍNEA: Derecho

SUBLÍNEA: Derecho Penal

TEMA: Delitos Contra la Fe Pública

FECHA DE SUSTENTACIÓN: 26 de abril del 2024

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

ACRÓNIMOS

DIVINDAT:	División de Investigación de Delitos de Alta Tecnología
INISEG:	Instituto Internacional de Estudios de Seguridad Global
OEA:	Organización de los Estados Americanos
ONU:	Organización de las Naciones Unidas
RENIEC:	Registro Nacional de Identificación y Estado Civil

RESUMEN

La presente investigación se centra en la suplantación de identidad en la vida electrónica o digital. Se lleva a cabo en Perú con el objetivo principal de examinar cómo se pueden utilizar los intermediarios de Internet para combatir el robo de identidad en Perú para el año 2020. Se utilizaron entrevistas como medio de recopilación de datos para el diseño de la investigación cualitativa. Ocho profesionales del Derecho vinculados al tema del estudio proporcionaron la información. Los principales hallazgos indican que en el Perú no existe un marco legal que regule las obligaciones y actividades de los intermediarios de Internet en la lucha contra el robo de identidad. Se concluye en parte que en la actualidad el rol intermediario es fundamental, manteniendo en su carga la necesaria implementación de medidas de seguridad al encontrase inmerso en este proceso digital de servicios telemáticos un conjunto de derechos personales y sociales que deben ser protegidos, como el derecho a la privacidad, a la reserva de la identidad e incluso el derecho a la dignidad, a la reputación, entre otros; además de que debe permitir que los órganos respectivos obtengan una clara identificación del usuario en el caso del cometimiento de delitos informáticos. No obstante, se concluyó igualmente que en los actuales momentos el rol del intermediario no termina siendo efectivamente eficaz o idóneo, por cuanto en general no cuenta con las herramientas digitales propicias como los aludidos sistemas de control biométrico o aplicativos y software para realizar el debido control de identidad. Aunado a ello, no existe una regulación exhaustiva sobre este rol, las medidas a aplicar y la responsabilidad penal y civil que resulten adjudicables, por lo que urge dictar una ley que abarque estos supuestos, o al menos una reforma legal que se actualice en cuanto a ello y al cometimiento de delitos informáticos.

Palabras clave: Delitos cibernéticos, Intermediarios de Internet, Responsabilidad, Suplantación de identidad.

ABSTRACT

This research focuses on identity theft in electronic or digital life. It is carried out in Peru and the main objective is circumscribed to inquire about the role of Internet intermediaries in the fight against the crime of identity theft in Peru, 2020. Regarding the research methodology, it was of a qualitative nature using the interview as a data collection instrument. The information was obtained from eight lawyers related to the subject of study. In the main results it is observed that in Peru there is no legislation that regulates the responsibility and actions of Internet intermediaries to fight against identity theft. It is partly concluded that at present the intermediary role is fundamental, keeping in charge the necessary implementation of security measures when immersed in this digital process of telematic services a set of personal and social rights that must be protected, such as the right to privacy, to the confidentiality of identity and even the right to dignity, reputation, among others; In addition, it must allow the respective bodies to obtain a clear identification of the user in the case of the commission of computer crimes. However, it was also concluded that at present the role of the intermediary does not end up being effectively effective or suitable, since in general it does not have the appropriate digital tools such as the biometric or application control systems and software to carry out the due control. of identity. In addition to this, there is no exhaustive regulation on this role, the measures to be applied and the criminal and civil liability that may be adjudicable, so it is urgent to enact a law that covers these cases, or at least a legal reform that is updated as soon as possible. to it and to the commission of computer crimes.

Keywords: Cyber-crimes, Identity theft, Internet intermediaries, Responsibility.

CAPÍTULO I

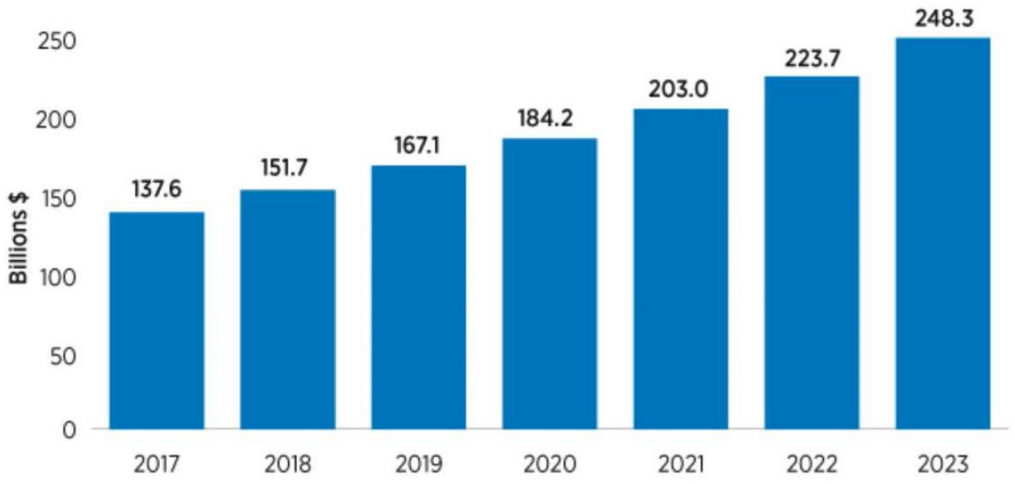
INTRODUCCIÓN

El Internet apareja un sin fin de oportunidades, pero a su vez representa numerosos riesgos para las sociedades, como ha sido la masificación los llamados delitos informáticos, cibercriminalidad o delincuencia informática, entre los que se encuentran la suplantación de identidad (López, 2016). De manera particular, desde el contexto procesal del derecho, una de las dificultades jurídicas devenidas por el uso del Internet es la determinación del lugar de comisión de los delitos informáticos y, consecuencialmente, la competencia del órgano encargado de juzgar los hechos que originan el delito; así como, el establecimiento de la autoría. Así, el crimen cibernético representa una secuencia de conductas disvaliosas que hasta hace poco eran impensables y que, hasta hoy día, algunos siguen siendo complejos de tipificar en las normas penales tradicionales (Acurio, 2015).

A nivel mundial, la ciberdelincuencia es el negocio ilícito más lucrativo, superando incluso al narcotráfico. Actualmente, las cifras negras por ataques informáticos y fraudes económicos empleando la tecnología, alcanzan números inimaginables (INISEG, 2019). Así, los datos recogidos y las predicciones para el siguiente año se concentran en la figura 1.

Figura 1

Proyecciones de los costos de los daños



Nota: USECIM (2019)

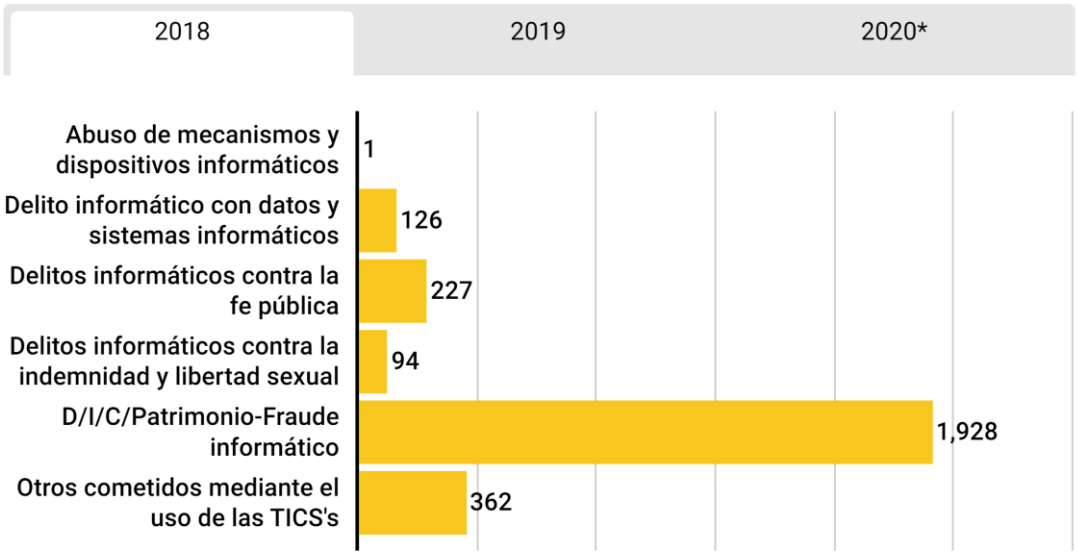
De acuerdo con ello, los costos anuales de los delitos cibernéticos en cada país representan cifras elevadas, demostrando que éstos se encuentran en constante y exponencial crecimiento, que se reflejan en daños y destrucción de datos, apropiación indebida de propiedad intelectual, sustracción de información personal y financiera, malversación, y actos fraudulentos, piratas informáticos, entre otros, por lo que se requieren mayores y mejores esfuerzos para combatirlos efectivamente (USECIM, 2019).

En el caso específico del Perú, en lo que respecta a las infracciones cibernéticos, solo para el año 2019 se registraron 3,012 denuncias ante la División de Investigación de Delitos de Alta Tecnología (Divindat), cuyas infracciones cibernéticas principales fueron pornografía infantil, suplantación de identidad, transacciones no autorizadas, compras fraudulentas, en cuyos casos los delincuentes recurrieron al uso de instrumentos digitales como los medios sociales, programas informáticos y otros sistemas online. El bien jurídico protegido más afectado fue el patrimonio (Pichihua, 2019). Para el primer semestre del 2020, comparativamente con el año anterior, las cifras se han incrementado

considerablemente ante el creciente uso del Internet, reflejándose la cantidad de denuncias en el presente gráfico (Gestión, 2020).

Figura 2

Denuncias de delitos informáticos de enero a junio 2020



Nota: Gestión (2020) Elaboración: Dividant PNP

De manera particular se tiene que para el año 2019, la Policía Nacional del Perú recibió 247 denuncias por el delito de suplantación de identidad a través de redes sociales y páginas de Internet, superando la cifra de 227 denuncias registradas en el año anterior. La mayoría de los denunciantes describían encontrar en perfiles con sus fotos, pero con nombres falsos (Gestión, 2020).

En lo que respecta al ordenamiento jurídico peruano, el Código Penal (1991) hizo un esfuerzo por abordar el tema de los delitos informáticos desde una perspectiva patrimonialista al restringir el uso de computadoras y el conocimiento informático como circunstancia agravante. Sin embargo, en la realidad, esta concepción era muy limitada pues sólo permitía sancionar un grupo limitado de conductas, lo cual resultaba problemático dado el imparable crecimiento de los delitos informáticos en sus diversas

modalidades y la amplia gama de estrategias empleadas para borrar por completo cualquier evidencia de los ilícitos (Morales, 2016).

Por lo tanto, la Ley de Delitos Informáticos, Ley N° 30096, fue publicada en 2013 con la intención de disuadir y perseguir la actividad delictiva relativa a los sistemas y datos informáticos, la privacidad y confidencialidad de las comunicaciones, los activos y la confianza pública, cuando el autor utiliza la tecnología moderna para cometer tales delitos (Ley N° 30096, 2013). La Ley N° 30171, publicada en 2014, revisó esta norma añadiendo una nueva categoría de delitos (Ley N° 30171, 2014).

El Convenio de Budapest o Convenio sobre Ciberdelincuencia, es la base también para estas leyes. Sin embargo, en 2019, el Poder Ejecutivo ratificó el Convenio a través del Decreto Supremo Nº 010-2019-RE del 10 de marzo de 2019, luego de que la Resolución Legislativa Nº 30913 del 12 de febrero de 2019 lo aprobara (Resolución Legislativa N° 30913, 2019).

Ahora bien, la gran magnitud del delito de suplantación de identidad se debe en parte a la multiplicidad de factores que intervienen en el proceso de prestación de servicio, en particular los distintos intermediarios que participan en las diversas fases que integran la red. De esta manera los intermediarios son quienes facilitan sus plataformas o redes para que terceros realicen transacciones, servicios o negocios entre ellos (Califano, 2017). Hasta hace poco existía la concepción convencional de la libertad en la red y la autonomía del rol de los intermediarios, por lo que prácticamente no eran regulados.

La capa física de Internet, donde se encuentran los proveedores de servicios de conectividad, es una de las distintas etapas en las que operan los numerosos intermediarios. Otras etapas son la capa de aplicación, que está constituida esencialmente por plataformas que alojan contenidos, prestan servicios de almacenamiento, motores de

búsqueda o indexadores, redes sociales, entre otras. En general, estas plataformas dan acceso a Internet, transmiten e indexan contenidos, productos y servicios originados por terceros (Califano, 2017).

En función de ello, existe un consenso unánime a nivel internacional del rol fundamental y necesario que ejercen estos sujetos que facilitan todas las comunicaciones en lo que respecta a la capacidad de los usuarios para acceder a contenidos en Internet (Manila Principles, 2015). Así, lo ha ratificado la OEA al indicar que la transmisión de ideas e informaciones en Internet sería imposible sin estos actores, pues desempeñan un papel fundamental en el ejercicio de distintos derechos para cualquier individuo como el de explorar y recibir información a través de la red o el de libertad de expresión (OEA, 2013).

Estas circunstancias tan particulares de Internet, representan obstáculos para incriminar los actos delictivos de orden informático sin contar además con la exhaustividad de las pruebas, la capacidad de los funcionarios para investigar este tipo de delitos, los equipos tecnológicos con los que cuentan para ello, por lo que ante los graves perjuicios que traen consigo esas conductas delictivas, con modus operandi cada vez más novedosos, distintos países han creado legislaciones específicas sobre delincuencia informática procurando especializarse aún más tanto en la teoría de la norma como en la pericia (Corcoy, 2007).

En América Latina, los desafíos en general son atendidos por una regulación dirigida especialmente a atacar estas conductas, de manera tal que, en estos casos la responsabilidad de los intermediarios no se rige por los principios básicos generales de responsabilidad civil sino por estas leyes particulares, y en los que no existe tal normativa continúa dicha regulación por la normativa civil (Corcoy, 2007).

Así, ante tal participación protagónica de estos intermediarios informáticos, las obligaciones y cargas legales vinculadas a su responsabilidad han cambiado hacia un paradigma más sancionador, involucrando una extensa regulación del comportamiento de sus usuarios y de la red, uno de los desarrollos más significativos ha sido la ampliación de la responsabilidad penal de estos intermediarios, derribando con ello las concepciones iníciales del desorden normativo de la red y creando fuertes arquitecturas de control ante las políticas criminales basadas en nociones de riesgo (Millaleo, 2015).

Ahora bien, es claro que los intermediarios de Internet no pueden tener un conocimiento minucioso sobre todas las acciones que los usuarios llevan a cabo usando sus redes, plataformas o servicios, pero se pretende enervar un nivel de responsabilidad jurídica al tener conocimiento que se facilitó la perpetración de un delito o se amplificó un perjuicio a través del servicio que brindan, que en este caso sería la responsabilidad de éstos agentes frente a contenidos, los cuales pueden ser tan amplios como los tipos de delitos, entre los más comunes están pornografía infantil, derechos de autor, infracción de derechos personales, difamación, censura, entre otros (Califano, 2017).

De hecho, la ONU alertó en 2011 sobre el papel y la posición de los intermediarios, que los han convertido en los centros técnicos que permiten ejercer el control sobre los contenidos en Internet (ONU, 2011).

No obstante, no en todos los modelos regulatorios existe tal responsabilidad para los facilitadores en Internet, ya que existe inmunidad total cuando el intermediario es considerado como un simple mediador y no asume responsabilidad por los contenidos cargados por terceros, así como también existe inmunidad condicionada, conforme a la cual se exime de esta responsabilidad, pero en determinadas circunstancias, como sería eliminar o bloquear el contenido que ha sido notificado de su existencia o debe notificar

al usuario infractor de la ilegalidad del contenido subido. En todo caso, aún no se prevé regulación alguna que haya adoptado un sistema de responsabilidad imparcial, mediante la cual el mediador asume responsabilidad. absoluto por lo expresado por los usuarios a través de sus servicios (Califano, 2017).

Por su parte, a pesar de que el Perú busca restringir la culpabilidad de los intermediaros referente a la conectividad en la web a cambio de que éstos colaboren en la remoción del material ilícito de sus servidores, tal como lo ha hecho Estados Unidos de América, con quien el Estado peruano suscribió el Acuerdo de Promoción Comercial, aún subsiste el vacío en este sentido y como se aprecia de los datos estadísticos el número de delitos informáticos, y en particular de suplantación de identidad, crece año a año, por lo que es apreciable la urgencia de establecer una regulación sobre la limitación de responsabilidad de los proveedores de servicios de Internet, que contribuya de manera más exhaustiva en la lucha contra el delito de suplantación de identidad.

En definitiva, se requiere mayor claridad respecto al rol que juegan los intermediarios de Internet en la lucha contra la usurpación de identidad en el Perú; específicamente, es importante saber si la responsabilidad penal de estos intermediarios fortalece el control del Estado peruano sobre los principales usuarios de Internet del país y, en consecuencia, si obliga a estos a incrementar su monitoreo y vigilancia de los contenidos y usuarios de sus redes, o si han tomado las precauciones necesarias para evitar daños (Millaleo, 2015). De esta manera, se tiene como interrogante principal de la investigación, ¿Cuál es el rol de los intermediarios de Internet en la lucha contra el delito suplantación de identidad en Perú, 2020?

1.1. OBJETIVO GENERAL

Indagar sobre el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad en Perú, 2020.

1.2. OBJETIVOS ESPECÍFICOS

Analizar si el establecimiento de la responsabilidad penal de los intermediarios de Internet contribuye a fortalecer la actuación del Estado peruano frente al delito de suplantación de identidad.

- Constatar si el obligar a los intermediarios de Internet a monitorear y vigilar exhaustivamente a los usuarios de sus plataformas y sus contenidos, evita el cometimiento de los delitos de usurpación de identidad en el Perú
- Evaluar la necesidad de propiciar una ley sobre la delimitación de la responsabilidad de los proveedores de servicios de Internet para disminuir delitos informáticos en el Perú.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES

No se evidencian estudios específicos recientes relacionados de manera similar con el objeto de la presente investigación; sin embargo, se encontraron algunas investigaciones académicas relacionadas con la responsabilidad de los intermediarios de Internet y sobre los delitos de Internet, que pueden contribuir con fortalecer el estudio de estas variables.

Entre los estudios internacionales, se puede señalar la tesis de Jijón (2017), titulada "Responsabilidad de intermediarios de Internet: hacia una regulación que garantice el ejercicio del derecho a la libertad de expresión y otros derechos fundamentales", presentada ante la Facultad de Jurisprudencia de la Universidad Católica Santiago de Guayaquil, Ecuador, con el objetivo de proponer una normativa que regule la responsabilidad de estos intermediarios a efectos de garantizar el ejercicio de la libertad de expresión y otros derechos humanos que podrían verse vulnerados por ésta. Bajo un estudio documental, aduce que los intermediarios facilitan la actividad de los usuarios en el Internet y tienen las herramientas y el control sobre ciertos contenidos ilegítimos publicados por usuarios que podrían violar derechos de terceros. Agrega entre sus conclusiones que sería necesario para regular los contenidos y responsabilidad de intermediarios en Internet clasificar los tipos de contenidos que se pueden encontrar en la red, considerando la posible vulneración de derechos que pueda existir a través de ellos, esto es, los contenidos manifiestamente ilegítimos de los aparentemente ilegítimos; regulación que permita que el usuario que estime una vulneración de alguno de sus derechos, por algún contenido que reposa en la red, pueda denunciarlo ante el

intermediario y que este, tenga la capacidad suficiente para discernir ese conflicto de derechos, así tenga que contratar profesionales del derecho para que puedan resolver estos conflictos, dentro del marco del sistema de justicia. Además, que se determine de qué forma se aplicará la carga de la prueba.

Otra de los estudios es de Celli (2019), titulado "Las nuevas tecnologías y los delitos informáticos. Análisis de la Ley N° 26.388, Modificación del Código Penal argentino", presentado ante la Escuela de Abogacía de la Universidad Siglo 21, Argentina, con el objetivo de indagar si mediante la aludida ley modificatoria, el legislador ha logrado adecuar sus normas internas a los parámetros internacionales referidos a la regulación y control de los delitos informáticos. Mediante una investigación bibliográfica, pudo concluir que la legislación internacional, de países desarrollados, presenta desde hace tiempo un ordenamiento apropiado que incluye tanto a los delitos cometidos por medio del empleo de tecnologías o sistemas informáticos. Se resalta lo señalado por la ONU al señalar que éstos establecen que las normas sobre delitos informáticos son abarcativas, tanto de definiciones como de la tipificación de distintas modalidades, los cuales Argentina aún no ha considerado, en particular aquellas normas procesales que permiten la implementación de medidas de prevención y control del delito en el siglo XXI, incluyendo la intervención de intermediarios. Además, afirma que estos instrumentos internacionales comprenden protocolos de cooperación interestatal que permitirían la completa eliminación de esta particular forma de actividad delictiva.

Asimismo, se tiene el estudio de Levy & Aguerre (2019), titulado "Intermediarios de Internet. Consideraciones para reflexionar en el contexto de Argentina", establecer los fundamentos y principios que sustentan el discurso en torno a la regulación de los intermediarios en Internet, para organizar sistemáticamente los aspectos clave del debate. De un estudio documental, en parte, pudo concluir que existe una mayor demanda de

supervisión reguladora de los intermediarios, en particular de los afiliados a plataformas de contenidos en Internet. Esto exige una mayor responsabilidad en el bloqueo, filtrado y retirada de contenidos, sobre todo cuando tales acciones vulneran la libertad de expresión. El objetivo fundamental es establecer un equilibrio adecuado entre los diversos derechos implicados. Sin embargo, las políticas que dictan la responsabilidad legal de los intermediarios por el contenido de estas comunicaciones sí influyen en los derechos de los usuarios.

En el ámbito nacional se tiene a Morales (2016), con la tesis titulada “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015”, presentada ante la Facultad de Derecho de la Universidad Señor de Sipán, con el objetivo de estudiar los delitos informáticos, desde su contexto histórico hasta las distintas situaciones que enfrenta el legislador para su adecuada tipificación y aplicación, considerando derechos particulares como el derecho a la intimidad y su inseguridad, así como el constante uso de herramientas delictivas más sofisticadas, empleadas además por las organizaciones delictivas existentes en el Perú. Conforme a un análisis bibliográfico, determinó en parte que la delincuencia informática ha sido regulada internacionalmente, la identificación del modus operandi y el funcionamiento del delincuente como un reto importante en todos los tipos de actividad delictiva, con el fin de aprehenderlos como una de las principales preocupaciones. La criminalística se ha centrado específicamente en los delitos informáticos, sostiene que el mecanismo o arma más adecuado para combatir este delito es la aplicación de una legislación a escala nacional, local e internacional que aborde esta cuestión.

Otro estudio es el de Pardo (2018), titulado “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018”, presentado

ante la Universidad César Vallejo, con el objetivo de analizar dicho tratamiento. De tal manera que, bajo una investigación cualitativa, de nivel descriptivo explicativo, empleando la entrevista, se ha determinado que el marco jurídico penal relativo a los delitos informáticos contra la propiedad es inadecuado, ya que no abarca todos los tipos o modalidades de delitos informáticos dentro del fraude informático. Esto crea ambigüedad en la interpretación de la norma y dificulta la capacidad de castigar eficazmente los delitos informáticos contra la propiedad. Por ello, se sugiere que se lleve a cabo una iniciativa legislativa que clasifique explícitamente los delitos informáticos contra la propiedad, distinguiendo entre las distintas modalidades, con el fin de establecer penas claras y efectivas.

Asimismo, se tiene la tesis de Vilca (2018), titulada "Los Hackers: "Delito informático frente al Código Penal peruano" presentada ante la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional Santiago Antúnez de Mayolo, con el objetivo de conocer el vacío legal en el Código Penal peruano sobre los delitos de las comunicaciones electrónicas comerciales, determinar su relevancia jurídica y efectos perjudiciales en la sociedad, en particular sobre el derecho fundamental a la intimidad. Una vez realizado su análisis bibliográfico, concluyó que, a pesar de que en Perú se regulan los delitos informáticos, esta regulación presenta deficiencias debido a su carácter generalizado, generando vacíos legales que obstaculizan la realización de investigaciones forenses en el ámbito informático. Dada la gravedad de este delito, la presencia de peritos e investigadores debidamente formados en el lugar de los hechos, además del cumplimiento de los protocolos adecuados, son imprescindibles para la resolución más eficaz del caso. Por otra parte, la implantación de una normativa precisa que delimite las particularidades de los delitos informáticos y sus correspondientes acciones es crucial para mejorar el control sobre la materia. Los agentes encargados están obligados a

manejar todos los indicadores y componentes que puedan ser considerados como material probatorio en el proceso penal. En este sentido, es necesario extremar las precauciones en la gestión de estos elementos para salvaguardar su integridad. El tratamiento meticuloso y la acumulación de estas pruebas son fundamentales para garantizar su presentación efectiva ante el tribunal. Por lo tanto, la experiencia y los conocimientos especializados en el ámbito de la delincuencia informática son indispensables.

Teniendo en cuenta las investigaciones mencionadas, y a pesar de que existen varias definiciones e interpretaciones ampliamente aceptadas de la delincuencia y los delitos informáticos, se alcanza a señalar que esta modalidad de delincuencia puede definirse como un método que emplea la tecnología para delinquir, generalmente accionado por grupos organizados mediante la piratería de programas informáticos y otras formas de violación de distintos derechos (Ortiz, 2019). Conocida también como delito cibernético, constituye entonces un conjunto de actos, conductas o acciones que pueden clasificarse en categorías sustentadas en el objeto del delito material y el modus operandi (Senado de la República de México, 2019).

Los ciberdelincuentes adoptan formas muy diversas, diferenciándose solo por el tipo de infracción perpetuado, pudiendo ser incluso empleados de la propia empresa, no obstante, los delitos generalmente son cometidos por sujetos externos (Acurio, 2015).

Por su parte, las personas víctimas de los delitos son muy amplios, como individuos, empresas, instituciones crediticias, gobiernos, cuya principal similitud es que los individuos que emplean sistemas automatizados de información comúnmente están vinculados a otras plataformas. Resulta esencial determinar cuáles son los sujetos pasivos para poder determinar la modalidad del delito (Acurio, 2015).

Específicamente la suplantación de identidad, llamada también como usurpación, falsificación o robo de identidad, es el delito de mayor crecimiento a nivel mundial, sin que se detecten contundentes y acertadas acciones políticas para enfrentar este delito (OEA, 2018).

Este delito se encuadra en la categoría de falsedad del artículo 438 del Código Penal peruano, que también abarca la usurpación del nombre, calidad o empleo de otra persona con la intención de causar perjuicio a terceros, así como la simulación y la alteración o suposición intencionada de la verdad mediante el uso de palabras o hechos (Código Penal, 1991). Según el artículo 9 de la Ley de Delitos Informáticos, suplantar la identidad de otra persona con la intención de obtener una ventaja injusta o un beneficio personal causando un perjuicio económico o moral a un tercero se considera delito (Ley N° 30096, 2013).

Ello así, la suplantación de identidad se materializa cuando una persona, de manera no autorizada, obtiene, transfiere, posee, emplea o utiliza alguna información que le pertenece o distingue a otro sujeto, con la intención de cometer cualquier delito, como fraude o conductas ofensivas (Alarcón, 2015).

Las dimensiones involucradas con la suplantación de identidad a los efectos de estudio son plataformas digitales, considerando las plataformas empleadas para ejecutar el delito; las estrategias de ingeniería social o modalidad de engaño, que culminará con un daño económico y posiblemente reputacional a la víctima (ABC Redes, 2021).

Una de las principales acciones evitar y combatir la actividad delictiva de suplantación de identidad es la aplicación de las medidas legales en todas las áreas, lo que incluye la penalización, los poderes de procedimiento, jurisdicción, competencia, autoridades en general, órganos jurisdiccionales y de investigación, cooperación

internacional y responsabilidad de todos los sectores (Senado de la República de México, 2019).

En función de esto último, la responsabilidad de todos los sectores cabe profundizar sobre el rol de los intermediarios.

Estos sujetos son todas aquellas entidades que le facilitan a terceros realizar múltiples transacciones, y para ello ejecutan acciones como el *hosteo*, accesos, transmiten e indexan contenidos, servicios y productos creados o producido por otros sujetos. Existen infinidad de ejemplos, pero entre los más destacados están Google, Yahoo, Instagram, Facebook, entre otros (Califano, 2017).

Estos proveedores de servicios de Internet suelen clasificarse en función del tipo de trabajo que realizan en el proceso de intercambio de información en línea; básicamente son proveedores de: "a. acceso; b. tránsito; c. alojamiento; d. servicios en línea; e. búsqueda y enlace" (Abad, 2018).

En este caso, la responsabilidad legal de los intermediarios se vincula con los actos o conductas ilegales o dañinas que son transmitidas por usuarios empleando como medios los servicios que aquellos ofrecen (Abad, 2018).

Así, son distintas las propuestas legislativas en cuanto a la responsabilidad de estos facilitadores, una de ellas por ejemplo para el caso de Argentina, es eximirlos de responsabilidad por el contenido que circulan en las redes y que de alguna manera afecten derechos de los ciudadanos; pudiendo tener matices en este sentido, como el hecho de que el intermediario si tendría responsabilidad si había sido previamente notificado por un órgano jurisdiccional de la existencia de un contenido ilegal (Reichertz, 2018).

Una de las discusiones por las que se evita otorgarles la libertad a estos agentes facilitadores, es al considerar que solo son empresas privadas que no ejercen ninguna representatividad sobre el público y otorgarles es poder de decisión sobre cuestiones de legalidad se entendería como ceder parte de la función de justicia (Reichertz, 2018).

El modelo de responsabilidad objetiva es una forma adicional de responsabilidad que obliga a estos prestadores de servicios a indemnizar civilmente a sus clientes por cualquier daño causado al utilizar sus bienes o servicios por el único motivo de generar una actividad que entrañe riesgos para la sociedad de la información. Asimismo, se encuentra la responsabilidad subjetiva, sustentada en el principio de la culpa, por obrar de manera descuidada, negligente o imprudente, y en este caso los intermediarios solo deberían responder por un obrar culposo que consistiría en no retirar o bloquear los contenidos que almacenan o transmiten una vez que aquellos han sido notificados acerca de la ilicitud de estos (Abad, 2018).

Ahora bien, dependiendo del tipo de responsabilidad pueden surgir obligaciones para estos intermediarios, en el caso de la responsabilidad objetiva se podría exigir u obligar a esta parte como ente responsable a implementar o adoptar con distintas medidas de control y auto restricción para, por ejemplo censurar aquellos anuncios o contenidos lesivos para los usuarios en general, que por un parte pueden generar consecuencias nocivas desde el plano constitucional, pero a su vez pudieran contribuir en el control del Estado contra los delitos informáticos (Abad, 2018).

La vigilancia y el control de un número infinito de operaciones que se ejecutan continuamente a diario en un número infinito de lugares es una de las limitaciones que pueden derivarse. En este sentido, se han puesto en marcha diversas normativas de carácter general. Por ejemplo, el 8 de junio de 2000, el Consejo de Europa (2001) y el

Parlamento Europeo adoptaron la Directiva 2000/31/CE (2000) relativa a los aspectos jurídicos específicos de los servicios de la sociedad de la información, con especial énfasis en el comercio electrónico. Esta directiva prohíbe a los Estados miembros exigir a los prestadores de servicios que persigan activamente hechos o circunstancias que indiquen una actividad ilícita, o que controlen los datos que transmiten o almacenan, en relación con la materia mencionada.

Para salvaguardar el crecimiento de Internet como herramienta vital para la realización de diversas transacciones o el intercambio de información, es necesaria una legislación específica que establezca directrices precisas acordes con la noción de seguridad jurídica; pero sin que por ello se deje de sancionar supuestos aislados donde exista un evidente abuso a los derechos de los usuarios o de individuos en general, además de la importancia de que todos los participantes del proceso contribuyan con la lucha de los delitos informáticos (Abad, 2018).

2.2. MARCO TEÓRICO

2.2.1. Internet

Debe definirse como una herramienta global que conecta distintos dispositivos adaptados para su funcionamiento, es una fuente de información que no del todo se puede considerar como fidedigna, por lo que se debe saber maniobrar lo relacionado al acceso de este (Gibs, 2017).

Entre las características que se pueden mencionar del Internet se observan (Gibs, 2017):

- Información disponible todo el tiempo.

- Se usa para cualquier actividad, educación, entretenimiento, comercio, política, negocios, entre otro.
- No pertenece a nadie.
- Todas las personas pueden cargar información en Internet.
- Pueden o no existir leyes que regulen, dependerá del territorio.
- Brinda oportunidades para satisfacer necesidades.

El Internet facilitó el acceso a la globalización, al desarrollo de negocios, entre otros.

2.2.2. Intermediarios en Internet

Los intermediarios son aquellos que hacen posible que las personas puedan acceder efectivamente a Internet, son diversos los modos que se observan en los que puedan ser intermediarios, se tienen proveedores de Internet, proveedores de alojamientos en Internet, plataformas que funcionan como buscadores y redes, entre otros (Din, 2014).

Los intermediarios de Internet según Rojas (2023), son entidades que facilitan el acceso, la difusión y el resguardo de datos en la red, cuya labor en el ecosistema digital se clasifica como proveedores de usuarios en las siguientes categorías:

a) Proveedores de acceso a Internet (IAP). Ofrecen infraestructura y conectividad para el acceso a Internet, incluidos servicios de banda ancha, operadores de redes móviles y proveedores de Wi-Fi público.

b) Servicios de alojamiento o conocido también como *hosting*. Proporcionan a usuarios y empresas, espacio e infraestructura para almacenar sitios web, aplicaciones y otros contenidos en línea.

c) Servicios en la nube. Ofrecen servicios de almacenamiento, procesamiento y gestión de datos a través de infraestructuras remotas y compartidas desde cualquier lugar y dispositivo.

d) Motor de búsqueda. Ofrecen herramientas para buscar y recuperar información en línea a través de la indexación y clasificación de contenidos web, cuyo servicio es determinante en la navegación y la interacción en línea de los usuarios.

e) Intermediario o Intermediación. Operan plataformas en línea que conectan a usuarios y proveedores de bienes, servicios o contenidos, como comercio en línea, plataformas de social media y aplicaciones de mensajería instantánea.

f) Enlace y agregación de contenidos. Recopilan y presentan enlaces a terceros facilitando acceso a información, por ejemplo, los sitios web de noticias que agregan enlaces a distintos artículos.

Como indica Millaleo (2015), intermedio de Internet son considerado como los agentes mediante los cuales se logra facilitar acciones realizadas para terceros mediante el uso de las diferentes capas que tiene red, con el propósito de facilitar la comunicación de externos con los consumidores finales.

Podemos señalar que los intermediarios de Internet son entidades o plataformas que facilitan comunicación y transferencia de información entre usuarios, es decir, actúan como mediadores entre los usuarios y el contenido en

línea, proporcionando servicios y funciones que permiten la publicación, el acceso e interacción con la información en línea.

Algunos ejemplos de intermediarios de Internet engloban motores de búsqueda como Google, plataformas de redes sociales como Facebook y Twitter, así como proveedores de servicios de correo electrónico como Gmail y Yahoo, y plataformas de comercio electrónico como Amazon y eBay. Estos intermediarios desempeñan un papel crucial en la manera en que interactuamos y accedemos a la información en línea, y su impacto en la sociedad y la economía es cada vez más significativa.

Es importante mencionar que los intermediarios no son creadores de contenido, pero si facilitan que los contenidos y las diferentes actuaciones de las personas que acceden a sus servicios se puedan publicar. Por lo que, los intermediarios deben desarrollar políticas que permitan crear un filtro de contenido para facilitar el funcionamiento y la convivencia dentro de Internet, es por lo que alrededor del mundo se han generado códigos de responsabilidades para los intermediarios (Cotino, 2017):

- *"Responsabilidad objetiva* – por ejemplo, en China, donde se requiere que los intermediarios monitoreen activamente el contenido o en su defecto pueden llegar a enfrentar sanciones."
- *"Régimen de puertos seguros* – como en Singapur, Ghana, Uganda, Sudáfrica y la UE, donde los intermediarios son efectivamente inmunes de responsabilidad si cumplen con los procedimientos de *«notificación y retirada»*."

- *"Inmunidad casi absoluta de la responsabilidad sobre el contenido producido por otros* – modelo favorecido por ARTICLE 19 – como en los casos de los EE. UU. y Chile, donde el intermediario no es responsable del contenido producido por otros, siempre y cuando no intervenga sobre dicho contenido. El intermediario sólo elimina contenido si recibe una orden por parte de un tribunal u otro órgano judicial independiente (modelo jurisdiccional)".

Estos son modelos globales y que se pueden incentivar en diferentes partes del mundo sin menoscabar la legislación y adhiriéndose según las necesidades. Sin embargo, se debe observar lo relacionado a la libre expresión y a las limitaciones que se pueden dar si los terciarios censuran de determinada manera contenidos pero por otro lado, se ve la necesidad de regular la censura para garantizar el funcionamiento del Internet (Millaleo, 2015). Para efectos de esta investigación, importa saber que los intermediarios de Internet pueden funcionar como limitadores de contenido según lo que establezca la legislación.

2.2.2.1. Responsabilidad de los intermediarios de Internet en el ámbito de los delitos informáticos

La Ley de Delitos Informáticos, también conocida como Ley Nº 30096, ilegaliza una serie de acciones que afectan los sistemas y datos informáticos, la libertad e indemnidad sexual, la intimidad y secreto de las comunicaciones, el patrimonio y la fe pública. En cuanto a los tipos penales relacionados con la suplantación de identidad, se pueden mencionar los siguientes:

- **Tipo penal:** La Ley N° 30096, que aborda la responsabilidad penal de los intermediarios de Internet en relación con los delitos informáticos, establece que, dependiendo del grado de implicación en la comisión del delito, los proveedores de alojamiento web y de servicios de Internet pueden ser considerados cómplices o coautores.
- **Sujeto activo**: puede existir como persona jurídica o como persona física. Dicho de otro modo, cualquier persona física o jurídica que proporcione, facilite o permita el acceso no autorizado a un sistema informático o interfiera en los datos informáticos puede considerarse sujeto activo.

  Por otro lado, el autor Jimenez (2017) precisa que en los delitos informáticos no cualquier sujeto puede ser autor mediato, autor inmediato, instigador o cómplice, porque sólo aquel que realiza actividades en el ámbito informático con conocimientos sobre los sistemas informáticos, puede ser el autor mediato o material, tal como lo hacen los hackers, crakers, preakers, entre otros.
- **Sujeto pasivo:** Es el encargado del sistema informático o de los datos informáticos que han sido objeto de acceso no autorizado, interceptación, interferencia, uso, acceso o copia no autorizados. En otras palabras, es la persona o entidad a la que pertenecen los sistemas o datos que han sido afectados por la conducta ilícita.
- **Bien jurídico protegido:** La seguridad y privacidad de los sistemas y datos informáticos, así como la preservación de la información privada y sensible de los usuarios de Internet, son los

intereses jurídicos que se salvaguardan con este tipo penal. El objetivo de la norma es proteger la privacidad de los usuarios y la integridad de los sistemas en el ámbito digital.

- **Responsabilidad penal:** La responsabilidad penal de los intermediarios de Internet en este delito puede manifestarse tanto en forma de coautoría como de complicidad, dependiendo del nivel de implicación en la perpetración del delito. La jurisprudencia ha aclarado que los intermediarios pueden ser considerados coautores cuando tienen una participación activa y decisiva en la realización del delito, como en el caso de proveedores de servicios de Internet que permiten la entrada no permitida a sistemas informáticos. Por otro lado, podrán ser cómplices si su participación es secundaria o subsidiaria, como proveedores de alojamiento web que permiten la publicación de contenidos ilícitos en sus servidores. La responsabilidad penal estará en consonancia con el nivel de implicación en el delito y podrá ser agravada o atenuada considerando las condiciones específicas de la situación.

2.2.2.2. La omisión impropia como puerta a la responsabilidad de los intermediarios de Internet

Para establecer la culpabilidad legal de los proveedores de servicios de Internet, se han considerado los siguientes elementos: la omisión impropia como primer elemento, luego la posición del garante en cuanto a la capacidad técnica del intermediario, y la tercera es la aplicación del principio de culpabilidad con la atribución del conocimiento sobre el contenido ilícito; aunque se puede determinar que la aplicación de medidas

o cooperación son consideradas como atenuantes de la responsabilidad (Rojas, 2023).

Las principales obligaciones de los intermediarios como indica Rojas (2023), son dos; se tiene que la primera obligación es la posición de garante que se centra en el deber de cuidado que tiene el intermediario y aplica en cuanto a la prevención de daños de los bienes protegidos jurídicamente y, la otra es equivalente a la normativa que se centra en el control de la fuente de peligro, es decir, la regulación de la acción en el servicio.

Los intermediarios de Internet establecen sus condiciones referentes al uso de sus plataformas, por lo que el intermediario que no aplique sanción alguna cuando se incumplan las condiciones de uso preestablecidas; dicha actitud debe ser considerada como un comportamiento de omisión que puede atentar contra el derecho de los usuarios (Lara & Vera, 2011).

Por consiguiente, La noción de omisión impropia como base para la responsabilidad penal de los intermediarios de Internet, hace argumentar que éstos podrían ser responsables penalmente, siempre que se cumplan ciertos criterios. En primer lugar, la existencia de una posición de garante que puede surgir del control de la fuente de peligro, del deber de supervisión de terceros o del mandato legal. En segundo lugar, el conocimiento cierto del contenido ilícito, que no puede basarse en meras suposiciones o conjeturas. Y por último, la adopción de medidas

preventivas y la cooperación con las autoridades pueden servir como atenuantes o eximentes de responsabilidad Rojas (2023).

2.2.3. Identidad – Identidad en Internet

La identidad va enfocada en términos generales a la formación que hacen las personas sobre sí mismo. “Podemos decir que la identidad personal es un conjunto de características y elementos que las personas van adquiriendo a través de la interacción consigo mismas y con el entorno que les rodea desde niños y adolescentes.” (School, 2022).

Ahora bien, se debe mencionar que la identidad en tiempos de globalización debe ser llevada al campo digital o del Internet. Es así entonces que se debe mencionar lo relacionado a la identidad digital y esta no es más que como las demás personas observan a un interlocutor por medios electrónicos y de las redes sociales disponibles (Gobierno de Canarias, 2016).

Es posible crear esta identidad sin que se corresponda perfectamente con la realidad. Sin embargo, las acciones realizadas que utilizan esta identidad digital tienen consecuencias en el mundo real, y viceversa. La conversión de una identidad física en un personaje virtual se conoce como identidad digital (Gobierno de Canarias, 2016).

La identidad digital tiene un conjunto de características que es importante mencionar, pues sobre está identidad es donde pueden recaer posibles delitos, tal como se mencionará más adelante. Entre las características se pueden mencionar las siguientes según lo menciona Soto (2022):

- Social: Las personas no reconocen la autenticidad de la identidad.

- Subjetiva: Depende de lo que los demás usuarios perciban sobre la identidad.
- Valiosa: Dependiendo de la identidad creada, esta puede ser valiosa y generará importancia a las distintas empresas.

Esto lleva a que la identidad en Internet deba ser protegida para evitar que existan inconvenientes relacionados con la misma. La autora Soto (2022) señala que se puede proteger la identidad digital tomando en consideración algunas cuestiones:

- No conectarse en Internet públicos donde cualquier persona pueda acceder a los datos de la identidad.
- Utilizar páginas webs protegidas: es decir, las páginas webs deben tener los protocolos de encriptación necesarios para garantizar la seguridad.
- Cambiar y mantener actualizadas las contraseñas de las redes sociales, bancos, entre otros.
- Repasar la privacidad de las páginas webs, los permisos, mantener softwares actualizados, entre otros.

2.2.4. Suplantación de Identidad

El robo de identidad y la suplantación de identidad son dos de los problemas más frecuentes en las redes y en Internet en general. Se trata de utilizar Internet para hacerse pasar por otra persona, pero ¿por qué ibas a hacerlo? ¿Por qué es necesario que lo hagas? Aunque hay muchas razones diferentes para hacerlo, la intención general es hacer daño y molestar a la persona que se hace pasar por ella. También se llevan a cabo actividades fraudulentas bajo falsos pretextos suplantando perfiles (Universidad Veracruzana, 2016).

La suplantación de la identidad es una forma en la que efectivamente el Internet se puede utilizar de forma negativa (Mendo, 2014). Esta modalidad delictiva puede ser utilizada para realizar cualquier tipo de actividad, consiste desde el hurto de información hasta la fabricación de perfiles ficticios para hacerse pasar por la persona que suplantan (Kinde, 2019).

La autora Fresneda (2021) sostiene que en este tipo de infracción de usurpación de identidad vulnera el bien jurídico de seguridad en las relaciones jurídicas y es un problema que ha crecido de manera alarmante, considerándose los más frecuente:

- *Phising*: consiste en el robo de la identidad de una persona por medio del uso de correos electrónicos y puede robar diversa información.
- Suplantación de identidad en redes sociales y whatsapp: Se generan perfiles falsos y se comienza a comunicar con las personas conocidas de la persona que suplanta.

2.2.5. Fundamentos para la implicación de terceros civiles en delitos informáticos

En Paraguay se ha identificado que no se encuentra tipificado a nivel penal algunos comportamientos realizados por las plataformas digitales, pero se puede indicar que solo la mala utilización de las redes sociales se encuentra tipificadas como delitos; porque se ha resaltado que es fundamental que los Estados regulen la tipificación de conductas inapropiadas para así sancionar el ciberbullying, suplantación de identidad, stalking, entre otros (Génez & González, 2023).

El fundamento legal sobre los delitos informáticos se encuentra el convenio de Budapest que es considerada como una acción ilícita por cuanto el acceso a información de terceros constituye una vulneración de las medidas de seguridad; por lo que, para incurrir en el ilícito se ha determinado que deben tener deliberación y falta de legitimación (Villavicencio, 2014).

El término "tercero civil" se refiere a una persona física o jurídica que tiene que cumplir obligaciones financieras para compensar los daños resultantes de un acto ilícito, aunque no haya participado activamente en la comisión del acto ilícito (Pérez-Prieto, 2015).

Se pueden identificar diversas razones jurídico-penales que podrían considerarse para delimitar la posible participación de un tercero civil responsable o partícipe en una infracción cibernética, particularmente en el ámbito de la usurpación de identidad en línea. Estas razones se derivan de los objetivos y contenidos presentados en la investigación:

Conocimiento y Participación Delictiva: En el análisis de la figura del intermediario de Internet en el delito de suplantación de identidad, es esencial evaluar si el tercero tenía conocimiento de la conducta ilícita o si participó activamente en la planificación, ejecución o encubrimiento del delito. La determinación de su grado de participación podría establecer su responsabilidad como partícipe (Vereau, 2021).

Colaboración y Beneficio: En casos donde el tercero civil haya colaborado de manera activa o haya obtenido algún tipo de beneficio a raíz del delito informático, su relación con el delito debe ser evaluada. Si se demuestra que el tercero colaboró intencionalmente con el autor material o se benefició de la

suplantación de identidad, podrían considerarse fundamentos para su responsabilidad (Acosta et al., 2020).

Obligación de Diligencia: Los intermediarios de Internet pueden ser considerados penalmente responsables por no actuar con diligencia razonable al prestar sus servicios. Si se determina que el tercero tenía la capacidad y los recursos para prevenir o detener la comisión del delito, pero no tomó medidas adecuadas para hacerlo, esto podría ser un argumento para su imputación (Martínez & Porcelli, 2015).

Cooperación Internacional: Dado que la delincuencia informática es un fenómeno global, la cooperación internacional y el cumplimiento de tratados y convenciones relevantes también podrían influir en la delimitación de la responsabilidad del tercero civil. Si se demuestra que el tercero no cooperó en la investigación o extradición de los delincuentes, esto podría considerarse en su responsabilidad (UNODC, 2018).

Regulación Específica: La revisión de literatura destaca la importancia de una regulación específica para abordar los delitos informáticos y la responsabilidad de los intermediarios de Internet. Si se demuestra que el tercero estaba sujeto a una regulación específica que establece obligaciones en relación con la suplantación de identidad en línea y no las cumplió, esto podría considerarse como una base para su responsabilidad (Quevedo, 2017).

Medidas de Prevención y Sanción: Podrían influir en la delimitación de la responsabilidad del tercero. Si se demuestra que el tercero no implementó medidas adecuadas para prevenir o sancionar este delito, esto podría considerarse en su imputación (Aguilar, 2019).

La determinación de si un tercero civil puede ser considerado responsable o partícipe en un delito informático, como la suplantación de identidad en línea, dependerá de una evaluación exhaustiva de su conocimiento, participación, colaboración, beneficio, obligaciones legales, cooperación internacional y cumplimiento de regulaciones específicas.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. ZONA DE ESTUDIO

El espacio geográfico donde se encuentra el problema y se desarrollará la investigación será el Perú, en el contexto nacional.

3.2. TIPO DE ESTUDIO

Se señala que el enfoque es cualitativo y, a la luz de ello, se observa que los investigadores cualitativos registran narrativamente los fenómenos que estudian utilizando métodos como la observación participante y las entrevistas no estructuradas para descubrir las intrincadas relaciones, la estructura dinámica y la naturaleza profunda de las realidades, entre otros componentes (Hernández et al., 2014).

Estos diseños se distinguen por el hecho de que la investigación se centra en la experiencia del participante o participantes. De naturaleza fenomenológica, el diseño propuesto para el enfoque cualitativo busca conocer la esencia, estructura y significado de la pedagogía, la psicología y la sociología a través de la experiencia de un sujeto o grupo colectivo en relación con una situación, fenómeno o evento de la vida real (Fuster, 2019).

Además, debido a que esta investigación es especializada por su examen de los delitos informáticos, se utilizará este método para recopilar, ordenar y sintetizar los datos. Del mismo modo, se empleará el modelo sistemático, ya que seguirá un orden y una estructura, para lograr una mejor comprensión del contenido del trabajo porque será necesario conocer varios elementos que unificarán muchos aspectos aislados. También se aplicará la hermenéutica, necesaria para alcanzar una buena interpretación de la doctrina

nacional y comparada, con especial atención a los artículos de la Constitución Política del Perú (Van, 2014).

Comparativamente, el problema de investigación se examinará correlativamente en los ámbitos de la doctrina, la legislación y la jurisprudencia.

3.3. POBLACIÓN Y MUESTRA

La población: Representa la totalidad del fenómeno a estudiar, donde las entidades de la población tienen una particularidad común que se estudia y da lugar a los datos necesarios para el estudio, ya que es el conjunto total de casos que coinciden con determinadas características (Hernández et al., 2014). Como población se ha considerado a la Unidad Fiscal Provincial Corporativa Especializada en Delitos de Ciberdelincuencia de Lima que fue reconocida mediante la Resolución N° 843-2021-MP-FN emitida con fecha 08 de junio del 2021 y de manera exclusivo se avocada a estos delitos informáticos.

La Muestra: De acuerdo con ello, los sujetos a estudiar en este caso corresponden a abogados con conocimiento en delitos informáticos y Fiscales del Ministerio Público con competencia en los delitos informáticos, quienes puedan suministrar datos e información necesaria para demostrar el problema identificado. Por otra parte, la muestra representa a un subgrupo de la población, (Hernández et al., 2014). En este escenario, la muestra a los efectos del estudio cualitativo estará representada por cinco (5) abogados con conocimiento en delitos informáticos y tres (3) Fiscales de la Fiscalía Provincial Corporativa Especializada en Delitos de Ciberdelincuencia de Lima.

Tabla 1

Muestra de investigación

N°	Nombre y Apellido	Grado académico	Especialización	Años de experiencia profesional
1.	Luis	Maestro	Derecho Penal	10 años
2.	Deissy Ayala Cáceres	Doctor	Derecho Penal	10 años
3	Jesús Quispe	Maestro	Derecho Penal	10 años
4	Listo Cáceres	Maestro	Derecho Penal	10 años
5	Erika del Carmen Cecilia Matos Bernal	Doctor	Delitos informáticos	8 años
6	Luis Diego Arauco Ingunza	Maestro	Derecho Penal	10 años
7	Jorge Zúñiga Escalante	Maestro	Política jurisdiccional	20 años
8	Cristian Manuel Navarro Arévalo	Maestro	Derecho penal	21 años

Nota: Elaboración propia

Cabe destacar que se trata de expertos en el tema de delitos informáticos, lo que garantiza que los resultados obtenidos en las entrevistas sean de alta calidad y confiables. La importancia de esta exposición reside en su capacidad para ofrecer una visión de las posibles lagunas jurídicas que puede ser necesario colmar en el ordenamiento legislativo, además de compartir sus experiencias en casos relacionados con la ciberdelincuencia.

3.4. TÉCNICA DE RECOLECCIÓN DE DATOS

Para lograr los objetivos planteados, las técnicas de recolección de datos comprenden todos los procesos, métodos y procedimientos utilizados para obtener los datos de la investigación (Carrasco, 2017). La presente investigación empleará las siguientes metodologías para su desarrollo:

- Se realizará una entrevista a abogados con conocimiento en delitos informáticos y Fiscales del Ministerio Público con competencia en los delitos informáticos.

Así pues, el procedimiento de recogida de datos consta de los siguientes pasos:

I. Definición de los objetivos de la recogida de dato

II. Iniciar la obtención de información en despacho de abogados o bufetes, además de en Fiscalías del Ministerios Públicos que tienen experiencia en delitos informáticos.

III. Antes de administrar el cuestionario, se garantizará que los participantes comprendan el propósito de la entrevista, los objetivos del estudio y el procedimiento y las directrices para la recogida de datos y el manejo de los instrumentos.

IV. Si es el caso, se utilizarán herramientas tecnológicas (como correo electrónico, chat, videos y otros) para mejorar el proceso de entrevista con el sujeto en caso de que la entrevista cara a cara resulte difícil por limitaciones de traducción.

V. Se realizará la entrevista respetiva.

Para este estudio, se ha ideado una entrevista no estructurada para facilitar la recopilación de datos exhaustivos, ya que se espera que el entrevistado divulgue verbalmente información relativa a un tema o acontecimiento concreto de su vida. Además, este modelo es versátil, lo que permite adaptar el evento a los requisitos de la investigación y a los atributos de los sujetos. En cuanto al instrumento de investigación, aquel que permite registrar datos verificables que representen genuinamente las características de las variables o unidades de análisis seleccionadas según Hernández et al. (2014) son las guías de entrevista, los cuestionarios, el análisis de contenido, la observación y las pruebas estandarizadas.

En cuanto a la metodología, en general se aplica la observación participante (Schettini & Cortazzo, 2016), a excepción de las entrevistas no presenciales. Para garantizar la exactitud y fiabilidad de los datos, en la medida de lo posible, las entrevistas se duplicarán y el audio o el vídeo se grabarán utilizando cualquier programa tecnológico

pertinente. Mediante el uso de un conjunto de preguntas abiertas basadas en enfoques globales y orientadas a tipos generales de clase y opinión, se pedirá al entrevistado que construya significados relacionados con el tema de estudio (Hernández et al., 2014). El entrevistado puede formular su respuesta ya que las preguntas son abiertas y el orden no está predeterminado.

Para llegar a la interpretación a través de la codificación y la categorización, comenzaremos con la descripción a efectos de la técnica de procesamiento y análisis de datos. Es decir, identificaremos, organizaremos, refinaremos, relacionaremos e integraremos las categorías extraídas de la entrevista para, finalmente, producir los resultados y conclusiones.

En el análisis de los resultados se utilizará la hermenéutica para interpretar las perspectivas de los encuestados y discernir la veracidad de cada respuesta. Además, empleando la técnica de la triangulación, seremos capaces de generar un cuadro comparativo que englobe cada respuesta y permita su examen y yuxtaposición con los avances teóricos de investigaciones alternativas.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Resulta importante observar lo relacionado a las entrevistas realizadas a las personas seleccionadas. Resaltando que tres son abogados y docentes universitarios, uno asistente legal y otro defensor público. Se comenzará a plasmar el instrumento y las respuestas dadas por los entrevistados.

Para determinar si los resultados apoyan la teoría y si fomentan el debate con las posturas establecidas, se presentan los resultados de las entrevistas y se conectan con la teoría esbozada en el marco teórico. La aplicación del instrumento se interpreta de acuerdo con la pregunta de investigación y los objetivos formulados. Cada entrevista se describe minuciosamente de acuerdo con la muestra propuesta, además del correspondiente análisis documental. Se utilizaron ocho entrevistas a expertos para seleccionar la muestra del estudio, y los objetivos sugeridos sirvieron de base para la interpretación general de los resultados que se expone a continuación.

En primer lugar, se van a trabajar con el objetivo general, que se ha planteado indagar sobre el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad en Perú, 2020.

Tabla 2

Resultados del objetivo general

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Ayala**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
1.¿Cuál es el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad?	Considero que el rol de los intermediarios en lucha contra el delito de suplantación es la de implementar medidas de seguridad extremas para no vulnerar la información de identidad de las personas.	En el entendido que los intermediarios de Internet son todos los agentes que facilitan o realizan las transacciones para terceras partes en Internet, el rol que deberían realizar es el de brindar información que permita identificar el lugar de las transacciones, entre otros datos que coadyuve en la investigación.	El rol de los intermediarios de Internet resulta de suma importancia en la lucha de los delitos de suplantación de identidad ya que estos serán los proveedores (entidades) que posibilitan el acceso a Internet, así como a las páginas web y redes sociales y son los que finalmente tienen el control de la producción de información y publicación de contenido y su permanencia, siendo entonces los encargados de brindar dicha información para su identificación.	Brindar protección digital utilizando verificadores con entidades de registro civil – Reniec, por ejemplo.	El rol que cumplen estas entidades en la lucha contra el delito de suplantación de identidad no es el más idóneo ya que muchas veces no cuentan los aplicativos y software para realizar el control de identidad como se debe.	toda entidad que brinda un servicio debe siempre tener en cuenta la observancia de criterios a implementar para que el entorno del servicio que ofrece sea seguro.	Siendo prestadores del servicio de Internet, su rol es el de otorgar dichos servicios únicamente a personas naturales y/o jurídicas debidamente identificadas, con sistema de control biométrico que permitan tener trazabilidad de cada conexión a través de sus respectivos códigos IP.	El rol que juegan estos intermediarios, en mi opinión es determinante, porque estos sitios antes de aceptar la identidad de un usuario deben de corroborar la misma a través de mecanismos rigurosos y de control. De igual manera, debe de proteger los datos que suministran los usuarios, a fin de que no se vulneren estas bases de datos y se utilicen para suplantar identidades.

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Ayala**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
2.¿De qué manera la responsabilidad penal de los intermediarios de Internet puede fortalecer el control y la detención que ejerce el Estado peruano sobre los sujetos que cometen el delito de suplantación de identidad? ¿Cómo se puede fijar esta responsabilidad?	El estado debería individualizar a los intermediarios, sean personas naturales y/o jurídicas a través de un registro y sancionar a los representantes por no implementar medidas de seguridad adecuadas.	El legislador en nuestro país establece responsabilidad penal respecto a quien realiza o coadyuva dolosamente la comisión del ilícito, supuestos que no son comprendidos en la labor de los intermediarios de Internet, cuyo aporte puede ser calificado "de neutral".	Determinar su responsabilidad penal resulta necesaria para fortalecer el control y la detección del Estado en la lucha contra la ciberdelincuencia, tanto en la investigación del crimen como en su labor de prevención; debiéndose fijar esta como se ha realizado en diversos ámbitos que se requiere mayor especialización en las acciones realizadas que se devienen en actividades de riesgo y que ameritan una supervisión y control adecuada, como en la lucha contra Lavado de Activos, Medio Ambiente entre otros, esto es, a través de los agentes u oficiales de cumplimiento (criminal compliance en el sector empresarial) respecto a los servicios de Internet que se ofrecen, pudiéndose fijar su responsabilidad como una modalidad omisiva dentro de los delitos informáticos como la omisión de operaciones sospechosas, replicando la figura penal propuesta en la Ley de Lavado de Activos.	Brindando acceso a su base de datos y de navegación. La responsabilidad debe ser monetaria.	Puede fortalecer en la medida en que exista una buena política de estado en cuanto a los delitos informáticos en la modalidad de suplantación de identidad. Por ejemplo, que, si los intermediarios de Internet no cumpliesen con los protocolos de seguridad o estos sean ineficientes, la sanción que podría ser una fuerte multa (3URP), si es primera vez, pero si son residentes el doble de la multa (3URP), y que esta sanción alcance a las personas naturales como el director o gerente.	la penalización de todas las conductas no siempre es la solución de control social, más aún cuando debe valorarse la real dimensión de las acciones, a un intermediario ser un proveedor, no siempre debe guardar una responsabilidad penal, o una responsabilidad real de todo lo que pasa en sus dominios virtuales, ya que muchas veces es solo la entrada a aun red global, por lo que lo que puede hacerse es un control de los parámetros de seguridad mínimos que como intermediario debe exigir a sus usuarios.	En la medida que se puede mantener una trazabilidad entre los titulares del servicio, y los servicios a los que estos acceden, se puede identificar las personas que pudieran cometer el delito de suplantación y con ello fijar la responsabilidad penal o civil según sea el caso.	Estos intermediarios son susceptibles de tener una responsabilidad civil, va a depender de cada caso en concreto, sin embargo, al ser beneficiados de manera económica cuando brindan estos servicios, del mismo modo deben asumir la responsabilidad en el pago de las reparaciones a las personas que se vean afectados por la vulnerabilidad de sus plataformas.
3.¿De qué manera puede ser viable que los intermediarios de Internet respondan civilmente por cualquier daño que se genere con el uso de su servicio?	Implementando una base normativa que permita identificar a los intermediarios y aplicar una sanción razonable por permitir la vulneración de derechos de las personas.	Es viable que los intermediarios de Internet respondan civilmente, en tanto se incurra en las causales establecidas en el código civil.	Como consecuencia de los deberes y obligaciones que se deben fijar al momento de suscribir los respectivos contratos que posibilitan el proveer el servicio, se podría establecer una cláusula penal de responsabilidad en cuando a sus deberes de omisión de cumplimiento; por otro lado, de no darse este supuesto pero sí la incorporación de un tipo penal de omisión a las labores de comunicación, debería sustentarse la posibilidad de atribuir un supuesto de responsabilidad civil extracontractual conforme a las normas establecidas en el Código Civil y la teoría del daño, en mérito a la lesión del bien jurídico protegido.	Determinando que no cumplan con los requisitos mínimos de seguridad cibernética.	Como ya se indicó en la 3 pregunta una multa cuando es por primera vez y si son residentes el doble y también con una sanción penal siempre y cuando se demuestre la complicidad o la omisión por cumplir implementar estos protocolos en el momento establecido por ley.	en el mismo sentido que la respuesta anterior, solo se puede exigir algún tipo de resarcimiento a quienes manifiestamente como intermediarios no hayan contado con los mínimos sistemas de seguridad o en concreto que teniendo dichos sistemas pasaron por alto a determinados usuarios.	No puede trasladarse dicha responsabilidad, salvo que legalmente se estuviera ello en razón a controles deficientes en la identificación de quienes adquieren los servicios.	La viabilidad se encuentra determinada en el Código Procesal Penal, luego de formalizada la investigación preparatoria, debe de solicitar que se incorpore a estos intermediarios como terceros civilmente responsables, cuando corresponda, para lo cual se debe de analizar cada caso.

Nota: Elaborado por la investigadora

Análisis interpretativo

De los participantes entrevistados, en virtud de la primera pregunta respecto a cuál es el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad. Los participantes (1), (4), (6) y (8) consideran que el rol de los intermediarios es brindar protección digital implementando medidas de seguridad extremas para no vulnerar la información de identidad de las personas. Asimismo, verificadores con entidades de registro civil – RENIEC, por ejemplo. Los participantes (2) y (3) coinciden en que el rol de los intermediarios es brindar la información que permita identificar el lugar de las transacciones, entre otros datos que coadyuve en la investigación. El participante (5) refiere que el rol de los intermediarios no es el más idóneo, ya que muchas veces no cuentan con los aplicativos y software para realizar el control de identidad como se debe. En tanto que el participante (7) señala que el rol de los intermediarios de Internet es de otorgar dichos servicios únicamente a personas naturales y/o jurídicas debidamente identificadas, con sistema de control biométrico que permitan tener trazabilidad de cada conexión a través de sus respectivos códigos IP.

De los participantes entrevistados, en virtud de la segunda pregunta respecto a de qué manera la responsabilidad penal de los intermediarios de Internet puede fortalecer el control y la detención que ejerce el Estado peruano sobre los sujetos que cometen el delito de suplantación de identidad y cómo se puede fijar esta responsabilidad. Los participantes (1) y (3) coinciden en que la responsabilidad penal resulta necesaria para los representantes por no implementar medidas de seguridad adecuadas, respecto a los servicios de Internet que se ofrecen, pudiéndose fijar su responsabilidad como una modalidad omisiva dentro de los delitos informáticos como la omisión de operaciones sospechosas. Los participantes (2) y (6) coinciden en que un proveedor, no siempre debe guardar una responsabilidad penal, o una responsabilidad real de todo lo que pasa en sus

dominios virtuales, ya que la Ley establece responsabilidad penal respecto a quien realiza o coadyuva dolosamente la comisión de la labor de los intermediarios de Internet, cuyo aporte puede ser calificado “de neutral”. En cuanto a los participantes (4), (5) y (8) coinciden en que la responsabilidad debería ser civil y monetaria, dependiendo de cada caso en concreto, debiendo brindar acceso a las bases de datos. Para el participante (7) la responsabilidad debería ser penal o civil según sea el caso.

De los participantes entrevistados, en virtud de la tercera pregunta respecto a de qué manera puede ser viable que los intermediarios de Internet respondan civilmente por cualquier daño que se genere con el uso de su servicio. Los participantes (1), (2), (5) y (8) coinciden en que se debe aplicar una sanción razonable por permitir la vulneración de derechos de las personas. El participante (3) señala que se podría establecer una cláusula penal de responsabilidad en cuando a sus deberes de omisión de cumplimiento; por otro lado, de no darse este supuesto, pero sí la incorporación de un tipo penal de omisión a las labores de comunicación debería sustentarse la posibilidad de atribuir un supuesto de responsabilidad civil extracontractual conforme a las normas establecidas en el Código Civil y la teoría del daño, en mérito a la lesión del bien jurídico protegido. En tanto que los participantes (4) y (6) coinciden en que se puede exigir algún tipo de resarcimiento a quienes manifiestamente como intermediarios no hayan contado con los mínimos sistemas de seguridad o en concreto que teniendo dichos sistemas pasaron por alto a determinados usuarios. El participante (7) indica que No puede trasladarse dicha responsabilidad, salvo que legalmente se estuviera ello en razón a controles deficientes en la identificación de quienes adquieren los servicios.

Al preguntar sobre el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad, se obtuvo que se debe verificar la identidad de las personas con todos los recursos que tengan a su disposición. Aun así, se debe mencionar

que hay opiniones encontradas sobre la responsabilidad penal de los intermediarios, en el sentido que algunos señalan que sí deben tener responsabilidad para poder garantizar que exijan y verifiquen la identidad de las personas, y otros señalan que se debe regular una responsabilidad mínima para incentivar a que la identidad sea exigida en todo momento.

Entre tanto, se reconoce que los intermediarios pueden ser civilmente responsables para efectos de garantizar la seguridad en los entornos cibernéticos. Siendo importante mencionar que existe legislación en Perú que regula diversos aspectos de la utilización del Internet y lo relacionado al control de contenidos, esta legislación es la Ley Nº 28119 que tiene la prohibición y la regulación para que los menores de edad no accedan a páginas de adultos, aquí se toma en consideración a los intermediarios como parte esencial para garantizar la seguridad.

Es importante mencionar también que, aunque en Perú se esté planteando en discusiones recientes Proyectos de Ley N° 3156/2018-CR, 3607/2018-CR, 5600/2020-CR y 5843/2020-CR el hecho que el Internet sea de libre acceso y se plantee como un derecho, no excluye a que el Internet y los intermediarios en términos generales deben seguir garantizando la seguridad y transparencia en el acceso.

De igual manera se debe destacar que hay otras leyes que regulan actividades como el Spam (Ley N° 28493), tributos (RS N.º 333-2010/SUNAT) en las que se observa que los intermediarios tienen un papel fundamental para prestar los servicios, pero también para garantizarlos.

Por ello, se ha planteado como primer objetivo de investigación efectuar un análisis si el establecimiento de la responsabilidad penal de los intermediarios de Internet contribuye a fortalecer la actuación del Estado peruano frente al delito de suplantación de identidad.

Tabla 3

Resultado del objetivo específico 1

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Milagros Ayala Cáceres**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
4. ¿De qué manera se puede obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos en el Perú?	Aplicando sanciones exorbitantes una vez identificado al intermediario, por ello es importante el registro y la creación de un organismo encargado exclusivamente de estos.	A través de normativa que imponga, regule y sancione la adopción de debida diligencia.	Criminalizando las conductas omisivas dolosas que deberían tener los intermediarios de Internet, respecto al registro y detección de actividades sospechosas, así como en agenciarse de los medios adecuados para posibilitar dichas labores, que coadyuvaría también en la investigación e identificación de las organizaciones criminales especializadas en delitos informáticos.	Estableciendo multas altas y/o penas de inhabilitación a los dueños directos	A través de incentivos, reconocimientos y asensos en el trabajo que motiven a los intermediarios de Internet a cumplir eficientemente su labor de monitoreo y vigilancia en la lucha contra los delitos informáticos en el Perú.	En un sistema como el Internet donde existen muchas "puertas" tanto de entrada como de salida, resulta muy complicado realizar un monitoreo efectivo, lo que si puede reforzarse es la forma de control de las personas que son usuarias de ciertas paginas donde existe un mayor riesgo de alguna afectación.	No resulta posible establecer un control de contenidos en la medida que ello afectaría el derecho de acceso a la información, así como a la libertad de quienes deciden acceder a información contenida en Internet.	En Perú, aun no existe una Entidad que regule y supervise las plataformas virtuales, no obstante, el Ministerio de Justicia tiene una unidad orgánica dedicada a la protección de los datos sensibles de los ciudadanos.
5. ¿De qué manera el control de los contenidos y usuarios por parte de los intermediarios de Internet puede resultar legalmente factible? ¿Cuáles derechos podrían vulnerarse?	Implementando capas de seguridad y control biométrico. Los derechos que podrían vulnerarse podrían ser el derecho a la privacidad, identidad e información.	Considero que el asunto no pasa por realizar un control de contenido (que se puede involucrar la afectación de derecho fundamentales) sino por la implementación de medidas que permiten garantizar la identidad del usuario al servicio de Internet.	Como zona de la sociedad que se visualiza como riesgosa, es factible se tomen las medidas adecuadas para su control en cuanto a los contenidos y usuarios, no obstante, por ello es necesario esta se realice únicamente por sujetos especializados y autorizados, quienes a su vez pueden ser controlados respecto a las actuaciones que realizan, a efectos de evitar el tráfico de dicha información y la trasgresión de los derechos comprometidos en esos aspectos, como es el derecho al secreto de las comunicaciones y el derecho a la intimidad.	Solo la verificación con el cotejo con sistemas de Identificación Civil. Ya que el establecer restricciones mayores o solicitar una mayor cantidad de datos no garantiza la seguridad, inclusive pone más en riesgo al usuario	Va a ser factible siempre y cuando no traspasen ni contravengan el derecho a la reserva de la información, el proteger los datos e información de los usuarios. Si no se cumpliesen estos derechos se vulneraria el derecho a la privacidad de información, de datos bancarios, etc.	Como se sabe ningún derecho es absoluto así que siempre debe justificarse de ser el caso de realizar algún tipo de vulneración, ahora la real dimensión de qué tipo de contenido quiere aislarse y protegerse y si este realmente en una ponderación tiene el valor suficiente para vulnerar el derecho a la libertad de expresión.	Conforme a lo señalado precedentemente afectaría el derecho de acceso a la información, así como a la libertad de quienes deciden acceder a información contenida en Internet.	Complementando la respuesta anterior, considero que, es a través de estas entidades que se debe de promover la legislación o la creación de otras normas que obliguen a establecer un procedimiento riguroso de control a estas plataformas virtuales, a fin de proteger el Derecho a la Identidad y a la Intimidad que debe de gozar todo ciudadano.

Nota: Elaborado por la investigadora

Análisis interpretativo

De los participantes entrevistados, en virtud de la cuarta pregunta respecto a de qué manera se puede obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos en el Perú. Los participantes (1), (2), (3,) y (4) coinciden en que se debe aplicar sanciones con sumas exorbitantes, a través de normativa que imponga, regule y sancione la adopción de debida diligencia, por ello es importante el registro y la creación de un organismo regulador. De modo positivo el participante (5) señala que se deben otorgar incentivos, reconocimientos y asensos en el trabajo que motiven a los intermediarios de Internet a cumplir eficientemente su labor de monitoreo y vigilancia en la lucha contra los delitos informáticos en el Perú. Los participantes (6) y (7) coinciden que resulta complicado realizar un monitoreo efectivo. En tanto que el participante (8) señala que, en Perú, aun no existe una Entidad que regule y supervise las plataformas virtuales, no obstante, el Ministerio de Justicia tiene una unidad orgánica dedicada a la protección de los datos sensibles de los ciudadanos.

De los participantes entrevistados, en virtud de la quinta pregunta respecto a de qué manera el control de los contenidos y usuarios por parte de los intermediarios de Internet puede resultar legalmente factible y cuáles derechos podrían vulnerarse. Todos los participantes coinciden en que será factible siempre y cuando no traspasen ni contravengan el derecho a la reserva de la información, el proteger los datos e información de los usuarios. Si no se cumpliesen estos derechos se vulneraria el derecho a la privacidad de información.

En cuanto a la manera se puede obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos, todos los entrevistados están de acuerdo en el

hecho que efectivamente no se puede, y en Perú no existe una forma de regular la responsabilidad. Solo se debe trabajar desde el incentivo para garantizar que se verifique lo relacionado al monitoreo de la identidad de las personas. Se observaron también respuestas diversas sobre la factibilidad legal del control de contenidos, en el sentido que existen derechos de carácter constitucional como la información y la libertad de expresión, por lo que, la capacidad de los intermediarios de limitar información puede ser poco factible sino se encuentra respaldada por una legislación que no violente derechos constitucionales, sino que propicie su respeto.

Resulta importante mencionar también que en la sentencia peruana ha quedado por sentado lo relacionado a las obligaciones, en el sentido que se debe ofrecer una protección al consumidor, tal es la situación del caso de Mercado Libre en una disputa por una venta realizada en su plataforma. La sentencia Resolución Final N.º 2419-2015/CC2 señala entre otras cosas que la obligación del intermediario es realmente estar presente y satisfacer las necesidades de ambas partes, por ello se debe dar seguridad, en el caso de mercado libre, que su plataforma de pago si es segura y ante cualquier disputa se harán responsable y es lo que afirma la sentencia, mercado libre como intermediario en las ventas por medio de Inter8net, tiene responsabilidad por no desarrollar un sistema totalmente seguro.

A continuación, se procede a realizar el objetivo específico 2 que se encuentra enfocado en constatar si el obligar a los intermediarios de Internet a monitorear y vigilar exhaustivamente a los usuarios de sus plataformas y sus contenidos, evita el cometimiento de los delitos de usurpación de identidad en el Perú.

Tabla 4

Resultado del objetivo específico 2

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Ayala**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
6. En su opinión, ¿cuál medida legal pudiera dictarse para limitar los actos que originan el delito de suplantación de identidad, especialmente cuando se involucran los servicios de Internet?	Aplicación de sanciones para intermediarios y usuarios que realicen dichos actos, tales como sanción pecuniaria y algunos años de cárcel.	La adopción de un protocolo de debida diligencia que permita garantizar que el titular que figura como usuario al servicio de Internet en efecto sea la persona con cuyos datos se identifica.	Resulta importante para estos efectos que se regulen las actividades que realizan los proveedores del servicio de Internet, páginas web y acceso a redes sociales, únicamente con la finalidad de requerirse mayores controles de identificación de sus diversos usuarios, para evitar la facilidad con la que actualmente se viene suplantando diversas identidades a efectos de acceder a las líneas telefónicas, cuentas bancarias, redes sociales, entre otros.	La limitación de un usuario por documento de identificación	Establecer una pena de efectiva de 12 años de cárcel para quienes cometan estos delitos de suplantación de identidad con el agravante de la sustracción del patrimonio a 15 años de cárcel.	Las páginas o aplicativos dentro de sus políticas públicas deben realizar un control real en la validación de identidad de las personas que se registran en las mismas, o crean dominios virtuales.	No existe medida legal para controlar ningún delito, por lo que no es viable controlar la disminución de la ejecución del delito de suplantación de identidad, requiriéndose más bien políticas públicas de prevención de dicho delito con medidas de mejor difusión de información relevante y control sobre la información y accesos en las redes.	Como ya he mencionado, actualmente es el Ministerio de Justicia quien lidera o se encuentra en cautela de los datos sensibles de los ciudadanos, a través de ellos promover directivas que obliguen a un procedimiento obligatorio y riguroso para hacer confiable estas plataformas virtuales.
7. En su opinión, ¿legalmente cómo podrían bloquearse plataformas digitales para evitar la ejecución de algún delito de suplantación de identidad? ¿Quién debería asumir esa responsabilidad?	Podrían bloquearse monitoreando a estos intermediarios a través de una agencia estatal exclusiva que vigile a estos. El Estado debería asumir ese rol.	Es escasa si es que no es nula la normativa que regule la restricción de Internet y ello se debe a que el servicio de Internet no tiene fronteras como el ámbito geográfico en el que c/d país ejerce jurisdicción.	En los deberes de cumplimiento que se deben regular respecto a los propios agentes y a los proveedores del servicio, se debe establecer la obligación de estos de proceder, en la identificación y registro de actividades sospechosas, además de realizarse el reporte respectivo, al bloqueo temporal preventivo o permanente de las plataformas, por lo que resulta necesaria la exigencia de regulaciones legales internas para los propios servicios que ofrecen, en el cual el propio usuario debe ser consciente de dichas posibilidades en el caso de detención de las mismas .	Aviso por parte de la persona afectada con la verificación del documento de identidad, la responsabilidad de cotejar y atender la solicitud es la plataforma digital.	A través de la compra de software de última generación que se encarguen de bloquearse automáticamente cuando detecte que la persona no es la que se corrobora a través de una pantalla o cámara web para proceder con la transacción, etc. La responsabilidad la asumiría las entidades que empleen estos aparatos ya sea entidades públicas o privadas.	lamentablemente, solo existen como se ha visto recientemente que entidades como Indecopi piden a los proveedores de Internet que bloqueen ciertos dominios que pueden incurrir en algún tipo de falta ahora esta medida tendría que extrapolarse a más ámbitos previa resolución de la entidad competente, y asumiría la responsabilidad la entidad encargada de dicho proceso y dicha orden de restricción.	No es posible bloquear medidas digitales antes de cualquier delito, sino únicamente como consecuencia de haberse demostrado que esta forma parte o medio de la comisión de un delito, pudiendo disponerse ello mediante una pena accesoria como consecuencia del proceso penal instaurado.	Legalmente, sabemos que quien impone estas suspensiones o clausuras es un juez; el problema se fomenta con la canalización de la orden, por lo que considero que debe de existir una autoridad que pueda regular y controlar a los operadores del Internet, a fin de poder ejecutar de manera directa los bloqueos a estas plataformas virtuales, sin embargo, esto implica un desarrollo mayor y coordinado con los proveedores de Internet que son extranjeros.

Nota: Elaborado por la investigadora

Análisis interpretativo

De los participantes entrevistados, en virtud de la sexta pregunta respecto a cuál medida legal pudiera dictarse para limitar los actos que originan el delito de suplantación de identidad, especialmente cuando se involucran los servicios de Internet. Los participantes (1) y (5) señalan que debe aplicarse sanciones para intermediarios y usuarios que realicen actos delitos de suplantación de identidad con el agravante de la sustracción del patrimonio, tales como sanción pecuniaria y algunos años de cárcel. El resto de los participantes tales como (2), (3), (4), (6), (7) y (8) coinciden en que resulta importante para estos efectos que se regulen las actividades que realizan los proveedores del servicio de Internet, páginas web y acceso a redes sociales, únicamente con la finalidad de requerirse. promoviendo directivas que obliguen a un procedimiento obligatorio y riguroso para hacer confiable estas plataformas virtuales.

De los participantes entrevistados en virtud de la séptima pregunta respecto a legalmente cómo podrían bloquearse plataformas digitales para evitar la ejecución de algún delito de suplantación de identidad y quién debería asumir esa responsabilidad. Los participantes (1), (3), (4), (5) y (6) coinciden en que deben existir mecanismos que sirvan para bloquear automáticamente cuando detecte que la persona no es la que se corrobora a través de una pantalla o cámara web para proceder con la transacción. De forma dividida señalan que la responsabilidad debe ser asumida por las entidades que empleen esos aparatos ya sean entidades públicas o privadas. Los participantes (2), (7) y (8) opinan que no es posible bloquear medidas digitales antes de cualquier delito, o es escasa si es que no es nula la normativa que regule la restricción de Internet y ello se debe a que el servicio no tiene fronteras como el ámbito geográfico en el que cada país ejerce jurisdicción, por tanto, debe de existir una autoridad que pueda regular y controlar a los operadores del Internet.

Respeto a la aplicación de medidas legales para limitar los actos que originan la suplantación de identidad, se observó que no hay una limitación para verificar en sí o

castigar lo relacionado a la suplantación de identidad, algunos están de acuerdo con penas de prisión, pero en el derecho peruano esto no ha sido tratado.

En base a lo señalado anteriormente, también resulta complicado establecer quien debe asumir la responsabilidad al bloquear plataformas digitales para evitar la ejecución de algún delito de suplantación de identidad. Se reseña que ya se ha dado la situación de bloqueo en determinadas situaciones, ante petición de un juez o un organismo competente, pero no son soluciones generalizadas.

La suplantación de identidad se consagra como un ilícito en la Ley Nº 30096 o Ley de delitos informáticos. Se señala entre otras cosas que la suplantación de identidad puede ser evitada si los intermediarios exigieran más rigurosidad al momento que las personas se registran en las diversas plataformas. Un punto que se debe observar es lo relacionado a la protección de los datos, en el que, si no se protegen los datos, se puede dar lo relacionado a la suplantación de identidad, la sentencia del año 2002 identificada como EXP. N° 0905-2001-AA/TC sostiene que siempre las empresas intermediarias en materia de Internet deben verificar la identidad de los clientes para evitar que se cometan daños a la imagen y a la identidad de las personas, para ello deben implementar los mecanismos que se encuentren presentes y a la vanguardia. Por lo que, la verificación de la identidad es primordial para prestar de manera eficiente los servicios de Internet.

En cuanto al tercer objetivo de investigación se ha planteado evaluar la necesidad de propiciar una ley sobre la delimitación de la responsabilidad de los proveedores de servicios de Internet para disminuir delitos informáticos en el Perú.

Tabla 5

Resultado del objetivo específico 3

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Ayala**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
8. En su opinión, ¿cómo la legislación podría determinar las modalidades de engaño para el cometimiento de los delitos suplantación de identidad?	Identificando las que comúnmente se realizan y prescribiendo estos expresamente en la normativa legal, considerando además esta númerus apertus.	No se puede pretender que la ley penal describa cada o todo tipo de supuesto fáctico típico que constituirá el delito de suplantación de identidad aunado a que nuestra legislación no establece como elemento típico el engaño	Resulta importante no solo limitar el ámbito de imputación en la falsedad informática, a la suplantación de identidad, sino también ubicar dentro de estos mismos delitos, la utilización de documentos digitales o datos fraudulentos, pues es común también dicha modalidad para posibilitar el engaño en las posibles víctimas, lo que resultaría un tipo penal pluriofensivo y necesaria regulación, sea de forma independiente, o como una modalidad agravada, respecto a la utilización de documentos digitales falsas, realizado en actos de suplantación de identidad.	Establecer si fue realizado por una persona o más de 2 personas, especialización de los equipos y grado de afectación	En sí, las modalidades podrían ser a través de páginas webs, apps, correos, etc.	en mi opinión la legislación ya contempla las formas ahora lo que debe hacerse es desarrollar los criterios y alcances de la determinación de cual conducta es permitida y cual no, cual está dentro de esa esfera de protección y cual no.	Atendiendo a que no existe medida legal para controlar ningún delito, legislativamente no sería posible determinar las modalidades de engaño para la comisión del delito bajo análisis.	De la revisión del Código Penal tenemos que en el numeral 5 del artículo 196°A ha previsto como una de las modalidades de la estafa agravada, cuando por cualquier medio se suplanta la identidad de otra persona, siendo que, el tipo se limita a cuando es para acceder a cuentas bancarias, tarjetas o similares, no existiendo tipos penales más específicos para casos de suplantación de identidad con fines de acoso cibernético, por ejemplo.
9. En su opinión, ¿de qué manera los daños virtuales que se producen con el delito de suplantación de identidad pueden valorarse en caso de declararse alguna responsabilidad civil?	En principio, sería una sanción pecuniaria ejemplar como se realiza en el sistema common law y si fuera el caso dependiendo la gravedad, aplicarse penas privativas de la libertad.	Desconozco la definición de daños virtuales, por lo que no puedo responder a la interrogante formulada.	La pretensión resarcitoria es una acumulada a la punitiva, dentro del mismo proceso Penal, empero, se rige por sus propias reglas, conforme a lo establecido en el Código Penal, en su artículo 92° y siguientes y lo establecido para su determinación en el Código Civil. En ese sentido, es la teoría del daño que determinaría los daños patrimoniales y extrapatrimoniales que deberán ser objeto de acreditación. Por lo que, no se encontraría mayor problema en acreditar, dentro del daño moral, los daños virtuales que se producen con la suplantación de identidad, lo cual debe ser cuantificable, de manera motivada, en cada caso en concreto, por el Juez al momento de emitir sentencia.	Con el grado de afectación que produzca a la víctima respecto a su dignidad, economía y otros.	No respondió	estos daños tendrán que calificarse y valorarse de acuerdo con el real prejuicio, con los criterios ya establecidos luego de establecer la real existencia de un daño real. Y en base los criterios ya establecidos para resarcir el daño estos pueden ser invocados y ejecutados.	Para dicho efecto previamente debería determinarse que se entiende por "daños virtuales", según lo cual debería catalogarse bajo los conceptos de la responsabilidad civil (lucro cesante, daño moral o daño emergente)	Debemos tener en cuenta que, lo que se busca proteger son el Derecho a la identidad y el de la intimidad de un ciudadano, por lo cual, el daño es contra esos bienes jurídicos, sin embargo, actualmente no existe una tabla o criterio objetivo para definir una situación tan subjetiva, como lo es el daño moral o llamado extra patrimonial. Cabe precisar que, en los casos mediante la cual la suplantación se realizó para apropiarse de dinero de cuentas o realizar compras con tarjetas de otra persona si se puede identificar un daño concreto.

Preguntas	Participantes							
	Fiscal (1) Luis	**Fiscal (2) Deissy Ayala**	**Fiscal (3) Jesús Quispe**	**Abogado (4) Listo Cáceres**	**Abogado (5) Erika**	**Abogado (6) Dr. Arauco Ingunza**	**Abogado (7) Jorge Zúñiga**	**Abogado (8) Christian Navarro**
10. ¿Quiénes podrían ser los responsables de los daños cometidos por usuarios en caso de los delitos de suplantación de identidad?	Los intermediarios deberían ser solidariamente responsables del daño y la indemnización correspondiente.	La pregunta es algo ambigua, quien debe responder por los daños que ocasione su conducta, evidentemente debe responder el sujeto que los ha ocasionado.	Conforme a las reglas para determinar la responsabilidad civil; lo será el mismo autor y/o participe del delito, quien ha vulnerado el bien jurídico, y de ser el caso, también podría establecerse una responsabilidad civil por parte de un tercero, como el proveedor de servicio o administrador de la web, si se puede establecer también su responsabilidad solidaria en su comisión, en virtud de una infracción a sus propios deberes.	solidariamente la plataforma porque no establece mecanismos de seguridad y directamente los suplantadores	En este caso, los responsables serían las personas naturales que a través de una computadora cometen estos delitos valiéndose de estos aparatos tecnológicos para realizar el hecho punible y la sustracción del patrimonio.	lo directos responsables son los causantes del daño, es decir que quienes con sus acciones realizaron el prejuicio directo de la persona afectada.	No es posible determinar ello a priori, sino que ello tendría que determinarse caso por caso, y luego del proceso penal respectivo que permita determinarlo.	Para el Derecho Penal, el responsable es quien comete el hecho, y quien dolosamente presta auxilio para que se cometa un hecho delictivo, muy aparte tenemos la responsabilidad civil, que tiene que ver con quienes deberían de reparar el daño causado por un hecho delictivo, donde no solo es responsable quien comete el hecho, sino aquel tercero que pudo haber mejorado sus niveles de control, pero que, sin embargo, al ser vulnerable su plataforma virtual permite que el delito se cometa.

Nota: Elaborado por la investigadora

Análisis interpretativo

De los participantes entrevistados, en virtud de la octava pregunta respecto a cómo la legislación podría determinar las modalidades de engaño para el cometimiento de los delitos suplantación de identidad. Los participantes (1), (3), (4), (5), (6) y (8) coinciden en que se debe identificar los delitos comúnmente realizados no solo limitar el ámbito de imputación en la falsedad informática, a la suplantación de identidad, sino también ubicar dentro de estos mismos delitos, la utilización de documentos digitales o datos fraudulentos, pues es común también dicha modalidad para posibilitar el engaño en las posibles víctimas, lo que resultaría un tipo penal pluriofensivo y necesaria regulación, sea de forma independiente, o como una modalidad agravada, respecto a la utilización de documentos digitales falsas, realizado en actos de suplantación de identidad. Los participantes (2) y (7) opinan que no existe medida legal para controlar ningún delito, legislativamente no sería posible determinar las modalidades de engaño para la comisión del delito bajo análisis. No se puede pretender que la ley penal describa cada o todo tipo de supuesto fáctico típico que constituirá el delito de suplantación de identidad aunado a que nuestra legislación no establece como elemento típico el engaño.

De los participantes entrevistados en virtud de la novena pregunta respecto a de qué manera los daños virtuales que se producen con el delito de suplantación de identidad pueden valorarse en caso de declararse alguna responsabilidad civil. Los participantes (1), (3), (4), (6), (7) y (8) coinciden en que, en principio, sería una sanción pecuniaria ejemplar y dependiendo de la gravedad, aplicarse penas privativas de la libertad. Es la teoría del daño que determinaría los daños patrimoniales y extrapatrimoniales que deberán ser objeto de acreditación. Por lo que, no se encontraría mayor problema en acreditar, dentro del daño moral, los daños virtuales que se producen con la suplantación de identidad, lo cual debe ser cuantificable. Estos daños tendrán que calificarse y valorarse de acuerdo

con el real prejuicio, con los criterios ya establecidos luego de establecer la real existencia de un daño real. Y en base los criterios ya establecidos para resarcir el daño estos pueden ser invocados y ejecutados. Los participantes (2) y (5) se abstuvieron de responder a la interrogante formulada.

De los participantes entrevistados en virtud de la décima pregunta respecto a quiénes podrían ser los responsables de los daños cometidos por usuarios en caso de los delitos de suplantación de identidad. El participante (1) opina que los intermediarios deberían ser solidariamente responsables del daño y la indemnización correspondiente. Los participantes (2), (3), (4), (5), (6) y (8) coinciden en que conforme a las reglas para determinar la responsabilidad civil; lo será el mismo autor y/o participe del delito, quien ha vulnerado el bien jurídico, y de ser el caso, también podría establecerse una responsabilidad civil por parte de un tercero, como el proveedor de servicio o administrador de la web, si se puede establecer también su responsabilidad solidaria en su comisión, en virtud de una infracción a sus propios deberes. El participante (7) opina que no es posible determinar ello a priori, sino que ello tendría que determinarse caso por caso, y luego del proceso penal respectivo que permita determinarlo

Se validan diversos parámetros legales en los que se deben establecer las formas de garantizar la identidad de las personas, de allí que el uso de ingeniería social se puede tratar como una estafa o delitos similares. Las respuestas van enfocadas a la dignidad de las personas, el derecho a la intimidad y el derecho a la identidad. Desde allí se podría valorar, sin menoscabo de los daños morales a los que haya lugar.

Entre tanto, en el caso de tener que determinar la responsabilidad de los daños cometidos en el caso de suplantación de identidad haciendo uso de la ingeniería social a través del Internet, se observa que se debe revisar cada caso en concreto, pero las personas que realizan la suplantación son las responsables directas de los hechos. En este aspecto

es importante mencionar que recientemente ha sido juzgada una mujer en Perú en la resolución 001466-2022-2-1826-JR-E-10, por crear perfiles falsos en Facebook y suplantar la identidad de otra persona. Esta persona fue sentenciada a tres años de prisión por el delito de suplantación de identidad, los medios para probar esta suplantación fueron otorgados por los intermediarios de Internet, estos fueron correos electrónicos, acta de comunicación de Facebook, acta fiscal de la cuenta de Facebook con código hash, entre otros. Se demuestra entonces, que, con las pruebas pertinentes, las personas mismas que cometen el acto son responsables, más allá de los intermediarios.

4.2. DISCUSIÓN

En virtud de lo anterior y conforme a lo analizado en el desarrollo de la presente investigación, se plantea la siguiente discusión:

4.2.1. Objetivo general: Indagar sobre el rol de los intermediarios de Internet en la lucha contra el delito de suplantación de identidad en Perú, 2020

Los entrevistados coincidieron en su mayoría en que el rol de los intermediarios es brindar protección digital implementando medidas de seguridad extremas para no vulnerar la información de identidad de las personas. Asimismo, agregaron los entrevistados que este rol conduce también a brindar la información que permita identificar, entre otros datos, el lugar de las transacciones, información que coadyuve en la investigación, además de otorgar dichos servicios únicamente a personas naturales y/o jurídicas debidamente identificadas, con sistema de control biométrico que permitan tener trazabilidad de cada conexión a través de sus respectivos códigos IP. Frente a ello, señaló uno de los participantes que el rol de los intermediarios no es el más idóneo, ya que muchas veces no

cuentan con los aplicativos y software para realizar el control de identidad como debería ser formalmente.

De ello se puede destacar la importancia de verificar la identidad de las personas con todos los recursos que tengan a su disposición. En todo caso, resulta fundamental determinar el rol de los intermediaros, tal como lo señaló Manila Principles (2015), coincidiendo con los entrevistados al indicar que este rol es fundamental y necesario, siendo un rol clave que facilita todas las comunicaciones para el acceso de usuarios a contenidos en Internet, tal como fue ratificado por la OEA (2013) al indicar que la transmisión de ideas e informaciones en Internet sería imposible sin estos actores, siendo su rol esencial para el ejercicio de distintos derechos para cualquier individuo como el de buscar y recibir información en línea o el de libertad de expresión.

De acuerdo con este rol, se concatena el estudio de Levy & Aguerre (2019), que enfatiza la necesidad de reconocer que ha aumentado la presión sobre la regulación de los intermediarios, particularmente los asociados a plataformas que manejan contenidos en internet. Esta presión se refiere a una mayor rendición de cuentas en las prácticas de bloqueo, filtrado y eliminación de contenidos, y más aún si tales prácticas violan la libertad de expresión, dado que su papel puede impactar significativamente en las disparidades.

La discusión se enfoca en el papel de los intermediarios de Internet en la lucha contra la suplantación de identidad en Perú y cómo esto puede afectar la privacidad y la libertad de expresión. Se mencionan dos perspectivas: la visión común de la criminología que apoya la seguridad digital a través de los intermediarios, y el "curanderismo criminológico", que critica la falta de

herramientas adecuadas. La privacidad es crucial, pero se plantea el equilibrio entre seguridad y libertades individuales. La implementación de medidas debe evitar excesos que restrinjan la libre expresión y la privacidad en línea.

Es evidente que actualmente se requiere una implementación más rigurosa de medidas de seguridad para proteger los derechos personales y sociales en el entorno digital. Estas medidas no solo resguardan la información, sino que también permiten la identificación de usuarios en casos de delitos informáticos, contribuyendo a investigaciones efectivas.

A pesar de su importancia, se nota que el rol del intermediario no siempre es eficaz debido a la falta de herramientas digitales adecuadas, como sistemas de control biométrico. Definir su función es esencial, ya que facilita el acceso a contenidos en Internet y promueve otros derechos como la libertad de expresión y el acceso a la información. Es esencial que se refuercen sus capacidades para asegurar la protección y privacidad en el entorno digital.

4.2.2. Objetivo específico 1: Analizar si el establecimiento de la responsabilidad penal de los intermediarios de Internet contribuye a fortalecer la actuación del Estado peruano frente al delito de suplantación de identidad

En principio, cabe señalar en función de la opinión de los **entrevistados** que la responsabilidad penal resulta necesaria para los representantes por no implementar medidas de seguridad adecuadas, respecto a los servicios de Internet que se ofrecen, pudiéndose fijar su responsabilidad como una modalidad omisiva dentro de los delitos informáticos como la omisión de operaciones sospechosas. No obstante, igualmente para determinados entrevistados un proveedor, no

siempre debe guardar una responsabilidad penal, o una responsabilidad real de todo lo que pasa en sus dominios virtuales, ya que la Ley establece responsabilidad penal respecto a quien realiza o coadyuva dolosamente la comisión de la labor de los intermediarios de Internet, cuyo aporte puede ser calificado de neutral.

En este contexto, se prevé la posibilidad de incorporar una cláusula penal de responsabilidad para los intermediarios en cuanto a los deberes de omisión de cumplimiento, o en su defecto por la omisión a las labores de comunicación. No obstante, debería sustentarse la posibilidad de atribuir un supuesto de responsabilidad civil extracontractual conforme a las normas establecidas en el Código Civil y la teoría del daño, en mérito a la lesión del bien jurídico protegido y contemplar el resarcimiento a quienes manifiestamente como intermediarios no hayan contado con los mínimos sistemas de seguridad o en concreto que teniendo dichos sistemas pasaron por alto a determinados usuarios. Frente a ello, resulta importante establecer controles eficientes en la identificación de quienes adquieren los servicios.

En ese sentido, se destaca la necesidad de determinar una responsabilidad civil, dependiendo de cada caso en concreto. En este ámbito civil, se estima que los intermediarios de Internet pueden responder civilmente por cualquier daño que se genere con el uso de su servicio, bajo una sanción razonable ante el hecho de permitir la vulneración de derechos de las personas.

Por otra parte, se estima que la responsabilidad penal de los intermediarios de Internet puede fortalecer el control y la detención que ejerce el Estado peruano sobre los sujetos que cometen el delito de suplantación de identidad, pero se destaca que debe ser necesaria una actualización de la norma, por cuanto -se

reitera- la ley establece responsabilidad penal respecto a quien realiza o coadyuva dolosamente la comisión de la labor de los intermediarios de Internet, cuyo aporte puede ser considerado neutral.

En este escenario se observa que existen posturas divergentes sobre la responsabilidad penal de los intermediarios, en el sentido que por una parte se plantea que debe existir la responsabilidad para poder garantizar que exijan y verifiquen la identidad de las personas, y por otra parte se plantea la posibilidad de regular una responsabilidad mínima para incentivar a que la identidad sea exigida en todo momento.

No obstante, un punto en que convergen las posturas es en que los intermediarios deben ser civilmente responsables para efectos de garantizar la seguridad en los entornos cibernéticos. Un punto importante es que la legislación peruana regula diversos aspectos de la utilización del Internet y lo relacionado al control de contenidos, mediante la Ley Nº 28119, como es el caso de la prohibición para los menores de acceder a determinadas páginas.

Por otra parte, un aspecto relevante es en cuanto a los daños virtuales que se producen con el delito de suplantación de identidad, planteándose la posibilidad de valorarse en caso de declararse alguna responsabilidad civil bajo el análisis de la teoría del daño que determinaría los daños patrimoniales y extrapatrimoniales que deberán ser objeto de acreditación. En tal caso, no se vislumbra un posible problema de acreditar, dentro del daño moral, los daños virtuales que se producen con la suplantación de identidad, lo cual debe ser cuantificable.

Al efecto, estos daños tendrán que calificarse y valorarse de acuerdo con el real prejuicio, con los criterios ya establecidos luego de establecer la real

existencia de un daño real. Y en base los criterios ya establecidos para resarcir el daño estos pueden ser invocados y ejecutados.

Por su parte, los intermediarios deberían ser solidariamente responsables del daño y la indemnización correspondiente, conforme a las reglas para determinar la responsabilidad civil. En el caso de tener que determinar la responsabilidad de los daños cometidos en el caso de suplantación de identidad haciendo uso de la ingeniería social a través del Internet, se debería revisar cada caso en concreto, teniendo en cuenta que las personas que realizan la suplantación son las responsables directas de los hechos.

Asimismo, los puntos de vista expresados por los entrevistados se alinean con los de Pardo (2018), quien sugiere que el marco jurídico penal relativo a los delitos informáticos contra la propiedad es inadecuado. Esta deficiencia se deriva de la no inclusión de todos los tipos y modalidades de delitos informáticos dentro de la definición de fraude informático. En consecuencia, esto crea ambigüedad en cuanto a la aplicación de la norma y obstaculiza la capacidad de imponer penas efectivas para tales delitos. Por lo tanto, se aconseja que se emprenda un esfuerzo legislativo para abordar explícitamente esta cuestión.

Desde el ámbito jurisprudencial se tiene la resolución 001466-2022-2-1826-JR-E-10, mediante la cual se juzgó a una ciudadana por crear perfiles falsos en Facebook y suplantar la identidad de otra persona, siendo sentenciada a tres años de prisión por el delito de suplantación de identidad, lo que demuestra a su vez que los usuarios que cometen el acto son responsables, más allá de los intermediarios, sin embargo, tal como se ha asomado puede exigirse una responsabilidad solidaria.

Se explora si las opiniones reflejan una visión tradicional de criminología o una perspectiva alternativa, llamada "curanderismo criminológico", que podría afectar la privacidad. Se aborda si imponer responsabilidad penal a intermediarios de Internet fortalecería la lucha contra la suplantación de identidad en Perú. Entrevistados difieren en si intermediarios deben ser penalmente responsables por falta de seguridad. Algunos apoyan esta responsabilidad para asegurar la seguridad, mientras otros dudan que deban ser penalmente responsables por todo. Se sugiere responsabilidad civil para fomentar seguridad digital.

Se considera que la responsabilidad penal de intermediarios podría reforzar control estatal sobre delincuentes de suplantación, pero se pide actualización legal para distinguir actos dolosos y neutrales. Se debate sobre si intermediarios deben ser responsables penal y civilmente para garantizar seguridad digital. Se menciona que leyes peruanas regulan Internet, pero se enfatiza en revisar casos para determinar responsabilidad en suplantación. Se resalta que autores de suplantación son responsables, aunque intermediarios estén involucrados. Resoluciones judiciales respaldan condenas a autores de estos delitos. En resumen, se discuten perspectivas sobre responsabilidad de intermediarios en suplantación. Se destaca equilibrio entre seguridad en línea, privacidad y derechos individuales, y se enfatiza en leyes actualizadas y análisis de casos.

En el Perú no existe una regulación específica para la responsabilidad penal de los intermediarios de Internet en casos de suplantación de identidad. Sin embargo, esta ausencia normativa no descarta la posibilidad de plantear tal responsabilidad, ya que es esencial para proteger a los usuarios y prevenir delitos.

La regulación penal actual contempla ciertos escenarios que podrían llevar a esta responsabilidad.

Además, se considera viable la imposición de una responsabilidad civil a los intermediarios, en línea con el Código Civil, para garantizar la compensación por daños y perjuicios a los usuarios afectados. En definitiva, establecer tanto responsabilidad penal como civil podría fortalecer la actuación estatal al incentivar a los intermediarios a implementar medidas de seguridad más rigurosas y contribuir al control del delito de suplantación de identidad en el entorno digital.

4.2.3. Objetivo específico 2: Constatar si el obligar a los intermediarios de Internet a monitorear y vigilar exhaustivamente a los usuarios de sus plataformas y sus contenidos, evita el cometimiento de los delitos de usurpación de identidad en el Perú

En cuanto al control de los contenidos y usuarios por parte de los intermediarios de Internet y su factibilidad legal, así como los derechos posiblemente vulnerados, se tiene que los entrevistados estiman que es factible dicho control mediante la norma siempre que no se traspasen ni contravengan derechos, como el derecho a la reserva de la información, el proteger los datos e información de los usuarios. Si no se cumpliesen estos derechos se vulneraria el derecho a la privacidad de información.

Así, se asoma la posibilidad de obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos, no obstante, en este ámbito en Perú no existe una forma de regular la responsabilidad, lo que a su vez imposibilita implementar este control; solo se debe trabajar desde el incentivo para garantizar

que se verifique lo relacionado al monitoreo de la identidad de las personas. A pesar de ellos, por parte de los entrevistados existe opiniones encontradas en cuanto a la real factibilidad legal del control de contenidos al existir derechos de carácter constitucional como la información y la libertad de expresión. Sin embargo, es claro que la capacidad de los intermediarios de limitar información puede ser poco factible sino se encuentra respaldada por una legislación que no violente derechos constitucionales, sino que propicie su respeto.

Las anteriores posturas se vinculan con la jurisprudencia peruana, en donde se ha dejado por sentado lo relacionado a las obligaciones, en el sentido que se debe ofrecer una protección al consumidor; un caso específico es el de Mercado Libre, sentencia Resolución Final N° 2419-2015/CC2, en la cual se destaca que la obligación del intermediario es realmente estar presente y satisfacer las necesidades de ambas partes, en todo caso se debe brindar seguridad en la plataforma de pago, siendo que frente a cualquier disputa se harán responsable, afirmando la sentencia que en ese caso de mercado libre como intermediario en las ventas por medio de Internet, tiene la responsabilidad por no desarrollar un sistema totalmente seguro.

Lo anterior conlleva a determinar la posibilidad de obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos en el Perú, de acuerdo a la opinión de los entrevistados, siendo que se deben aplicar sanciones con sumas exorbitantes, a través de normativa que imponga, regule y sancione la adopción de debida diligencia, resultando importante el registro y la creación de un organismo regulador, por cuanto en Perú no existe en la actualidad una Entidad que regule y supervise las plataformas virtuales, no obstante, el

Ministerio de Justicia tiene una unidad orgánica dedicada a la protección de los datos sensibles de los ciudadanos.

También resulta fundamental el otorgamiento de incentivos, reconocimientos y asensos en el trabajo que motiven a los intermediarios de Internet a cumplir eficientemente su labor de monitoreo y vigilancia en la lucha contra los delitos informáticos en el Perú, así como también debe realizarse un monitoreo efectivo y continuo.

En todo caso, lo anterior se conjuga con lo señalado por Vilca (2018) en su estudio, en el sentido de que las personas encargadas de investigar los delitos informáticos poseen los indicadores o componentes que pueden ser utilizados como evidencia y prueba en el proceso penal. Por ello, su cuidado debe garantizar la protección de su contenido; es decir, deben ser recolectados y procesados con sumo cuidado para ser presentados ante las autoridades judiciales correspondientes; por lo que es imperativo que los mismos sean protegidos.

Los entrevistados están de acuerdo en que el control de contenidos y usuarios por parte de intermediarios es posible, siempre que no infrinja derechos fundamentales como la privacidad y la protección de datos. Sin embargo, se resalta que en Perú no existe una regulación efectiva para abordar esta responsabilidad. Surge un debate sobre la legalidad de esta vigilancia, en vista de derechos constitucionales como la libertad de expresión e información. Se destaca la necesidad de establecer una legislación que respalde la capacidad de los intermediarios para limitar información sin vulnerar los derechos fundamentales. Estas perspectivas se relacionan con la jurisprudencia, como en el caso de Mercado Libre, donde se enfatiza la responsabilidad del intermediario en asegurar

la seguridad en su plataforma. Los entrevistados sugieren que los intermediarios deberían intensificar la vigilancia para prevenir delitos informáticos en Perú, implementando sanciones significativas y regulaciones gubernamentales. También se plantea la idea de ofrecer incentivos para motivar a los intermediarios a llevar a cabo un monitoreo constante. Asimismo, se analiza si las opiniones reflejan una visión criminológica convencional o una perspectiva alternativa, y cómo esto podría estar impactando la privacidad. Se recalca la importancia de encontrar un equilibrio entre la seguridad, la privacidad y el respeto a los derechos constitucionales para lograr una vigilancia efectiva y ética en el contexto digital.

Aunque no se pudo confirmar directamente que esta medida evite de manera absoluta la suplantación de identidad, es innegable que el monitoreo se presenta como una herramienta fundamental para el control y la prevención de dicho delito. Aunque no se pueda afirmar una eliminación total de la usurpación de identidad mediante el monitoreo, su implementación adecuada y focalizada puede desempeñar un papel significativo en la reducción de este delito y en la protección de los derechos constitucionales, como el derecho a la información y la libertad de expresión. Además, el monitoreo podría contribuir a una respuesta más rápida y efectiva ante situaciones de suplantación de identidad, lo que, a su vez, podría disuadir a potenciales perpetradores. En este sentido, la investigación resalta la importancia de encontrar un equilibrio entre la prevención de delitos y la preservación de los derechos fundamentales de los usuarios en el entorno digital.

4.2.4. Objetivo específico 3: Evaluar la necesidad de propiciar una ley sobre la delimitación de la responsabilidad de los proveedores de servicios de Internet para disminuir delitos informáticos en el Perú.

De acuerdo con la postura de la mayoría de los entrevistados, se debe efectivamente evaluar la necesidad de propiciar una ley sobre la delimitación de la responsabilidad de los proveedores de servicios de Internet para disminuir delitos informáticos en el Perú. Para ello es importante establecer una medida legal para limitar los actos que originan el delito de suplantación de identidad, especialmente cuando se involucran los servicios de Internet.

Esta requerida legislación debe contener sanciones para intermediarios y usuarios que realicen actos delitos de suplantación de identidad con el agravante de la sustracción del patrimonio, tales como sanción pecuniaria y algunos años de cárcel. De igual manera resulta importante para estos efectos que se regulen las actividades que realizan los proveedores del servicio de Internet, páginas web y acceso a redes sociales, promoviendo directivas que obliguen a un procedimiento obligatorio y riguroso para hacer confiable estas plataformas virtuales.

Un aspecto importante para ello es que legislación determine las modalidades de engaño para el cometimiento de los delitos suplantación de identidad, ante lo cual, de acuerdo a los entrevistados, se debe identificar los delitos comúnmente realizados no solo limitar el ámbito de imputación en la falsedad informática, a la suplantación de identidad, sino también ubicar dentro de estos mismos delitos, la utilización de documentos digitales o datos fraudulentos, pues es común también dicha modalidad para posibilitar el engaño en las posibles víctimas, lo que resultaría un tipo penal pluriofensivo y necesaria

regulación, sea de forma independiente, o como una modalidad agravada, respecto a la utilización de documentos digitales falsas, realizado en actos de suplantación de identidad. A pesar de ello, igualmente existe la postura que la ley penal no puede describir cada o todo tipo de supuesto fáctico típico que constituirá el delito de suplantación de identidad.

En todo caso, la opinión mayoritaria de los entrevistados coincide con el estudio de Jijón (2017), en el sentido de que existe la necesidad de dictarse una normativa para salvaguardar el ejercicio de derechos humanos como la libertad de expresión, es imprescindible establecer un marco normativo que regule la responsabilidad de los intermediarios en Internet. Esto supondría clasificar los distintos tipos de contenidos disponibles en la red y tener en cuenta la posible vulneración de derechos que pueden facilitar dichos contenidos.

Además, esta necesidad no sería distinta a lo que ya existe en otros países, pues tal como lo señaló el estudio de Celli (2019), el legislador argentino ha logrado adecuar sus normas internas a los parámetros internacionales referidos a la regulación y control de los delitos informáticos, y la legislación internacional, de países desarrollados, presenta desde hace tiempo un ordenamiento apropiado que incluye tanto a los delitos cometidos por medio del empleo de la tecnología, como a aquellos cuyo objetivo son los propios sistemas informáticos.

Asimismo, el estudio de Morales (2016), evidenció al igual que lo antes señalado que la delincuencia informática ha sido regulada internacionalmente, como por ejemplo mediante el Convenio de Budapest, la medida más efectiva para combatir este delito radica en la implementación de legislaciones adecuadas que aborden la problemática, tanto a nivel nacional como local e internacional.

La discusión aborda si las opiniones representan una criminología convencional o un enfoque más alternativo, y cómo esto impacta la privacidad. Se evalúa la necesidad de una ley para regular la responsabilidad de los proveedores de servicios de Internet y prevenir delitos informáticos en Perú. La mayoría de los entrevistados concuerda en la importancia de establecer una legislación que delimite la responsabilidad de los proveedores de servicios de Internet para reducir los delitos informáticos. Esto involucra sanciones para intermediarios y usuarios que cometan delitos de suplantación de identidad, con énfasis en la protección del patrimonio. La regulación también debe abordar las actividades de plataformas digitales para garantizar su confiabilidad. Se destaca la necesidad de definir modalidades de engaño en los delitos de suplantación de identidad, como el uso de documentos digitales falsos. Aunque algunos creen que la ley penal no puede cubrir todos los escenarios, se coincide en la importancia de regular los contenidos y la responsabilidad de los intermediarios en línea. En concordancia con estudios internacionales, se subraya la necesidad de seguir ejemplos de legislación de otros países y se hace referencia al Convenio de Budapest. En definitiva, la discusión busca equilibrar la prevención de delitos informáticos con la protección de la privacidad y los derechos humanos.

V. CONCLUSIONES

PRIMERA: Se ha identificado que el rol de los intermediarios de Internet es fundamental por cuanto se enfoca en la generación de la seguridad digital, aunque se ha evidenciado la carencia de herramientas para la lucha contra el delito de suplantación de identidad en el Perú; por lo que, se debería generar un mecanismo en los cuales se gestione un equilibrio entre los derechos fundamentales con la seguridad digital.

SEGUNDA: Se ha determinado que la responsabilidad de los intermediarios de Internet puede regirse mediante una cláusula penal que aborde acciones u omisiones perjudiciales para la persona. Esto se basa en la definición de responsabilidad civil, la cual incluiría indemnizaciones por daños y perjuicios como parte de la reparación civil. Aunque es esencial establecer responsabilidad penal para los intermediarios en casos de suplantación de identidad, como parte de la sanción por el incumplimiento intencional de las normas fundamentales por parte de dichos intermediarios.

TERCERA: Se ha identificado que es factible realizar el monitoreo y vigilancia siempre y cuando se proteja los derechos fundamentales de los usuarios en cuanto al tratamiento de sus datos para evitar prevenir la suplantación de identidad; por ello, en caso de omisión a esta obligación debe ser sancionada de manera penal.

CUARTA: Se ha identificado que es necesario la regulación en el marco normativo sobre los límites que tiene en su actividad los intermediarios y proveedores de servicios de Internet, por cuanto son los encargados de velar por el acceso seguro y confiable a la red. Por ello, se puede indicar que la

creación de una legislación adecuada, acorde con la evolución de los servicios en línea, y que establezca claramente los roles y responsabilidades de los involucrados resultaría beneficioso para disminuir los delitos informáticos en el Perú.

VI. RECOMENDACIONES

En virtud de las conclusiones expuestas, se plantean las siguientes recomendaciones:

PRIMERA: Se recomienda propiciar una adecuada formación o capacitación de los intermediarios sobre la enorme responsabilidad que tienen en la actuación de brindar los servicios de Internet, al encontrarse vinculados o en juego derechos fundamentales de los usuarios del servicio. Así es fundamental crear conciencia, aún ante una negativa de la reforma legislativa, del rol fundamental de estos intermediarios, por cuanto a pesar de que el Perú no cuenta con una legislación exhaustiva, si permite aplicar sanciones, desde leves o graves, para disminuir el cometimiento de delitos.

De igual manera es propicia la capacitación de los juzgadores, por cuanto la materia de delitos informáticos es aún poco conocida y cada día evoluciona ferozmente, por lo que cada vez más surgen distintas modalidades de delitos, así como numerosos prestadores de servicio que no se encuentran posiblemente debidamente supervisados por los órganos competentes. De allí que, es esencial que los jueces tengan un claro conocimiento, continuo, además, de estos temas y de las posibles responsabilidades penales y civiles que deben aplicar aun cuando se trate del proveedor o el intermediario del servicio.

SEGUNDA: La determinación de la responsabilidad penal de los intermediarios de Internet, por cuanto ello puede contribuir a fortalecer la actuación del Estado peruano frente al delito de suplantación de identidad, y esto puede

lograrse a través de una clara legislación adecuada y adelantada a los cambios tecnológicos.

TERCERA: Establecer por ley la obligatoriedad medidas de monitoreo y vigilancia extremas y adecuadas a los cambios constantes de la tecnología, o al menos que se actualicen contantemente, para evitar el cometimiento de delitos, como el delito de usurpación de identidad, siendo éste apenas uno de los distintos que pueden cometerse con el uso de la tecnología. Para aplicar medidas en principio internas rápidas y expeditas, como el bloqueo del usuario, así como la denuncia inmediata de lo constatado a los órganos de seguridad.

CUARTA: Promulgar una ley sobre la delimitación de la responsabilidad de los proveedores de servicios de Internet para disminuir los delitos informáticos en el Perú. Así pues, se recomienda al Estado peruano legislar de manera eficiente sobre la suplantación de identidad, entre otros delitos, y la responsabilidad civil o penal dentro de esta acción.

VII. REFERENCIAS BIBLIOGRÁFICAS

Abad, L. (2018). Responsabilidad de los Intermediarios de Internet (ISP) dedicados al comercio electrónico. *Repositorio Institucional Universidad Austral*, 1-13.

ABC Redes. (2021). *Alertan sobre una oleada de casos de suplantación de identidad en Instagram*. https://www.abc.es/tecnologia/redes/abci-alertan-sobre-oleada-casos-suplantacion-identidad-instagram-202102220109_noticia.html

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia: RVG, 25(89)*, 351-368. https://dialnet.unirioja.es/servlet/articulo?codigo=8890269

Acurio, S. (2015). Delitos Informáticos: Generalidades. *Delitos Informáticos*, 5-18. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aguilar, E. (2019). Suplantación de la identidad digital con fines de trata de personas en Facebook. *México: INFOTEC centro de investigación e innovación en tecnologías de la información y comunicación*. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf

Alarcón, C. (2015). La suplantación de identidad en los trámites notariales de compraventa de bienes muebles e inmuebles y el perjuicio patrimonial del adquiriente. *Universidad Regional Autónoma de los Andes*. https://dspace.uniandes.edu.ec/bitstream/123456789/5591/1/TUAMDN002-2017.pdf

Califano, B. (2017). Responsabilidad de intermediarios en Internet: un análisis a partir del caso Maiorana. *Revista Fibra. Tecnologías de la Comunicación*, 3-51. https://ri.conicet.gov.ar/handle/11336/75332

Carrasco, S. (2017). Metodología de la Investigación Científica. *Editorial San Marcos*. https://www.academia.edu/26909781/Metodologia_de_La_Investigacion_Cientifica_Carrasco_Diaz_1_

Celli, S. (2019). Las nuevas tecnologías y los delitos informáticos. Análisis de la Ley 26.388 Modificación del Código Penal argentino. *Universidad Siglo 21*. https://repositorio.21.edu.ar/bitstream/handle/ues21/16861/CELLI%20TRIUNFETTI%20Sebastian.pdf?sequence=1

Código Penal. (1991). Código Penal. En *Poder ejecutivo del Perú*. http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. *Council of Europe*. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Corcoy, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos. Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos. *Eguzkilore*, 7-32. https://dialnet.unirioja.es/servlet/articulo?codigo=3289399

Cotino, L. (2017). Responsabilidad de intermediarios y prestadores de servicios de internet en Europa y Estados Unidos y su importancia para la libertad de expresión. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 17. https://dialnet.unirioja.es/servlet/articulo?codigo=7499158

Din, T. (2014). Los intermediarios del Internet: Dilema de responsabilidad –sesión de preguntas y respuestas. *ARTICLE 19*. https://www.article19.org/es/resources/Internet-intermediaries-dilemma-liability-q/

Directiva 31/CE. (2000). Directiva 2000/31/CE del Parlamento Europeo y del Consejo. *Diario Oficial de las Comunidades Europeas, L178*. https://www.boe.es/doue/2000/178/L00001-00016.pdf

Fresneda, S. (2021). ¿Es delito el robo o suplantación de identidad en Internet? *Dexia Abogados*. https://www.dexiaabogados.com/blog/suplantacion-identidad-Internet/

Fuster, D. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. *Propósitos y representaciones, 7(1),* 201-229. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992019000100010

Génez, O., & González, H. (2023). Responsabilidad penal en el uso de las redes sociales. *Revista Jurídica, 15 (1),* 33-43. https://doi.org/10.5281/zenodo.8014538

Gestión. (2020a). Fraudes en línea se disparan este año en Perú ante mayor uso de Internet. *Gestión*. https://gestion.pe/peru/fraudes-en-linea-se-disparan-este-ano-en-peru-ante-mayor-uso-de-Internet-noticia/

Gestión. (2020b). PNP explica cómo denunciar la suplantación de identidad en redes sociales. *Gestión*. https://gestion.pe/peru/pnp-explica-como-denunciar-la-suplantacion-de-identidad- en-redes-sociales-nndc-noticia/

Gibs, J. (2017). *Conceptos basicos sobre Internet*. https://www3.uji.es/~pacheco/INTERN~1.html

Gobierno de Canarias. (2016). ¿Qué es la Identidad digital? *Uso seguro y responsable de las TIC*. https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/

Hernández, R., Fernández, C., & Baptista, M. del P. (2014). *Metodología de la Investigación* (6ta Ed). Mc Graw Hill.

INISEG. (2019). *Cibercrimen organizado: último estudio de la Europol 2019*. https://www.iniseg.es/blog/ciberseguridad/cibercrimen-organizado- ultimo-estudio-de-la-europol-2019/

Jijón, E. (2017). Responsabilidad de intermediarios de internet : hacia una regulación que garantice el ejercicio del derecho a la libertad de expresión y otros derechos fundamentales. *Universidad Católica de Santiago de Guayaquil*. http://repositorio.ucsg.edu.ec/handle/3317/8132

Jimenez, J. (2017). Manual de Derecho Penal Informatico. *Lima: Jurista Editores*.

Kinde, K. (2019). *Los principales mecanismos de protección de la propiedad inmueble para evitar los fraudes inmobiliarios por suplantación de identidad y falsificación de documentos. ¿Son estos mecanismos eficientes?* https://pirhua.udep.edu.pe/handle/11042/3938.

Lara, J., & Vera, F. (2011). Responsabilidad de los prestadores de servicios de Internet. *ONG Derechos digitales*. https://www.derechosdigitales.org/wp-content/uploads/pp03.pdf

Levy, M., & Aguerre, C. (2019). Intermediarios de Internet : consideraciones para reflexionar en el contexto de Argentina. *Universidad de San Andrés*. http://hdl.handle.net/10908/16475

Ley N° 30171. (2014). *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. https://www.gob.pe/institucion/minsa/normas-legales/197055- 30171

Ley Nº 30096. (2013). *Ley de Delitos Informáticos*. http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF052583160 06064AB/$FILE/6_Ley_30096.pdf

López, J. (2016). *¿Cuáles son los grandes riesgos del Internet según el Banco Mundial?* https://www.elfinanciero.com.mx/tech/cuales-son-los-grandes-riesgos-del-internet-segun-el-banco-mundial/

Manila Principles. (2015). The Manila Principles on Intermediary Liability Background Paper. *Electronic Frontier Foundation*. https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf

Martínez, A., & Porcelli, A. (2015). Alcances de la Responsabilidad Civil de los Proveedores de Servicios de Internet (ISP) y de los Proveedores de Servicios Online (OSP) a nivel internacional, regional y nacional. Las disposiciones de Puerto Seguro, Notificación y Deshabilitación. *Revista Pensr en Derecho, 6(1)*.

Mendo, A. (2014). Delitos y redes sociales: Mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad. *Revista General de Derecho Penal*, 22.

Millaleo, S. (2015). Los intermediarios de Internet como agentes normativos. *Revista de derecho (Valdivia)*. http://dx.doi.org/10.4067/S0718-09502015000100002

Morales, D. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú - 2015. *Universidad Señor de Sipán*. https://hdl.handle.net/20.500.12802/3161

OEA. (2013). Libertad de expresión e Internet. Informe de la Relatoría Especial para la Libertad de Expresión. *CIDH*.

OEA. (2018). *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

ONU. (2011). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. *Asamblea General*. https://www.acnur.org/fileadmin/Documentos/BDL/2015/10048.pdf

Ortiz, N. (2019). *Normativa Legal sobre Delitos Informáticos en Ecuador*. https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. *Universidad César Vallejo*. https://hdl.handle.net/20.500.12692/20372

Pérez-Prieto, R. (2015). ¿Qué juzgado debe ser el competente (en razón de la materia) cuando se involucra a un tercero civilmente responsable? *THEMIS Revista De Derecho*, *68*, 217-226.

Pichihua, S. (2019). *Estos son los delitos informáticos más frecuentes en el Perú, según la Policía*. https://andina.pe/agencia/noticia-estos-son-los- delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

Quevedo, J. (2017). Investigación y prueba del ciberdelito. *Universidad de Barcelona*. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1

Reichertz, J. (2018). *Responsabilidad de los intermediarios de Internet: ¿qué es lo que se discute?* https://josecrettaz.com/contenidos/responsabilidad-de-los-intermediarios-de-Internet-que-es- lo-que-se-discute/

Resolución Legislativa N° 30913. (2019). *Resolución legislativa que aprueba el Convenio sobre la Ciberdelincuencia*. https://busquedas.elperuano.pe/dispositivo/NL/1740637-2

Rojas, J. (2023). Análisis de la responsabilidad penal de los intermediarios de Internet frente a los contenidos ilícitos. En V. Espinoza & R. Elías (Eds.), *Cibercriminalidad y Delitos Informáticos* (pp. 181-198). Instituto Pacífico.

Schettini, P., & Cortazzo, I. (2016). Técnicas y estrategias en la investigación cualitativa. *Editorial de la Universidad Nacional de La Plata (EDULP)*.

School, E. (2022). ¿Qué es la identidad personal y ejemplos? *Euroinnova International Online Education*. https://acortar.link/z7Afuj

Senado de la República de México. (2019). Proposición con punto de acuerdo que exhorta al Ejecutivo Federal a enviar al Senado el Convenio de Budapest sobre Ciberdelincuencia. *LXIV LEGISLATURA*. https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-09-18-1/assets/documentos/PA_PVEM_Sen_Lagunes_Convenio_Budapest.pdf

Soto, L. (2022). *¿Qué es la identidad digital y cómo puedes protegerla?* https://www.signaturit.com/es/blog/que-es-la-identidad-digital/

Universidad Veracruzana. (2016). *Conocimientos generales: ¿Cómo reducir el riesgo de suplantación de identidad? – Seguridad de la información*. https://www.uv.mx/infosegura/general/conocimientos_suplantacion/

UNODC. (2018). Cybercrime module 7 key issues: Formal international cooperation mechanisms. *Unodc.org*. https://www.unodc.org/e4j/es/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

USECIM. (2019). *Los delitos cibernéticos causarán daños por un valor de $6 billones de dólares en 2021*. https://acortar.link/ztdhZo

Van, M. (2014). *Doctrina jurídica: ¿Qué métodos para qué tipo de disciplina?* https://acortar.link/XQoaL2

Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, *053*, 95-110. https://bit.ly/3sNpYOV

Vilca, G. (2018). Los hackers: Delito informático frente al Código Penal peruano. *UNASAM*. http://repositorio.unasam.edu.pe/handle/UNASAM/2496

Villavicencio, F. (2014). Delitos Informáticos. *Revista ius et veritas*, *49*.

ANEXOS

ANEXO 1. Instrumento de recolección de datos

GUÍA DE PREGUNTAS

La presente entrevista se realiza con el propósito de Indagar sobre el rol de los intermediarios de Internet en la lucha contra el delito informático en Perú, 2020. Cabe destacar que las respuestas suministradas por usted, solo se utilizarán con fines académicos para la elaboración de mi tesis para optar al grado de Profesional de Abogado en la Universidad Nacional del Altiplano. En este contexto,se considerarán todos los principios éticos a los fines de resguardar los datos suministrados.

Instrucciones: Para cada planteamiento, se agradece fundamentar sus respuestas.

INTERMEDIARIOS DE INTERNET

Criterio 1. Analizar la responsabilidad de los intermediarios

1. ¿Cuál es el rol de los intermediarios de Internet en la lucha contra el delito de suplantaciónde identidad?
2. ¿De qué manera la responsabilidad penal de los intermediarios de Internet puede fortalecerel control y la detención que ejerce el Estado peruano sobre los sujetos que cometen el delito de suplantación de identidad? ¿Cómo se puede fijar esta responsabilidad?
3. ¿De qué manera puede ser viable que los intermediarios de Internet respondan civilmente por cualquier daño que se genere con el uso de su servicio?

Criterio 2. Indagar sobre obligaciones de los intermediarios de Internet

1. ¿De qué manera se puede obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos en el Perú?

2. ¿De qué manera se puede obligar a los intermediarios de Internet a incrementar sus actividades de monitoreo y vigilancia de los contenidos y usuarios de sus redes para evitar los delitos informáticos en el Perú?

3. ¿De qué manera el control de los contenidos y usuarios por parte de los intermediarios de Internet puede resultar legalmente factible? ¿Cuáles derechos podrían vulnerarse?

SUPLANTACIÓN DE IDENTIDAD

Criterio 3. Profundizar sobre los medios empleados en el delito de suplantación de identidad

4. En su opinión, ¿cuál medida legal pudiera dictarse para limitar los actos que originan el delito de suplantación de identidad, especialmente cuando se involucran los servicios de Internet?

5. En su opinión, ¿legalmente cómo podrían bloquearse plataformas digitales para evitar la ejecución de algún delito de suplantación de identidad? ¿Quién debería asumir esa responsabilidad?

Criterio 4. Profundizar sobre las estrategias de ingeniería social para el cometimiento del delito desuplantación de identidad

6. En su opinión, ¿cómo la legislación podría determinar las modalidades de engaño para el cometimiento de los delitos suplantación de identidad?

7. En su opinión, ¿de qué manera los daños virtuales que se producen con el delito de suplantación de identidad pueden valorarse en caso de declararse alguna responsabilidad civil?

8. ¿Quiénes podrían ser los responsables de los daños cometidos por usuarios en caso de losdelitos de suplantación de identidad?

ANEXO 2. Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Yesenia Lupaca Quispe,
identificado con DNI 73624349 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

de Derecho,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"Rol de los intermediarios de Internet en la lucha contra el delito de suplantación de Identidad en Perú, 2020."

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 10 de abril del 2024

FIRMA (obligatoria)

Huella

ANEXO 3. Autorización para el depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Yesenia Lupaca Quispe,
identificado con DNI 73624349 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

de Derecho,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

" Rol de los Intermediarios de Internet en la lucha contra el delito de suplantación de identidad en Perú, 2020. "

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 10 de abril del 2024

FIRMA (obligatoria)

Huella