FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TESIS

El Doxing y su necesaria incorporación en los Delitos Informáticos

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADA

Autora

Bach. Puican Ordoñez Ana Lucia
https://orcid.org/0009-0002-9148-5199

Asesor
Mg. Cabrera Leonardini Daniel Guillermo
https://orcid.org/0000-0001-5963-9405

Línea de Investigación

Desarrollo Humano, Comunicación y Ciencias Jurídicas para Enfrentar los Desafíos Globales

Sublínea de Investigación

Derecho Público y Derecho Privado

Pimentel – Perú

2024

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, Ana Lucia Puican Ordoñez, del Programa de Estudios de Curso-Taller Actualización de Tesis para egresados de pregrado y posgrado de la USS y egresados de pregrado de universidades con licencia denegada, de la escuela profesional de Derecho de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autora del trabajo titulado:

El Doxing y su necesaria incorporación en los Delitos Informáticos

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Puican Ordoñez Ana Lucia	DNI: 41958085	

Pimentel, 12 de junio de 2024.

REPORTE DE SIMILITUD TURINITIN

Reporte de similitud

NOMBRE DEL TRABAJO
El Doxing y su necesaria incorporación en los Delitos Informáticos.docx

AUTOR
Ana Lucia Puican Ordoñez

RECUENTO DE PALABRAS
10952 Words

RECUENTO DE CARACTERES
59966 Characters

RECUENTO DE PÁGINAS
37 Pages

TAMAÑO DEL ARCHIVO
61.4KB

FECHA DE ENTREGA
Sep 4, 2024 8:22 AM GMT-5

FECHA DEL INFORME
Sep 4, 2024 8:22 AM GMT-5

11% de similitud general

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

- 11% Base de datos de Internet
- 3% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 7% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

EL DOXING Y SU NECESARIA INCORPORACIÓN EN LOS DELITOS INFORMÁTICOS

Aprobación del jurado

MG. OBIOL ANAYA ERIK FRANCESC

Presidente del Jurado de Tesis

MG. HANANEL CASSARO CECILIA ELIZABETH

Secretario del Jurado de Tesis

MG. CABRERA LEONARDINI DANIEL GUILLERMO

Vocal del Jurado de Tesis

EL DOXING Y SU NECESARIA INCORPORACIÓN EN LOS DELITOS INFORMÁTICOS

Resumen

El presente estudio tuvo por objetivo Incorporar el Doxing como delito informático en la Ley 30096 para proteger el derecho a la intimidad; la metodología empleada fue cuantitativa con diseño no experimental - descriptiva; la técnica empleada fue el análisis documental, mediante el instrumento de guía de análisis documental. Los resultados demostraron que el Perú en materias de normativas asociadas a los delitos informáticos no se encuentra actualizado, dado que, la última modificación del código penal para agregar las nuevas formas de vulneración de derechos por plataformas digitales fue en el año 2014, por ello, se puede afirmar que la ley cuenta con vacíos legales en casos de ciberdelincuencia; concluyendo que se debe incorporar el Doxing como delito informático en la Ley 30096 específicamente en el primer párrafo del artículo 7, agregando a los nuevas causales de delito informático a la exposición no autorizada de nombres reales, direcciones, lugar de trabajo, informes médicos, con el propósito de causar humillación, intimidación, acoso con el fin de dañar la trayectoria pública, profesional o familiar.

Palabras Clave: Doxing, delito informático, derecho a la intimidad.

Abstract

The objective of this study was to incorporate Doxing as a computer crime in Law 30096 to protect the right to privacy; the methodology used was quantitative with a non-experimental - descriptive design; the technique used was the documentary analysis, using the documentary analysis guide instrument. The results showed that Peru in matters of regulations associated with cybercrime is not updated, since the last amendment of the criminal code to add new forms of violation of rights by digital platforms was in 2014, therefore, it can be said that the law has legal gaps in cases of cybercrime; concluding that Doxing should be incorporated as a computer crime in Law 30096 specifically in the first paragraph of article 7, adding to the new causes of computer crime the unauthorized exposure of real names, addresses, place of work, medical reports, with the purpose of causing humiliation, intimidation, harassment in order to damage the public, professional or family trajectory.

Keywords: Doxing, computer crime, right to privacy.

I. INTRODUCCIÓN

En el Perú, hasta el año 2022 se denunciaron más de 300 casos mensuales asociados al delito informático, llegando a la cifra de 3946 en total (Pichihua, 2023), ante lo señalado se puede precisar que existen múltiples métodos que utilizan los ciberdelincuentes para adquirir información sobre las personas para diferentes fines, los cuales abarcan desde el acoso, extorsión hasta el robo sistemático de dinero.

En el contexto legal estadounidense Mery (2021) señala se han promulgado diversas directrices legales para combatir de manera directa y correcta el acoso cibernético, se tiene en consideración la promulgación de una enmienda a la Ley de privacidad que aborda de manera directa la divulgación pública de las informaciones que identifica a una persona u organización en particular.

Gregory (2021) menciona que la Unión Europea (UE) ha ido implementando de manera significativa su Reglamento General de Protección de Datos (GDPR) desde mayo del 2018 mediante el cual ha podido brindar a los usuarios un control más óptimo sobre sus datos personales en línea.

El Doxing es entendido como la revelación de datos e información sin consentimiento previo de las personas, mostrando los nombres reales, direcciones, lugar de trabajo, informes médicos, con el propósito de causar humillación, intimidación, acoso con el fin de dañar la trayectoria pública, profesional o familiar. (Latto, 2023).

En el contexto social turco Kukul (2023) describieron que más del 62% de los jóvenes inocentes han enfrentado diversos conflictos relacionados a la perdida de la reputación, pérdidas de su trabajo, acosos, daños físicos o muerte, debido a los constantes acontecimientos de Doxing hacia personas equivocadas, provocando problemas graves en la integridad de las personas que son afectadas en estas situaciones.

Desde el panorama hindú, Abarna et al. (2022) describieron que el 36% de personas sufrieron de ciberacoso, debido al incrementado uso de los dispositivos móviles y redes sociales por parte de los adolescentes, mediante el cual los acosadores compartían publicaciones negativas, informaciones personales sin el consentimiento de la otra persona, contenidos falsos o mensajes en relación a las víctimas con la intención de humillarlas o amenazarlas de manera repetidas en las diferentes plataformas digitales.

Desde la perspectiva de Chen et al. (2019) detectaron que en las sociedades chinas, el 50% de los jóvenes son acosados cibernéticamente, mediante el cual se perciben factores que se relacionan de manera directa con la publicación de mensajes provocativos u ofensivos, como también, la suplantación de identidad, revelaciones de información sin el consentimiento y engaños, generando problemas severos de comportamiento en los adolescentes bajo actitudes prosociales, hiperactividad e inseguridades; a la vez, Cheung (2021) señala que los delitos de Doxing entre las comunidades chinas se han encontrado relacionados directamente con el “vigilantismo” digital por parte de las autoridades sobre la población, trayendo como consecuencia pérdidas de confianza con las autoridades gobernantes.

En el panorama social canadiense, Jagayat y Choma (2021) correspondieron que, el 52% aproximado de mujeres jóvenes han descrito haber recibido mensajes de índole amenazante, compartimiento de sus fotografías privadas con otras personas sin su consentimiento o el constante acoso sexual en línea, siendo considerado estos casos como principales ejemplos de ciber agresión hacia las mujeres.

Tan (2023) describe que más del 52% de personas en el contexto social japonés, han sido víctimas en la publicación no autorizada y a menudo maliciosa de la información personal, causando graves daños a su integridad, intimidaciones o acosos de índole sexual, asimismo, menciona que la problemática del Doxing genera mayormente en las víctimas graves angustias y traumas psicológicos, como también efectos duraderos en la reputación, posición social y el bienestar económico de la persona.

En el contexto social chino, Chen et al. (2018) revelaron por medio de su estudio que aproximadamente el 25% de los adolescentes han informado experimentar de manera directa acoso y victimización en las redes sociales, asimismo, describieron también que el 35% de los adolescentes víctimas de este tipo de acoso han recibido diversas publicaciones y mensajes amenazantes en algún momento de su interacción en estas plataformas.

Según Adetunji (2018) se pudo revelar que un docente de la Universidad de Temple se encontraba involucrado de manera directa con una cuenta en línea denominada “buscador de la verdad”, mediante el cual había realizados publicaciones con al menos un comentario anti musulmán en un sitio web de derecha y también había promovido teorías conspirativas conservadoras.

Conforme lo indica Rubio (2023) la manera legal de encontrar información sobre diferentes individuos consiste en la revisión exhaustiva en sus perfiles de redes sociales correspondientes, una vez se logre acceder a sus hábitos o rutinas, es entonces donde profundiza buscando en los perfiles de familiares y amigos, asimismo, menciona que las propias empresas del investigado puede compartir información a que primera mano suele ser inocente, sin embargo, combinado con otros datos pueden perjudicar al individuo.

Según el diario El Peruano (2023) sostiene que, en el Perú, el Banco de la nación, ha alertado de forma significativa a sus clientes y usuarios para que no sean partícipes de los ciberdelincuentes, en donde solicitan a los usuarios saber con quienes comparten su información por las redes sociales, verificar de quienes aceptan como amistades o seguidores en las redes sociales personales y que tipo de información publican en relación a su domicilio, propiedades, autos, familia, etc.

Por otra parte, Radio Programas del Perú (2023) menciona que el 51% de personas emplearon app de citas en alguna situación en específica, en donde cerca del 23% de estos admitieron haber sido engañados por perfiles falsos, asimismo, de una manera más alarmante, un 19% de los consultados en la región admitieron que fueron víctimas de Doxing,

esto quiere decir, que su información privada se pudo hacer pública en internet o fueron vendidas sin su consentimiento.

En perspectiva de Zegarra (2023) describió que de los individuos que han sido víctimas de Doxing por medio de las plataformas digitales de citas online, indicaron que el 32% fuero a través de enlaces o archivos adjuntos maliciosos, 23% fueron por medio de perfiles falsos y el 25% fueron víctimas del robo de su identidad, asimismo, el 15% de las victimas manifestaron que su supuesto “match” logró compartir información personal sin su consentimiento, la filtración de fotos intimas o el acoso en la vida real.

En la actualidad la Ley N° 30096 menciona penas para personas que interceptan data informática, pero no especifica los nuevos posibles delitos que se vienen desarrollando como es el Doxing el cual abarca no solo la interceptación de datos, sino, la publicación de estos a fin de intimidar, chantajear, acosar, etc., a las personas, violando así su derecho a la intimidad (Ley Nº 30096, 2014).

Entonces, bajo lo señalado líneas arriba, las consecuencias del Doxing en las personas agraviadas son diversas, sin embargo, a la gran mayoría pueden causarle niveles elevados de ansiedad, insomnio, estrés, miedo, en periodos de corto, mediano y largo plazo, hasta llegar al punto de esconderse de la sociedad por la vergüenza que pudieron haber desarrollado con la exposición de los datos. Cabe señalar que el Doxing se encuentra muy alineado a la violación del derecho a la intimidad debido a que se perturba el espacio, imagen y tiempo de un determinado sujeto al momento que se divulga datos o hechos privados.

Por lo tanto, la necesidad de la investigación se manifiesta debido a que en la actualidad en el plano nacional el Doxing viene siendo un problema social ya que se viene utilizando más seguido para acosar, intimidar, chantajear, publicar información personal (direcciones, números telefónicos, lugares de trabajo, información financiera) sin autorización previa de las víctimas, o hasta información falseada; por lo cual, es relevante su incorporación a los delitos informáticos.

La problemática surge a partir de cómo se comparte y entrega información personal y se mira pasivamente información ajena a través de redes sociales, es por ello que se necesita regular y mejorar la legislación para contrarrestar el delito informático. Después del análisis de la realidad problemática en los diversos contextos, se formuló como problema: ¿De qué manera el Doxing afecta el derecho a la intimidad?

El estudio se justifica teóricamente porque se analizó la problemática del Doxing en los contextos internacionales, nacional y local, asimismo, se analizaron legislaciones comparadas, teorías, conceptos y definiciones, todo ello se realizó para permitir un entendimiento profundo sobre las variables analizadas. Metodológicamente, debido a que se empleará el enfoque cualitativo para obtener conocimientos válidos y confiables sobre el fenómeno investigado (Doxing) para explicar detalladamente sobre los problemas que genera al no estar normado como delito informático. En el plano social, debido a que se pretende dar solución a un potencial delito que afecta la intimidad de las personas, siendo relevante los resultados y recomendaciones que se desarrollarán.

La investigación tuvo una implicancia practica al momento que se propuso la modificatoria de los delitos informáticos para incorporar al Doxing en el art. 7-A, mediante un anteproyecto de Ley, lo cual velará los derechos humanos y la correcta aplicación de justicia.

En función a la realidad problemática descrita se planteó por objetivo general: Incorporar el Doxing como delito informático en la Ley 30096 para proteger el derecho a la intimidad. Para lograr el objetivo general se establecieron objetivos específicos: Examinar la naturaleza del Doxing y su afectación al derecho a la intimidad. Determinar si la falta de regulación del Doxing incide en los delitos informáticos. Analizar la necesidad de regular el Doxing a través de la legislación comparada.

La hipótesis planteada fue: H1: La incorporación del Doxing como delito informático en la Ley 30096 protegerá el derecho a la intimidad.

Como antecedentes previos se analizaron estudios internacionales como son: En China, Chen et al. (2019), por medio de su artículo denominado “victimización por Doxing y problemas emocionales entre estudiantes de secundaria en Hong Kong”, afirma que el Doxing es tomado como ciberbullying en las instituciones educativas debido a que es en ese contexto donde más se viene practicando, cabe señalar que con esta práctica no solo se vulneran la privacidad de información de cada víctima al exponer su información, sino, también facilita y aumenta el acoso en la internet, llegando a producirse acoso y violencia física ya que los potenciales victimarios conocen todos los datos. Se puede concluir que en las instituciones educativas la práctica del Doxing puede intensificar el bullyng de las victimas dada la exposición de la información.

De acuerdo a lo mencionado por el investigador el Doxing en las instituciones educativas se viene presentando cada vez con mayor frecuencia fortaleciendo así el bullyng, destacándose que en oportunidades suele pasar del plano virtual al plano físico ya que por medio de la información obtenida de las víctimas se producen agresiones físicas, siendo preocupante porque no existe barrera entre lo que se publica en el mundo digital con el contexto físico.

En México, García (2021) en su artículo sobre “el derecho internacional frente a los nuevos medios y espacios en que desarrollar la ciberguerra”, describió que las practicas del Doxing no solo vulnera la privacidad de las personas al exhibir los datos personales sino también sobre las instituciones públicas, estas prácticas siendo muy preocupante debido a que no se encuentra dentro de los delitos considerados por el derecho internacional ya que no alcanza a tallar en el denominado uso de la fuerza. Concluyendo que la democracia y el derecho humano de las personas se vulneran bajo sistemas digitales, por ello, se requieren de políticas que impidan la violación del derecho a la libertad y privacidad.

Conforme al análisis del autor se puede afirmar que el Doxing es un problema social que no solo se centra en vulnerar la privacidad de las personas, sino que, se utiliza para otros fines como es la vulneración de información sensible de instituciones públicas, siendo muy

necesaria su regulación en los sistemas jurídicos.

En México, Rodríguez & Rodríguez (2021) en su artículo sobre “violencia de género en instituciones de educación superior”, describió que en las instituciones de educación superior se viene manifestando problemas asociados al Doxing, siendo muy latente en el ámbito universitario, por ello, por medio de su artículo tuvo como propósito analizar las formas de la violencia, lo cual inicia con la divulgación de información intima de las víctimas, a la vez menciona que la violencia digital se viene utilizando con la finalidad de acosar mediante mensajes amenazadores o intimidantes en redes sociales, a la vez para hostigar sexualmente.

Los autores dan a conocer la problemática que se viene viviendo en el plano latinoamericano respecto al Doxing, lo cual es una práctica que causa intimidación, ansiedad, daño psicológico, etc., por ello, menciona las formas de violencia para visibilizarlas, prevenirlas y atender rápidamente.

En Chile, Ananías & Vergara (2019) en su artículo sobre “violencia en internet contra feministas y otras activistas chilenas”, menciona que el Doxing viene jugando un papel importante en el aumento del ciberacoso ya que se vienen alterando y publicando fotos, videos, direcciones, etc., sin consentimiento de algunas activistas que buscan igualdad de derechos, a la vez, se precisó que un 82% de víctimas fueron mujeres, centrándose en un problema de género. Se determinó que en la actualidad no existe normas jurídicas que permitan penalizar la violencia y vulneración de derechos generados en el mundo cibernético, abarcando violencia por raza, religión, etnias, orientaciones sexuales, etc., siendo estas conductas dañinas y perjudiciales a nivel psicológico y físico de las víctimas.

De acuerdo a lo mencionado por el investigador un sector violentado por las prácticas de Doxing en Chile son las activistas y organizaciones sociales que luchan por el respeto de los derechos de las personas, precisándose que en su gran mayoría son mujeres las afectadas, destacándose que la falta de leyes que lo regulen hace que cada día incremente más.

Romani (2021) en su artículo, señaló que el Doxing se presenta mediante la recuperación de información privada (nombre completo, dirección, número telefónico, correos personales, hijos, etc.) y posterior publicación sin autorización previa en plataformas digitales, lo cual puede llegar a causar acoso y hostigamiento al recibir mensajes o solicitudes reiteradamente de personas que no se conocen. Según la investigación el 80% de personas sufrieron hostigamiento, 58% insultos, 49% amenazas, etc.

Este estudio da a conocer las consecuencias que trae consigo la práctica del Doxing y como esta vulnera el derecho a la privacidad de las personas y desencadenando una serie de problemas que abarca dese el hostigamiento hasta las amenazas.

Contreras & Lovera (2021) en el artículo señalan que las redes sociales son plataformas que facilitan la comunicación e información actualizada sobre los diferentes aspectos académicos, científicos, noticiosos, etc., muchas veces se utilizan para practicar el ciberacoso por medio del “Doxing”, donde se expone información personal importante de las personas siendo perjudiciales atentando contra la honra y vida privada de las víctimas. Concluyendo que no existe jurisprudencia asociada al Doxing y al rol de las redes sociales a fin de prevalecer los derechos de las personas como es de la honra y la intimidad.

El estudio de los autores mencionan que el papel que tienen las redes sociales mediante las diferentes plataformas son muy importantes para la mayoría de personas debido a que se mantienen actualizados de las noticias que suceden día a día, sin embargo, también existe un vacío legal que no monitorea, controle y juzgue a aquellas personas que vulneran los derechos de las personas como es la honra y la intimidad, por lo tanto, es urgente el diseño de propuestas que puedan sancionar este tipo de actos.

El Doxing y su necesaria incorporación en los delitos informáticos se explican considerando diferentes fundamentos epistemológicos como también teorías, conceptos, características y definiciones a fin de comprender a profundidad el problema actual, para ello, se plantearon los siguientes aspectos:

Respecto a las teorías relacionadas al tema, en el presente apartado se inicia con la definición de la teoría unitaria personal, mediante el cual en la obra de Hassemer y Muñoz Conde se percibe una percepción única en relación al bien jurídico fundamentada en el individuo. En relación a los autores, quienes tiene en cuenta que la lesión o el daño que recibe un bien jurídico se basa en factores que determinan de manera potencial el merecimiento de una pena, asimismo, se describe que un mandato penal o una prohibición recibe una justificación única en el momento que se brinda la protección a intereses calificables como bienes jurídico penales (Szczaranski, 2012).

Teoría de la pena, se basa en responder a las penas aplicadas por el sistema jurídico, por ello, se puede decir que las penas son coerciones impuestas que supone la privación de un derecho, el cual no se reparará ni restituirá o detendrá alguna lesión o peligro inminente. Esta teoría es relevante y tiene sentido por medio del ordenamiento jurídico moderno, por la cual las penas se convierten en consecuencias jurídicas de los delitos por excelencia frente a cada excepción, medida de seguridad o consecuencia accesoria de un delito (Rodríguez, 2019).

En relación al Doxing, Contreras y Lovera (2021) definen que el Doxing es considerado como una tipología de acoso cibernético mediante el cual los datos personales de un individuo, o sus quehaceres cotidianos son circulados por medio de cualquier plataforma digital o red social, asimismo, sostienen que esas informaciones de índole personal, que en situaciones incluyen el lugar donde trabajan y otros antecedentes sensibles, traen consigo diferentes perjuicios para el respeto y protección de la vida privada y honra de los individuos.

Olivero et al. (2020) señala que el Doxing se refiere a la acción de revelar las informaciones personales de algún individuo en línea, se le considera como una tipología de ciberacoso que involucra la revelación de datos personales de las víctimas como lo son el nombre personal, dirección, trabajo u otras informaciones confidenciales sin el consentimiento de la persona, asimismo, sostienen que el Doxing tiene como principal objetivo humillar, intimidar, acosar o perjudicar a la víctima.

Según la definición de Zulfahmi et al. (2023) el Doxing se encuentra relacionado al conjunto de acciones mediante el cual se recopila y se publica diversas informaciones personales de algún individuo o de un grupo en particular sin el consentimiento previamente debido, con el principal objetivo de hacer daño a la trayectoria pública o profesional de la víctima, asimismo, mencionan que esta práctica no solamente afecta a la víctima sino también sus familiares y amigos más cercanos se ven afectados.

Como lo menciona García B. (2021) el Doxing se refiere a la práctica que realizan ciertos individuos con intenciones negativas en las cuales consiste en la publicación, mayormente de manera digital, de informaciones personales de sus víctimas con la finalidad de avergonzar o intimidar.

En relación a Kelley y Weaver (2020) definen al Doxing como el conjunto de acciones maliciosas mediante el cual unos individuos recopilan y comparten informaciones digitales de índole personal de diferentes personas sin el consentimiento debido para su difusión con la única intención de desprestigiar y hacer daño, afectando considerablemente su bienestar como el de su familia y amigos más cercanos.

Romani (2021) señala que el Doxing se encuentra definido como la acción de revelar diversas informaciones personales de algún individuo en línea, que se encuentre relacionado sus nombres reales, dirección particular, datos financieros, entre otras informaciones personales, en donde posteriormente estas informaciones son divulgadas al público sin el consentimiento ni el permiso de la víctima, afectando su bienestar y dignidad.

Conforme lo menciona Porcedda (2023) el Doxing se relaciona de manera directa en la acción de revelar datos personales de alguna persona en particular de manera digital, asimismo, se le considera una tipología de ciberacoso que involucra a la revelación considerable de informaciones personales, como lo es el nombre real del individuo, su dirección de hogar u otros datos sin el consentimiento de la víctima, mediante el cual tiene como principal objetivo la humillación, intimidación, acoso y perjudicar hacia la persona.

Según el portal de ciberseguridad Ayudaley (2021) dentro de los tipos de Doxing se encuentran el Celebrity Doxing, como se sabe gran parte de periodistas o personas fanáticas averiguan información relevante sobre la vida íntima de personas públicas o celebridades, cuyos datos son expuestos en diversas plataformas de comunicación; sin embargo, se concreta la práctica de Doxing al momento que se publican datos confidenciales de estas celebridades como son sus correos, tarjetas de crédito/debito, seguro sociales, teléfono personal, etc. Doxing defectuoso, se basa cuando existe una equivocación al momento de investigar a una determinada persona por parte del criminal, generándose erróneamente perdida de reputación, empleo, acosos, daños físicos, etc., de una persona que no es pública. Revenge Doxing, se basa en una acción de venganza por parte de un individuo hacia otro con el propósito de causar vergüenza o humillación, por lo general se emplea para desenmascarar a otros criminales que practican Doxing. Crimen Doxing, en general se emplea para fines de homicidio o asesinato, ya que el propósito es brindar información privada de los criminales para que se cometan daños físicos, por lo general se exponen fotos, direcciones, etc.

Respecto a los delitos informáticos, según la definición de Mayer y Oliver (2020) los delitos informáticos se refieren a todas aquellas acciones de índole ilegal, delictivas, antiética o no autorizada mediante el cual se hace el empleo de dispositivos electrónicos empleando la internet, con el objetivo de lograr una vulneración del sistema a fin de recoger información clasificada o causar algún daño patrimonial de una persona o entidad pública o privada.

En relación a Acosta et al. (2020) definen a los delitos informáticos como el conglomerado de acciones que generan delitos penales, y mediante el cual debe ser tratado de manera legal debido a que tiene por objetivo el generar daño hacia un tercero, generando algún tipo de lesión y/o, la perdida de algún bien jurídico, asimismo, confirma que este tipo de situaciones se desarrollan directamente desde el ciberespacio.

En relación a Mayer et al. (2020) manifiestan que el delito informático abarca diferentes

comportamientos delictivos, ilegal, antiético o no autorizado empleándose algún dispositivo electrónico con internet, causando una vulneración en los sistemas o plataformas digitales para adquirir de manera ilegal información o dañar patrimonio.

Según lo define Saltos et al. (2021) los delitos informáticos engloban una amplia gama de actividades denominadas ilegales utilizando diversas herramientas tecnológicas, teniendo en cuenta el empleo de TICs, se tiene en consideración que los sujetos que realizan estas acciones tienen suficiente experiencia en TICs, facilitándoles el fácil acceso a la información.

En relación a, Lee (2019) los delitos informáticos se refieren a cualquier comportamiento o acción ilegal cuya perpetración, investigación o acusación genera la exigencia de poseer conocimientos basados en la tecnología informática con la intención de poder hacer daño al bienestar e integridad de las víctimas y su círculo social.

Según lo definen Broadhead (2018) los delitos informáticos son aquellos actos delictivos mediante el cual se hace el empleo directo de las tecnologías informáticas para la comisión correspondiente, sea como el medio o como el principal objetivo del mismo, generando un daño potencial hacia las personas que son víctimas de estos actos.

Por otra parte, Chandra y Snowe (2020) definen a los delitos informáticos como aquellos comportamientos ilegales, realizados por la utilización de instrumentos tecnológicos con la ayuda de la internet, por la cual se vulnera y menoscaba múltiples derechos.

Según Dupont y Holt (2023) estos delitos abarcan acciones antijuridicas en las cuales se desarrollan en entornos digitales, teniendo como propósito la destrucción y daños hacia activos, etc., con la utilización de la internet.

Se tiene en consideración que no se presenta una definición concreta para referirse al delito informático que sea comprobado y aceptado por el derecho penal debido a que, la delincuencia de carácter informático abarca un conjunto de actitudes que son difíciles de conceptualizar de manera sencilla. Generalmente, se logra definir al delito informático como

aquellas acciones ilícitas que son realizadas por medio del empleo de sistemas automáticos de procesamientos de datos o de transmisión de datos.

Según lo manifiesta Hernández (2003) la informática es abarcado como la sistematización de índole racional de las informaciones. Se considera que el concepto se encuentra previsto como un comportamiento que más se acerca a una ciencia y en base a las informaciones, pero siempre abarcada en términos de sistema o sistemas. Esto quiere decir, que la sistematización de las informaciones es un fundamento primordial en la informática, en la cual se debería desarrollar de manera racional, caso contrario el empleo de los mecanismos que van desde el papel y el lápiz hasta los computadores más desarrollados, teniendo una dependencia potencial de los datos que se logren manejar para la generación de las informaciones y los procedimientos que se determinen para el procesamiento oportuno de los datos en particular.

Según Peña (2011) indica que el individuo con el objetivo de poder satisfacer sus necesidades más principales y en su anhelo de poder obtener ganancias importantes, no solo hace el empleo eficaz de los medios lícitos, sino que también hace el uso de diversos mecanismos que de manera ilegal realizan ataques a ciertos bienes jurídicos merecedores de tutela penal. Mecanismos que actualmente mantienen características más sofisticadas, en relación a las grandes ventajas que ha brindado la ciencia y la tecnología, generando de esta manera sistemas informatizados plenamente en el desarrollo oportuno de las informaciones en relación a los datos y otros aspectos similares.

El fraude informático, se encuentra relacionado a las acciones de manera deliberada e ilegítima que generen daños patrimoniales a otros individuos por medio de la, a) integración, modificación, eliminación o supresión de los datos informáticos, b) cualquier manifestación de interrupción en el desarrollo eficaz de un sistema informático (Oxman, 2013).

El Doxing, se refiere a la acción en donde se revelan informaciones de carácter identificadora de un individuo en línea, que se asocie a sus nombres reales, direcciones particulares, centro

de labores, número telefónico, datos financieros y otras informaciones de índole personal para que posteriormente sea divulgado en público sin el permiso o consentimiento de la víctima (Euan y Pinto, 2022).

El Pharming complementado al Phishing se refiere a, una clase de fraude informático que se ha presentado desde a comienzos de la década pasada, mediante el cual presenta como principal objetivo la apropiación de las informaciones personales de diferentes individuos de internet, con la finalidad de que se pueda ingresar a sus cuentas de correo o redes sociales y conseguir de manera adicional cualquier información de sus contactos virtuales, con el objetivo de que se logre la comercialización ilícita, o bien, obtener las claves del e-banking para que se logre el ingreso oportuno de la cuenta bancaria de cada titular y utilizar el dinero en las que estas se encuentran, generando operaciones de transferencia de activos a terceros en las cuales son denominados como mule (Oxman, 2013).

De acuerdo a lo mencionado por la Organización de Naciones Unidas, mediante el cual registra como delito al fraude acaecido por medio de manipulación de herramientas computacionales, asimismo, considera que el fraude puede ser ocasionado, por medio de la manipulación eficaz de las computadoras. (Bartsiotas & Achamkulangare, 2016).

Katerin (2019) añade que, en el grupo de los delitos informáticos, al sexting, mediante el cual consiste en el envío de mensajes, plenamente erótico y sexual por medio de los dispositivos móviles a través de las redes sociales o aplicaciones de mensajería instantánea. El grooming, es considerado como el delito mediante el cual realiza comportamientos y acciones empleadas por un adulto, en donde de manera anónima pretende realizar videos o imágenes a menores de edad. Se tiene también a las extorsiones, mediante el cual se define como la obligación hacia una persona empleando la violencia, amenazas e intimidaciones, con el fin de desarrollar u omitir el desarrollo de cualquier negocio jurídico con ánimos de lucrarse personalmente y originar daños al bienestar de la víctima.

El Pheraking, es considerado un delito mediante el cual consiste en el acceso a las redes

sociales empleando cuentas ajenas con la intención de que se realicen llamadas telefónicas.

Conforme a la legislación comparada, la falsificación de índole informática se encuentra fundamentado en la introducción, alteración deliberada e ilegítima de data informatica que generen informaciones no auténticas, con la autonomía de que las informaciones sean ilegibles de manera directa.

Conforme lo manifiesta la ONU, la falsificación informática se contextualiza a través de una sub clasificación: falsificaciones informáticas en donde se realiza la modificación de datos referidos de los documentos que son almacenados de manera digital. Falsificación informática como mecanismo, se desarrolla en el momento que se realizan la falsificación de documento de uso comercial teniendo en cuenta el empleo eficaz de las computadoras (Bartsiotas & Achamkulangare, 2016).

En Estados Unidos, el caso más cercano es del estado de Kentucky el cual en 2021 el senado crea la Ley Senatorial 267, también conocido como “Proyecto de Ley Anti-Doxing”, que tipifica como delito la difusión de información de identificación personal con la intención de intimidar, abusar, amenazar, acosar o asustar. Además de las posibles sanciones penales, la nueva ley también proporciona a los habitantes de Kentucky, y a sus familiares inmediatos y miembros del hogar, una causa de acción privada para recuperar sanciones potencialmente extensas, incluidos daños punitivos y honorarios de abogados, contra los divulgadores que violan la ley (Fox & Fowles, 2021).

Se tiene en consideración a la legislación francesa, mediante el cual prevé la falsificación de documentos informáticos por medio de su artículo 462-5, en donde a través de ese artículo se manifiesta la sanción a quien de cualquier modo genere la falsificación de documentos informatizados con el objetivo directo de originar algún daño perjudicial hacia la otra persona.

Analizando la legislación actual de Chile, Caro (2010) manifiesta que Chile es el principal país de Latinoamérica mediante el cual desarrolla la sanción en contra de los delitos informáticos.

Conforme lo manifiesta la Ley 19223, establecida en el Diario Oficial en junio de 1993, en donde realiza la tipificación y la sanción que se asocia en la destrucción o inutilización de los sistemas que tratan las informaciones.

A través de la ley 19223 se logra pretender la protección de nuevos bienes jurídicos que se originan a través del empleo eficaz de las tecnologías modernas, se considera también la calidad de las informaciones que se encuentran dentro de un sistema automatizado que realiza el tratamiento oportuno, como de los diferentes productos que por medio de sus operaciones se obtienen. Sin embargo, no solo se realiza la protección eficaz de tales bienes, sino que también se desarrolla hacia los patrimonios y privacidad de las informaciones de los datos y el tráfico de la norma, el derecho que se tiene en cuenta hacia las propiedades sobre las informaciones y los elementos físicos (Caro, 2010).

En Colombia, en relación a las regulaciones de los medios electrónicos establecidos en la Ley 527 (1999) manifiesta que el legislador mantiene el objetivo de brindar la adaptación de los regímenes jurídicos presentes hacia las realidades nuevas, asimismo, se originaron criterios asociados a los equivalentes funcionales. Tal criterio se logra describir de la siguiente manera: en el momento que un mensaje en particular brinda los datos pertinentes en relación al cumplimiento de las diferentes metas establecidas y manifiesta las mismas funciones que los medios tradicionales o físicos de transmisión, tales mensajes manifestaran los mismos efectos jurídicos que otros medios físicos correspondientes. A través de esto no se logra negar las consecuencias jurídicas, validez o fuerzas a tales informaciones solo porque se encuentran establecidas en forma de mensajes de datos. Se tiene en consideración que los delitos informaticos en Colombia no se encuentra descrito de manera expresa en la norma. En relación a ello, se cuenta con un artículo principal, que es el artículo n°195, mediante el cual bajo el fundamento de un abusivo acceso de un sistema informático en particular, manifiesta sanciones pertinentes sin la necesidad de que se logre la especificación de las cuantías pertinentes, para todos aquellos que se introduzcan de manera abusiva en cualquier sistema informático protegiéndose con criterios estables o que se logre mantener contra la

voluntad de quienes tienen el exclusivo derecho de excluir.

En el contexto argentino, el 4 de Junio del 2008 por medio de la Ley n°26388 (2008) se logró la modificación del código penal argentino con la intención que se incluya a los delitos informáticos sus penas respectivas, manifestándose dentro de sus contenidos temas como lo son, la distribución y tenencia pertinente con el objetivo de que se logre distribuir pornografía infantil, la violación significativa de los correos electrónicos, ingreso no legitimo a los distintos medios informáticos, perjuicios informáticos y generación de códigos maliciosos, interrupciones de las comunicaciones.

De manera posterior, el 4 de diciembre del 2013 se estableció la Ley Grooming (2013) mediante el cual la Ley n° 26904, mediante el cual realiza las respuestas necesarias hacia las diferentes necesidades para la protección a menores de edad en las comunicaciones cibernéticas, siendo de esta manera, se logró incorporar el artículo 131 en el código penal argentino, mediante el cual logra sancionar a los individuos que a través de las comunicaciones digitales, logran contactarse con otros individuos menores de edad, con el único objetivo de que se cometan diferentes delitos en contra de la integridad sexual de los mismos.

Influencia del convenio de Budapest en Perú en relación a la ciberdelincuencia trae consigo un conglomerado de beneficios significativos para los estados parte que manifestaron constancias mundiales de su consentimiento a la obligación de emplear estas herramientas mundiales. En relación a lo descrito en el pacto, se percibe los principales beneficios para los estados parte del acuerdo son los próximos (Huamán, 2020).

Manifestar políticas penales comunes con la finalidad de brindar la defensa a la sociedad; emplear mecanismos determinados en el mismo acuerdo con la finalidad de que se prevengan alteraciones a los sistemas; tener el apoyo normativo-legal instantáneo y fiable, lo que generará el fortalecimiento de las destrezas en relación a las detecciones, averiguaciones y sanciones de los estados parte para la contienda positiva contra los delitos establecidos en

los artículos del capítulo II del Acuerdo (Huamán, 2020)..

Además, diversos mecanismos infectados con software malicioso, controlados remotamente por delincuentes, utilizan páginas web con la intención de cometer actos de hostigamiento, amenazas, extorsión y difusión de información privada. También se presentan casos de fraude en línea mediante el uso de tarjetas de crédito, robo y suplantación de identidades, entre otros delitos (Huamán, 2020).

Sobre el bien jurídico, sujeto activo y sujeto pasivo, se tiene en cuenta lo mencionado por Villavicencio (2014) en relación al bien jurídico protegido con el objetivo de que se identifique el bien jurídico protegido en los delitos de índole informático, mediante el cual se desarrolla en los planos conjuntamente y de manera concatenada, en donde en el primero se desarrolla las informaciones de forma general (informaciones almacenadas, tratadas y transmitidas por medio de los sistemas.

Por medio de este delito no se considera a los datos como bienes jurídicos protegidos, debido a que es el principal y fundamental, sino a un conglomerado de bienes que son dañados, debido a las cualidades de los comportamientos típicos en estas modalidades delictivas que colisionan con diferentes intereses colectivos. Se logra coincidir con lo mencionado por Gutiérrez, mediante el cual indica que es un delito pluriofensivo, sin el daño de que de manera independiente uno de esos bienes sea tutelado por tipos penales (Villavicencio, 2014).

Los sujetos activos, en relación al delito informático no necesita características especiales para que se logren considerar como un sujeto activo, asimismo, según lo menciona Peña (2011) es suficiente con que se cuente con diversos intelectos propios de la informática para que se logre generar los comportamientos prohibidos.

Es considerado como aceptable la apreciación de una autoría mediata, en el momento que el individuo abusa de la buena fe. Se percibe que no se consideran a los sujetos activos como persona jurídica, no obstante, si se encuentra involucrado una persona jurídica, se pueden

generar consecuencias accesorias encontrándose fundamentadas en el CP art. 105° (Huamán, 2020).

Sujeto pasivo, se asocia a cualquier individuo; de acuerdo a Villavicencio (2014) el sujeto pasivo es considerado como el individuo que, dados los tráficos económicos mediante el cual se desenvuelve cada actividad, es por eso que son los sectores que reciben una mayor afectación por medio de las computadoras, y entre estos se encuentran, los bancos, entidades estatales, las industrias, entre otras.

Conforme al bien jurídico, sujeto, en el Perú la Ley N°30096 (2014) añade al delito informático en las categorías dadas en la legislación de Budapest, siendo ejecutadas de manera posterior por medio de diversos protocolos.

Lo anterior mencionado no se encuentra libre de alguna disputa correspondiente, no obstante, en términos prácticos no genera ninguna afectación al empleo futuro del Acuerdo establecido, toda circunstancia mediante el cual se realiza la discusión de los protocolos con la intención de que se logre la tipificación de los nuevos delitos en relación a los discursos de odio y la xenofobia a través de los medios informáticos.

En el Perú, no se encuentra ajeno en casos de robo de informaciones digitales, atentados al bienestar de los sistemas informáticos, delitos informativos entre otros, que van en contra del patrimonio, fraudes informáticos, delitos informáticos contra la fe pública y las suplantaciones de identidad (Ley Nº 30096, 2014).

El contexto demuestra la constancia mediante el cual estos problemas se cometen, de esta manera Andina (2018) indica que son tres las modalidades principales de delitos informáticos que complican a los usuarios y empresas peruanas, en donde se tiene en consideración al, ransomware, phishing y cryptojacking.

La infección a través de los códigos maliciosos y el empleo inadecuado de la infraestructura informática, se adapta conforme a los supuestos determinados por el artículo 3 y 4 de la Ley

30069, mediante el cual realiza la sanción de los atentados a la integridad de los datos y de los sistemas informáticos.

La privación y/o secuestro de las informaciones, se adaptan de manera directa a al supuesto descrito en art. 7 de la ley 30069, mediante el cual realiza las sanciones a las interceptaciones de los datos informáticos.

En conclusión, el delito informático en la Ley 30096 (2014) en la actualidad son los siguientes: el delito informatico, mediante el cual abarca: Artículo 2 asociado al ingreso ilegal. Toda acción mediante el cual de manera deliberada e ilegal ingresa a todo o parte de un sistema informático en particular, siempre que se pueda desarrollar por medio de la vulneración de las medidas de seguridad determinadas para su impedimento, esto será reprimido con la pena privativa de la libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días de multa. Se tiene en consideración que será reprimido con la pena similar, a todos aquellos que realizan el ingreso a un sistema informático excediendo lo que se encuentra autorizado por el reglamento.

II. MATERIALES Y MÉTODO

La presente investigación fue de tipo básico, debido a que se tuvo como propósito conocer la percepción y fundamentación teórica y conceptual de las variables como es el Doxing, teniendo como finalidad la comprensión profunda de diversos fenómenos investigados considerando el contexto complejo donde se desarrolla. Cabe señalar que su finalidad no fue medir las variables, sino interpretarlos detalladamente (Álvarez et al., 2023).

El diseño de investigación fue fundamentado; debido a que tienen el propósito de describir el problema o fenómeno que se viene presentando en un contexto determinado, por ello, se basó en recoger información relevante sobre el Doxing y su necesaria incorporación en delitos informáticos (Arias y Covinos, 2021).

Investigación con fin propositivo**,** el propósito fue proponer una solución práctica a un fenómeno o problema identificado específico. Se buscó la implementación y puesta en marcha la solución propuesta para el mejoramiento de cierta situación (Estela, 2020).

El escenario de estudio en la presente investigación fue el teórico documental, la cual se basó en recopilar y analizar información como son conceptos, características, jurisprudencias, antecedentes, conceptos, legislación comparada, etc., que expliquen el problema actual de las variables investigadas.

Las caracterizaciones de cada sujeto en los estudios cualitativos hacen referencia a procesos de identificación y descripción de cualidades de una persona o grupo de personas que son considerados como objeto de estudio; por lo tanto, los sujetos de estudio fueron aquellos que brinden información relevante sobre el fenómeno investigado, lo cual es crucial su correcta clasificación para una comprensión profunda del problema (Ñaupas et al., 2018).

En la investigación se consideró sentencias por delitos informáticos y jurisprudencia sobre delitos información asociados al Doxing y la intimidad.

La técnica utilizada fue de análisis documental la cual fue fundamental en investigaciones

cualitativas, teniendo como finalidad recopilar datos e información de fuentes fidedignas como pueden ser artículos, libros, investigaciones, sentencias, carpetas fiscales, etc., a fin de analizar a profundidad y crear una síntesis del fenómeno actual (Hernández y Mendoza, 2018).

Se aplicó como Instrumentos de recolección de datos la guía de análisis documental, la cual fue una herramienta importante por la cual se recogieron toda la información receptada a fin de dar lectura, analizar y sintetizar todos los documentos, artículos, libros, etc., sobre el fenómeno estudiado (Hernández y Mendoza, 2018).

Los procedimientos sobre el análisis documental abarcaron diferentes pasos relevantes para su correcta interpretación y exposición, iniciando con la selección de las fuentes de información, enfocándose con la selección de fuentes bibliográficas importantes alineadas a la investigación como son los artículos indexados en plataformas científicas, jurisprudencias, legislación comparada, libros, documentación oficial, etc. La revisión y organización de la información, se empleó después de haber recogido la información y datos, se procedió a filtrar la información más relevante a fin de organizarla y exponerla de manera sistematizada y ordenada; En el análisis de los datos se transcribirán todos los datos recogidos por el análisis documental. clasificándolos por relevancia para la construcción de la narrativa del Doxing y delitos informáticos en Perú.

Por otro lado, en la interpretación de los datos se identificaron los aportes más relevantes de la revisión documentaria para poder extraer la información precisa que responda a los objetivos planteados.

Se consideraron aspectos estipulados por los artículos de la universidad USS S.A.C., a la vez el Reporte Belmont. Asimismo, se consideró manifestado por Aguilar et al (2023), el cual menciona que las investigaciones cualitativas jurídicas deben tomar en cuenta los siguientes: Consentimiento informado, confidencialidad, protección de los derechos y justicia.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

3.1.1 Naturaleza del Doxing y su afectación al derecho a la intimidad.

El Doxing, según Zulfahmi et al. (2023) se encuentra relacionado al conjunto de acciones mediante el cual se recopila y se publican informaciones personales de algún individuo o de un grupo en particular sin el consentimiento previamente debido, con el principal objetivo de hacer daño a la trayectoria pública o profesional de la víctima, asimismo, mencionan que esta práctica no solamente afecta a la víctima sino también sus familiares y amigos más cercanos se ven afectados.

Según la Comisión Interamericana de Derechos Humanos (2023) considera que el ejercicio de la crítica a una persona y/o celebridad no abusen o vulneres derechos fundamentales, por lo tanto, el doxing y las amenazas pueden provocar una autocensura significativa que limita la libertad de expresión y afecta negativamente el debate público. Asimismo, la Comisión señala que los comportamientos inauténticos y coordinados en redes sociales no necesariamente reflejan un verdadero debate ciudadano y democrático. Por lo tanto, es crucial diferenciar, cuando sea aplicable, entre la crítica ciudadana legítima y las acciones intencionales que buscan promover posiciones perjudiciales mediante comportamientos inauténticos y coordinados.

Caro (2010) manifiesta que Chile es el principal país de Latinoamérica en tomar acciones legales que regulen el uso de medios digitales y redes, mediante el cual desarrolla sanciones en contra de los delitos informáticos que se puedan generar en estas plataformas. Conforme lo manifiesta la Ley 19223, establecida en el Diario Oficial en junio de 1993, sea tipifica y sanciona la destrucción, publicación e inutilización de los sistemas que tratan las informaciones.

a) Naturaleza del Doxing

Contreras y Lovera (2021) señalan que el Doxing es considerado como una tipología de acoso cibernético mediante el cual los datos personales de un individuo, o sus quehaceres cotidianos son circulados por medio de cualquier plataforma digital o red social, asimismo, sostienen que esas informaciones de índole personal, que en situaciones incluyen el lugar donde trabajan y otros antecedentes sensibles, traen consigo diferentes perjuicios para el respeto y protección de la vida privada y honra de los individuos.

Olivero et al. (2020) señala que el Doxing se refiere a la acción de revelar las informaciones personales de algún individuo en línea, se le considera como una tipología de ciberacoso que involucra la revelación de datos personales de las víctimas como lo son el nombre personal, dirección, trabajo u otras informaciones confidenciales sin el consentimiento de la persona, asimismo, sostienen que el Doxing tiene como principal objetivo humillar, intimidar, acosar o perjudicar a la víctima.

Como lo menciona García (2021) el Doxing se refiere a la práctica que realizan ciertos individuos con intenciones negativas en las cuales consiste en la publicación, mayormente de manera digital, de informaciones personales de sus víctimas con la finalidad de avergonzar o intimidar.

En relación a Kelley y Weaver (2020) el Doxing es el conjunto de acciones maliciosas mediante el cual unos individuos recopilan y comparten informaciones digitales de índole personal de diferentes personas sin el consentimiento debido para su difusión con la única intención de desprestigiar y hacer daño, afectando considerablemente su bienestar como el de su familia y amigos más cercanos.

Romani (2021) señala que el Doxing se basa en revelar diversas informaciones personales de algún individuo en línea, que se encuentre relacionado sus nombres reales, dirección particular, datos financieros, entre otras informaciones

personales, en donde posteriormente estas informaciones son divulgadas al público sin el consentimiento ni el permiso de la víctima, afectando su bienestar y dignidad.

Conforme lo menciona Porcedda (2023) el Doxing se relaciona de manera directa en la acción de revelar datos personales de alguna persona en particular de manera digital, asimismo, se le considera una tipología de ciberacoso que involucra a la revelación considerable de informaciones personales, como lo es el nombre real del individuo, su dirección de hogar u otros datos sin el consentimiento de la víctima, mediante el cual tiene como principal objetivo la humillación, intimidación, acoso y perjudicar hacia la persona.

b) Derecho a la intimidad

El derecho a la intimidad asegura el respeto y la protección de la vida personal y familiar de los ciudadanos, además de la confidencialidad de las comunicaciones, conforme a lo dispuesto en la Ley N.º 30096 (2014). El artículo 2, inciso siete, de la Constitución del Perú, establece que toda persona tiene derecho a la intimidad, lo que implica una protección legal para su vida privada, familiar y el secreto de sus comunicaciones. Así, el derecho a la intimidad ayuda a

b.1) Propósito y alcance del derecho a la intimidad

El derecho a la intimidad resguarda a las personas, permitiéndoles tener un espacio privado donde puedan desarrollar su personalidad libremente según sus propias convicciones (Ley N.º 30096, 2014). Desde esta perspectiva, la intimidad incluye la esfera personal y reservada de cada individuo, como su residencia, creencias, orientación sexual, afinidades políticas o culturales, entre otros aspectos. Esta protección legal se refleja en el artículo 18 de la Constitución del Perú, que reconoce el derecho de toda persona a mantener en reserva sus convicciones ideológicas, religiosas o de cualquier otro tipo.

b.2) Transgresión al derecho a la intimidad

Quienes infrinjan el derecho a la intimidad de otros serán castigados con pena privativa de libertad, de acuerdo con el artículo 154 del Código Penal. Este artículo señala que la pena puede ser de uno a tres años si una persona revela la intimidad de otro sin su consentimiento, además de una multa de treinta a ciento veinte días. Si se emplea un medio de comunicación social para divulgar la vida íntima de alguien, la pena será de dos a cuatro años y la multa oscilará entre sesenta y ciento ochenta días. Por último, el artículo 156 del Código Penal regula la divulgación de la intimidad personal y familiar, estableciendo una pena privativa de libertad no mayor a un año para quien divulgue información privada sobre otra persona..

3.1.2 Carencia de la regulación del Doxing frente a los delitos informáticos

El Perú en materias de normativas asociadas a los delitos informáticos no se encuentra actualizado, dado que, la última modificación del código penal para agregar las nuevas formas de vulneración de derechos por plataformas digitales fue en el año 2014, por ello, se puede afirmar que la ley cuenta con vacíos legales en casos de ciberdelincuencia.

a) El delito del Doxing en la legislación extranjera

El Doxing es un delito que se encuentra penado solo en determinados países a nivel mundial, el caso más cercano es del estado de Kentucky el cual en 2021 el senado crea la Ley Senatorial 267, también conocido como “Proyecto de Ley Anti-Doxing”, que tipifica como delito la difusión de información de identificación personal con la intención de intimidar, abusar, amenazar, acosar o asustar. Además de las posibles sanciones penales, la nueva ley también proporciona a los habitantes de Kentucky, y a sus familiares inmediatos y miembros del hogar, una causa de acción privada para recuperar sanciones potencialmente extensas, incluidos daños punitivos y honorarios de abogados, contra los divulgadores que

violan la ley (Fox & Fowles, 2021).

Asimismo, Gregory (2021) menciona que otros países que sanciona la práctica del Doxing es China, y Europa por medio del RGPD (Reglamento General de Protección de Datos).

3.1.3 Necesidad de regular el Doxing a través de la legislación comparada

La ley de fraude y abuso informático de los EE.UU. penaliza a quienes acceden a computadoras sin autorización o eluden los controles de acceso con fines maliciosos o para beneficio personal. Según la gravedad del delito, las sanciones pueden incluir multas de hasta 500.000 USD y largas penas de prisión. Así que es esencial reconocer que actividades como el acceso no autorizado a bases de datos o el uso de software malicioso para comprometer redes protegidas están severamente prohibidas y pueden conllevar graves consecuencias legales para los infractores (Caseguard, 2022).

En Europa, el RGPD (Reglamento General de Protección de Datos) otorga a las personas derechos sobre sus datos personales y regula cómo las empresas deben recopilar, almacenar, procesar, utilizar, compartir, eliminar, transferir y manejar esta información. Las organizaciones que violen estas regulaciones pueden enfrentar multas de hasta 20 millones de euros o el 4% de sus ingresos anuales, según cuál sea mayor (Gregory, 2021).

En el contexto chino, específicamente de Hong Kong en el 2021 reformuló su código penal cuyo fin es penalizar a los infractores que revelen datos personales sin consentimiento, con la intención de causar daño psicológico, es ahora un delito penal en Hong Kong que puede castigarse con una multa de hasta 1 millón de dólares de Hong Kong y cinco años de cárcel. La legislación tiene un efecto extraterritorial, ya que el comisionado de privacidad puede enviar un aviso a los proveedores de servicios de Internet, tanto con sede en Hong Kong como fuera

de la ciudad, para que eliminen información que las autoridades consideren Doxing dentro de un plazo designado. La legislación fue propuesta luego de un aumento en los casos de Doxing durante los meses de protestas contra el proyecto de ley de extradición (BBC Nws Mundo, 2021).

El organismo de control de la privacidad dijo que se registraron más de 5.700 quejas entre junio de 2019 y abril de este año, involucrando a agentes de policía y sus familiares, así como a partidarios del gobierno y la fuerza. Los periodistas también fueron blanco de Doxing, y muchas de las víctimas eran ex empleados del ya desaparecido periódico Apple Daily y de la emisora pública RTHK (Ho, 2021).

3.2. Discusión

Considerando el **primer objetivo específico** sobre el análisis de la naturaleza del Doxing y su afectación al derecho a la intimidad, se pudo reconocer que el Doxing es considerado como una tipología de acoso cibernético mediante el cual los datos personales de un individuo, o sus quehaceres cotidianos son circulados por medio de cualquier plataforma digital o red social, asimismo, sostienen que esas informaciones de índole personal, que en situaciones incluyen el lugar donde trabajan y otros antecedentes sensibles, traen consigo diferentes perjuicios para el respeto y protección de la vida privada y honra de los individuos.

Por su parte, Olivero et al. (2020) señala que el Doxing se refiere a la acción de revelar las informaciones personales de algún individuo en línea, se le considera como una tipología de ciberacoso que involucra la revelación de datos personales de las víctimas como lo son el nombre personal, dirección, trabajo u otras informaciones confidenciales sin el consentimiento de la persona, asimismo, sostienen que el Doxing tiene como principal objetivo humillar, intimidar, acosar o perjudicar a la víctima.

Los resultados encontrados coinciden con lo manifestado por García. (2021) el cual investigó sobre las nuevas modalidades de robo de información afectando la intimidad de las personas, en la cual precisó que el Doxing es un problema social que no solo se centra en vulnerar la privacidad de las personas, sino que, se utiliza para otros fines como es la vulneración de información sensible de instituciones públicas, siendo muy necesaria su regulación en los sistemas jurídicos.

Por lo tanto, se puede identificar que el papel que tienen las plataformas virtuales son muy beneficiosas ya que ayudan en el proceso de comunicación de las personas, sin embargo, existen delitos no contemplados en las leyes como el Doxing que vulnera el derecho a la honra e intimidad, ya que el vacío legal no permite monitorear, controlar y juzgar a aquellas personas que vulneran los derechos de las personas mencionados, por lo tanto, es urgente el diseño de propuestas que puedan sancionar este tipo de actos.

Considerando el **segundo objetivo específico** sobre la falta de regulación del Doxing que incide en los delitos informáticos, se pudo identificar que el Perú en materias de normativas asociadas a los delitos informáticos no se encuentra actualizado, dado que, la última modificación del código penal para agregar las nuevas formas de vulneración de derechos por plataformas digitales fue en el año 2014, por ello, se puede afirmar que la ley cuenta con vacíos legales en casos de ciberdelincuencia.

Asimismo, el Doxing es un delito que se encuentra penado solo en determinados países a nivel mundial, el caso más cercano es del estado de Kentucky el cual en 2021 el senado crea la Ley Senatorial 267, también conocido como “Proyecto de Ley Anti-Doxing”, que tipifica como delito la difusión de información de

identificación personal con la intención de intimidar, abusar, amenazar, acosar o asustar. Además de las posibles sanciones penales, la nueva ley también proporciona a los habitantes de Kentucky, y a sus familiares inmediatos y miembros del hogar, una causa de acción privada para recuperar sanciones potencialmente extensas, incluidos daños punitivos y honorarios de abogados, contra los divulgadores que violan la ley (Fox & Fowles, 2021).

Considerando lo mencionado por el autor, el Doxing viene siendo penado ya hace varios años por la vulneración de derechos que presenta, como es la difusión de información de identificación personal con la intención de intimidar, abusar, amenazar, acosar o asustar, es necesaria la incorporación entonces en la realidad peruana debido a que la última modificación del código penal para agregar las nuevas formas de vulneración de derechos por plataformas digitales fue en el año 2014, por ello, se puede afirmar que la ley cuenta con vacíos legales en casos de ciberdelincuencia.

Se coincide con el estudio de Rodríguez & Rodríguez (2021), el cual por medio de su investigación pudo reconocer que la falta de regulación del Doxing trae consigo que se vulneren derechos fundamentales, a la vez, se dan a conocer la problemática que se viene viviendo en el plano latinoamericano respecto al Doxing, lo cual es una práctica que causa intimidación, ansiedad, daño psicológico, etc., por ello, menciona las formas de violencia para visibilizarlas, prevenirlas y atender rápidamente.

Se confirma la relación con el estudio de Ananías & Vergara (2019), quienes mencionan que la falta de medidas preventiva del Doxing permiten que los activistas y defensores de derechos sufran de acoso y divulgación de sus datos personales, trayendo consigo un potencial riesgo para su integridad física y psicológica; recalcando que es necesario la pronta regulación de las nuevas

formas de acoso y robo de información en la legislación chilena.

Por lo tanto, la necesidad de incorporar la norma surge debido a que en la actualidad en el plano nacional el Doxing viene siendo un problema social debido a que se viene utilizando más seguido para acosar, intimidar, chantajear, publicar información personal sin autorización previa de las víctimas, o hasta información falseada; por lo cual, es relevante su incorporación a los delitos informáticos.

Con respecto al **tercer objetivo específico** sobre la necesidad de la regulación del Doxing a través de la legislación comparada, se pudo identificar que las nuevas directivas de protección de información personal, como el Reglamento General de Protección de Datos (GDPR) de los Estados Unidos y la Ley General de Protección de Datos de Brasil (LGPD), así como el mayor escrutinio de los consumidores ante la administración de sus datos, han obligado a las organizaciones a mejorar sus políticas de seguridad y tomar con más seriedad las filtraciones de datos.

La ley de fraude y abuso informático de los EE.UU. penaliza a quienes acceden a computadoras sin autorización o eluden los controles de acceso con fines maliciosos o para beneficio personal. Según la gravedad del delito, las sanciones pueden incluir multas de hasta 500.000 USD y largas penas de prisión. Así que es esencial reconocer que actividades como el acceso no autorizado a bases de datos o el uso de software malicioso para comprometer redes protegidas están severamente prohibidas y pueden conllevar graves consecuencias legales para los infractores (Caseguard, 2022).

En Europa, el RGPD (Reglamento General de Protección de Datos) otorga a las personas derechos sobre sus datos personales y regula cómo las empresas deben recopilar, almacenar, procesar, utilizar, compartir, eliminar, transferir y manejar esta información. Las organizaciones que violen estas regulaciones pueden enfrentar multas de hasta 20 millones de euros o el 4% de sus ingresos anuales,

según cuál sea mayor (Gregory, 2021).

Por último, también se coincide con el estudio de Romani (2021) el cual menciona que la falta de normativas efectivas contra el Doxing permite que se vulnere el derecho a la privacidad de las personas, desencadenando una serie de problemas que abarca dese el hostigamiento hasta las amenazas.

De acuerdo a la revisión sistemática de información y antecedentes se sustenta entonces la necesidad de regular el Doxing en el Perú mediante la incorporación de una norma para evitar que se sigan vulnerando determinados derechos como es la intimidad, así como se viene regulando en EE.UU., China, La Unión Europea, etc.

Respecto al **objetivo general** sobre la incorporación del Doxing como delito informático en la Ley 30096 para proteger el derecho a la intimidad.

Se encontró que muchos países han vivido la problemática asociada al Doxing, por lo tanto, es importante que se tomen medidas preventivas legales para salvaguardar el derecho a la intimidad como lo vienen desarrollando diversos países a nivel mundial ya que están reforzando sus políticas para proteger los datos personales y algunos gobiernos incluso están imponiendo nuevas directivas para garantizar la protección de los datos de sus ciudadanos y penalizar su administración irresponsable.

Las consecuencias del Doxing en las personas agraviadas son diversas, sin embargo, a la gran mayoría pueden causarle niveles elevados de ansiedad, insomnio, estrés, miedo, en periodos de corto, mediano y largo plazo, hasta llegar al punto de esconderse de la sociedad por la vergüenza que pudieron haber desarrollado con la exposición de los datos.

Proyecto de Ley

a. **<u>Sumilla: Ley que adiciona y modifica el artículo 7 de la Ley N°30096 Ley de delitos informáticos</u>**

1. Identidad del autor

La autora Puican Ordoñez Ana Lucía estudiante de la Escuela de Derecho de la Universidad Señor de Sipán ejerciendo el Derecho de iniciativa legislativa que le confiere el Artículo 107° de la Constitución Política del Perú, presenta el siguiente:

2. Exposición de motivos

La Constitución Política, en su Artículo 107°, en su segundo párrafo, señala tácitamente que cualquier persona puede realizar iniciativas o propuestas legislativas con respecto a las normas.

Teniendo en cuenta la constitucionalidad de las facultades a los ciudadanos para realizar propuestas a fin que el poder legislativo tengo en consideración su implementación en la norma.

Siendo así, se necesita modificar el art. 7 de La ley N°30096 de la Ley de delitos informáticos, en donde se regulan los presupuestos a considerar para la aplicación de la interceptación de datos académicos, de esta norma se sustentan los procesos penales por delitos informáticos, donde muchas veces quedan impunes los delitos por falta de tipificación objetiva de la norma.

La norma procesal que regula la interceptación de datos informáticos no es objetiva y hace falta complementar el articulo 7 en la cual será el sustento de futuros delitos informáticos.

Las estadísticas han demostrado que, en el Perú, no existen procesos penales que se puedan imputar por el delito del Doxing, siendo necesario que se regule los actos delictivos que utilizan, perjudicando la dignidad de las personas, siendo necesario modificar la norma procesal penal y tipificar criterios objetivos que deberán

ser valorados en un juicio penal.

3. ANALISIS DEL COSTO BENEFICIO

La propuesta legislativa que formulamos, no irroga mayores gastos al erario nacional; más bien, de concretarse habrá de contribuir al mejoramiento de la administración de justicia, debido a que se podrá tipificar otros tipos de actos delictivos en la interceptación de datos informáticos.

4. Fórmula legal

“Ley que adiciona y modifica el artículo 7 de la Ley N°30096

ARTÍCULO 1. Modifíquese el artículo **7 de la Ley N°30096**

Antiguo artículo: “El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas (…)”.

Nuevo artículo: Artículo 7- Interceptación de datos informáticos

“El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático o redes sociales, originados en un sistema informático o efectuado dentro del mismo, incluyendo la exposición no autorizada de nombres reales, direcciones, lugar de trabajo, informes médicos, con el propósito de causar humillación, intimidación, acoso con el fin de dañar la trayectoria pública, profesional o familiar; también, emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.”

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, de contenido sexual, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.”

Si la información que transmite es falseada y perjudica la dignidad de la persona se sancionará con el máximo legal previsto en los supuestos anteriores.

ARTÍCULO 2. Deróguese los dispositivos legales que se opongan a la presente ley.

ARTÍCULO 3. La presente ley entrará en vigencia al día siguiente de su publicación en el Diario Oficial “El Peruano”.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los 01 días del mes de diciembre del 2023.

DINA ERCILIA BOLUARTE ZEGARRA

Presidente Constitucional de la República

ALBERTO OTÁROLA PEÑARANDA.

Presidente del Consejo de Ministros

FÉLIX CHERO MEDINA

Ministro de Justicia y Derechos Humanos

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. Se concluyó que el Doxing es considerado como una tipología de acoso cibernético mediante el cual los datos personales de un individuo, o sus quehaceres cotidianos son circulados por medio de cualquier plataforma digital o red social.

2. Se conoció que el Perú en materias de normativas asociadas a los delitos informáticos no se encuentra actualizado, dado que, la última modificación del código penal para agregar las nuevas formas de vulneración de derechos por plataformas digitales fue en el año 2014, por ello, se puede afirmar que la ley cuenta con vacíos legales en casos de ciberdelincuencia.

3. De acuerdo a la legislación comparada, se concluyó la necesidad de regular el Doxing como lo vienen realizando otros países como es el Reglamento General de Protección de Datos (GDPR) de los Estados Unidos y la Ley General de Protección de Datos de Brasil (LGPD) y en Europa el RGPD (Reglamento General de Protección de Datos) les otorga a los individuos derechos sobre sus datos personales.

4. Se propuso un anteproyecto para incorporar el Doxing como delito informático en la Ley 30096 específicamente en el primer párrafo del artículo 7, agregando específicamente "(…) *la exposición no autorizada de nombres reales, direcciones, lugar de trabajo, informes médicos, con el propósito de causar humillación, intimidación, acoso con el fin de dañar la trayectoria pública, profesional o familiar (…)*" a fin de proteger el derecho a la intimidad.

4.2. Recomendaciones

1. Se recomienda a los magistrados considerar al Doxing como un delito informático debido a que se ha comprobado por la legislación comparada el peligro que causa la información que circula en redes, pudiendo surgir agresiones y/o vandalismo atentando contra la vida de las víctimas.

2. Se recomienda a los fiscales establecer a los delitos asociados al Doxing como delitos informáticos y pedir penas efectivas a los magistrados, ya que mediante los resultados obtenidos se ha comprobado que se vulnera el derecho a la intimidad.

3. Se recomienda considerar la presente propuesta como una iniciativa legislativa a fin de proteger derechos fundamentales, y evitar potenciales atentados contra las víctimas de Doxing.

REFERENCIAS

Abarna, S., Sheeba, J., Jayasrilaksmi, S., & Pradeep, S. (2022). Identification of cyber harassment and intention of target users on social media platforms. *Engineering Applications of Artificial Intelligence*, 1-15. https://www.sciencedirect.com/science/article/pii/S0952197622003359

Adetunji, J. (2018). What is doxxing, and why is it so scary? *The Conversation*, 1-10. https://theconversation.com/what-is-doxxing-and-why-is-it-so-scary-95848

Ananías, C., & Vergara, K. (2019). Violencia en Internet contra feministas y otras activistas chilenas. *Artigos, 27*(3), 1-13. https://www.scielo.br/j/ref/a/XXNJ6GQQvBSpxpRpFdsncGd/?format=pdf&lang=es

Ayudaley. (8 de Julio de 2021). *¿Qué es el doxing? Con ejemplos*. https://ayudaleyprotecciondatos.es/2021/04/30/doxing/

Bartsiotas, G., & Achamkulangare, G. (2016). *Prevención y detección del fraude y respuesta a él en las organizaciones del sistema de las Naciones Unidas.* España: Naciones Unidas. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_document_files/products/es/reports-notes/JIU%20Products/JIU_REP_2016_4_Spanish.pdf

BBC Nws Mundo. (8 de Julio de 2021). *Qué es el "doxing" y por qué enfrenta a las grandes tecnológicas con el gobierno de Hong Kong.* https://www.bbc.com/mundo/noticias-57749377

Caseguard. (2022). *La Ley de Fraude y Abuso Informático de 1986.* EE.UU.: Congreso de EE.UU. https://caseguard.com/es/articles/la-ley-de-fraude-y-abuso-informatico-de-1986/

Chen, M., Yue, A., & Ling, K. (2019). Doxing: What Adolescents Look for and Their Intentions. *Int J Environ Res Public Health*, 1-16. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6352099/

Chen, Q., Ling, K., & Yue, A. (2019). Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong. *Int J Environ Res Public Health.*, 1-10.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6313484/

Cheung, A. (2021). Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon. *University of Hong Kong Faculty of Law Research Paper*, 1-10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3864766

Contreras, P., & Lovera, D. (2021). Redes sociales, funas, honor y libertad de expresión: análisis crítico de los estándares de la jurisprudencia de la Corte Suprema chilena. *Derecho PUCP, 1*(87), 345-371. http://www.scielo.org.pe/pdf/derecho/n87/0251-3420-derecho-87-345.pdf

El Peruano. (17 de 02 de 2023). Banco de la Nación alerta a sus clientes y usuarios para no ser víctimas de ciberdelincuentes. *El Peruano*, pág. 1. https://www.elperuano.pe/noticia/204818-banco-de-la-nacion-alerta-a-sus-clientes-y-usuarios-para-no-ser-victimas-de-ciberdelincuentes

García, B. (2021). El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra. *REVISTA CHILENA DE DERECHO Y TECNOLOGÍA, 10*(2), 43-68. https://www.scielo.cl/pdf/rchdt/v10n2/0719-2584-rchdt-10-2-00043.pdf

Gregory, J. (2021). How Doxing Affects Gen Z. *Security Intelligence*, 1-10. https://securityintelligence.com/articles/how-Doxing-affects-gen-z/

Grooming, L. d. (2013). *Ley 26904.* Buenos Aires: Congreso de la nación Argentina. https://www.gba.gob.ar/content/ley_26904_ley_de_grooming#:~:text=Descripcion%3A,integridad%20sexual%20de%20la%20misma.

Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del convenio de Budapest.* Cusco: Universidad Andina de Cusco. https://repositorio.uandina.edu.pe/handle/20.500.12557/4116

Jagayat, A., & Choma, B. (2021). Cyber-aggression towards women: Measurement and psychological predictors in gaming communities. *Computers in Human Behavior*, 1-10. https://www.sciencedirect.com/science/article/abs/pii/S0747563221000753

Kukul, B. (2023). Personal data and personal safety: re-examining the limits of public data in

the context of Doxing. *International Data Privacy Law*, 182-193. https://watermark.silverchair.com/ipad011.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA08wggNLBgkqhkiG9w0BBwagggM8MIIDOAIBADCCAzEGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMK5HQTqNnF8WxEXv0AgEQgIIDAkY3vwoqXRsuNwwYmv3tiRbuzdW8yxhYpLE_dFGj1CizE2N

Latto, N. (2023). ¿Qué es el doxxing? ¿Es ilegal? ¿Se puede evitar y denunciar? *Academy*, 1-3. https://www.avast.com/es-es/c-what-is-doxxing#:~:text=Es%20un%20tipo%20de%20ciberacoso,o%20perjudicar%20a%20la%20v%C3%ADctima.

Ley 26388. (2008). *Delitos informáticos.* Buenos Aires: Congreso de la nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley 527. (1999). *Reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.* Bogotá: Congreso de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=4276

Ley Nº 30096. (2014). *Ley de delitos informáticos.* Lima: Congreso de la República. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Mery, H. (2021). The dangers of Doxing and swatting: Why Texas should criminalize these malicious forms of cyberharassment. *St. Mary's Law Journal*, 1-41. https://commons.stmarytx.edu/cgi/viewcontent.cgi?article=1119&context=thestmaryslawjournal

Pichihua, S. (2023). Sepa cómo evitar ser víctima de un delito informático. *El Peruano*, 1-3. https://www.elperuano.pe/noticia/204416-sepa-como-evitar-ser-victima-de-un-delito-informatico#:~:text=En%20el%20Per%C3%BA%20se%20registran,la%20Polic%C3%ADa%20Nacional%20del%20Per%C3%BA.

Radio Programas del Perú. (10 de 02 de 2023). Apps de citas: 1 de cada 5 usuarios en el Perú fue engañado por un perfil falso. *Radio Programas del Perú*, pág. 1. https://rpp.pe/tecnologia/apps/san-valentin-1-de-cada-5-usuarios-de-apps-de-citas-

en-el-peru-fue-enganado-por-un-perfil-falso-noticia-1465854

Rodríguez, K., & Rodríguez, A. (2021). Violencia de género en instituciones de educación superior. *Revista Dilemas Contemporáneos: Educación, Política y Valores., 1*(14), 1-22. https://www.scielo.org.mx/pdf/dilemas/v8nspe1/2007-7890-dilemas-8-spe1-00014.pdf

Romani, U. (2021). Lineamientos curriculares para enfrentar el acoso en línea hacia la mujer en el marco de la responsabilidad social universitaria. *Revista redipe, 10*(1), 78-95. https://revista.redipe.org/index.php/1/article/view/1162

Rubio, C. (17 de 10 de 2023). El peligro del Doxing: tu rastro digital te puede hacer la vida imposible. *El peligro del Doxing: tu rastro digital te puede hacer la vida imposible*, pág. 1. https://www.eldebate.com/tecnologia/20231017/peligro-Doxing-rastro-digital-te-puede-hacer-vida-imposible_146664.html

Tan, A. (2023). To Dox or Not to Dox, that is The Question. *SSRN*, 1-10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4369643

Zegarra, J. (11 de 02 de 2023). Kaspersky advierte sobre el peligro de los perfiles falsos en las Apps de Citas. *IT/USERS*, pág. 1. https://itusers.today/kaspersky-advierte-sobre-el-peligro-de-los-perfiles-falsos-en-las-apps-de-citas/

ANEXOS

Anexo 1: Resolución de aprobación de proyecto de investigación

Universidad Señor de Sipán

FACULTAD DE DERECHO Y HUMANIDADES
RESOLUCIÓN N° 0003-2024/FADHU-USS

Pimentel, 19 de enero del 2024

VISTO:
El oficio N° 0022-2024/FADHU-ED-USS de fecha 19 de enero del 2024, presentado por la Escuela Profesional de Derecho, donde solicita se emita la resolución de la aprobación de los proyectos de Investigación (tesis) del CURSO-TALLER ACTUALIZACIÓN DE TESIS PARA EGRESADOS DE PREGRADO Y POSGRADO DE LA USS Y EGRESADOS DE PREGRADO DE UNIVERSIDADES CON LICENCIA DENEGADA, y;

CONSIDERANDO:
Que, la Constitución Política del Perú en su Artículo 18° establece que: "*La educación universitaria tiene como fines la formación profesional, la difusión cultural, la creación intelectual y artística y la investigación científica y tecnológica (…) Cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes.*"

Que, acorde con lo establecido en el Artículo 8° de la Ley Universitaria, Ley N° 30220, "*La autonomía inherente a las Universidades se ejerce de conformidad con lo establecido en la Constitución, la presente ley demás normativa aplicable. Esta autonomía se manifiesta en los siguientes regímenes: normativo, de gobierno, académico, administrativo y económico*". La Universidad Señor de Sipán desarrolla sus actividades dentro de su autonomía prevista en la Constitución Política del Estado y la Ley Universitaria N° 30220.

Que, acorde con lo establecido en la Ley Universitaria N°30220; indica:
- Artículo N° 6°: Fines de la Universidad, Inciso 6.5) "Realizar y promover la investigación científica, tecnológica y humanística la creación intelectual y artística".

Que, el Reglamento de Investigación de la USS Versión 8, aprobado con Resolución de Directorio N°015-2022/PD-USS, señala:

- Artículo 72°: Aprobación del tema de investigación: El Comité de Investigación de la escuela profesional eleva los temas del proyecto de investigación y del trabajo de investigación que esté acorde a las líneas de investigación institucional a Facultad para la emisión de la resolución.

- Artículo 73°: Aprobación del proyecto de investigación El (los) estudiante (s) expone ante el Comité de Investigación de la escuela profesional el proyecto de investigación para su aprobación y emisión de la resolución de facultad.

Que, Reglamento de Grados y Títulos Versión 09 aprobado con resolución de directorio N° 0120-2022/PD-USS, señala:
- Artículo 21°: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación (…).

- Artículo 24°: *"La tesis, es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela académico profesional (…)".*

- Artículo 25°: *"El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C".*

Que, visto el oficio N° 0022-2024/FADHU-ED-USS de fecha 19 de enero del 2024, en el cual se establece la procedencia para la aprobación de los proyectos de tesis del CURSO-TALLER ACTUALIZACIÓN DE TESIS PARA EGRESADOS DE PREGRADO Y POSGRADO DE LA USS Y EGRESADOS DE PREGRADO DE UNIVERSIDADES CON LICENCIA DENEGADA, de la escuela profesional de Derecho, quienes cumplen con los requisitos, por lo que se debe proceder a su inscripción respectiva, con fines de sustentación.

Estando a lo expuesto y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes.

Universidad Señor de Sipán

RESOLUCIÓN N° 0003-2024/FADHU-USS

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR los **PROYECTOS DE INVESTIGACIÓN (TESIS)** del CURSO-TALLER ACTUALIZACIÓN DE TESIS PARA EGRESADOS DE PREGRADO Y POSGRADO DE LA USS Y EGRESADOS DE PREGRADO DE UNIVERSIDADES CON LICENCIA DENEGADA de la escuela profesional de Derecho, que a continuación se detalla:

N°	APELLIDOS Y NOMBRES	PROYECTOS DE INVESTIGACIÓN
1	ALVARADO VERA CARLA DEL CARMEN	LA AMPLIACIÓN DEL PLAZO DE INVESTIGA-CIÓN PREPARATORIA EN CASOS COMPLEJOS A CAUSA DEL PROCESO DE COLABORACIÓN EFICAZ
2	CABALLERO ALFARO MANUEL EDUARDO	EL IMPACTO EN LOS PROCESOS DE CONTRATACIÓN PÚBLICA DEL PNSU ANTE LA PRESUNTA COMISIÓN DE DELITOS DE CORRUPCIÓN
3	- CHICANA GUTIERREZ KERTIN MARIANA - DE LA CRUZ GARAYAR EDWARD ALBERTO	EL CONDICIONAMIENTO AL PADRE EN LA INSCRIPCIÓN DE NACIMIENTO Y LA AFECTACIÓN AL DERECHO A LA IDENTIDAD DEL NIÑO/A
4	CHING RUIZ VELKA EUGENIA	LA ADOPCIÓN DE NIÑOS(AS) Y ADOLESCENTES, SOLICITADAS POR PERSONAS SOLTERAS PARA FORMAR UNA FAMILIA MONOPARENTAL
5	CALDAS CASTAÑEDA SONIA MONICA	LA PROTECCIÓN DEL CONSUMIDOR FRENTE AL OLVIDO ONCOLÓGICO
6	GONZA CASTILLO SANTOS IGNACIO	LA MALA ADMINISTRACIÓN DE LAS PENSIONES ALIMENTICIAS COMO FORMA DE VIOLENCIA ECONÓMICA
7	LAZARO QUISPE ALEXANDER DANIEL	LA LEY 31874 FRENTE AL DEBIDO PROCESO PENAL EN LA INTERVENCIÓN DE VEHÍCULOS EN EL CONTROL DE BIENES NO FISCALIZADOS
8	NUNTON ÑIQUEN LESLY DE JESUS	PROPONER EL LÍMITE DE EDAD COMO AGRAVANTE EN EL DELITO DE INDUCCIÓN A LA FUGA DE MENOR
9	PUICAN ORDOÑEZ ANA LUCIA	EL DOXING Y SU NECESARIA INCORPORACIÓN EN LOS DELITOS INFORMÁTICOS
10	REBOLLEDO MORE MANUEL JESÚS	LA TUTELA DE DERECHOS Y SU PLAZO FRENTE A LA ACUSACIÓN DIRECTA
11	SONO GOMEZ DAYANA CRISTINA	LA DISMINUCIÓN DEL PLAZO EN LA MODIFICACIÓN DE RESOLUCIONES DE TENENCIA DEL CÓDIGO DE LOS NIÑOS Y ADOLESCENTES

ARTÍCULO SEGUNDO: DISPONER que las áreas competentes tomen conocimiento de la presente resolución con la finalidad de dar las facilidades para la ejecución de la presente Investigación.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dra. Dioses Lescano Nelly
Decana de la Facultad de Derecho y Humanidades

Mg. Delgado Vega Paula Elena
Secretaria Académica Facultad de Derecho y Humanidades

Anexo 2: Acta de aprobación de asesor

Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **MG. CABRERA LEONARDINI DANIEL GUILLERMO**. quien suscribe como asesor designado mediante Resolución de Facultad N° 0192-2024/FADHU-USS, del proyecto de investigación titulado EL DOXING Y SU NECESARIA INCORPORACIÓN EN LOS DELITOS INFORMÁTICOS, desarrollado por la Bachiller : PUICAN ORDOÑEZ ANA LUCIA, del programa de estudios de Derecho , acredito haber revisado, y declaro expedito para que continue con el trámite pertinentes.

En virtud de lo antes mencionado, firman:

MG. CABRERA LEONARDINI DANIEL GUILLERMO	DNI: número 16412120	Firma 

Pimentel, 24 de abril de 2024

Anexo 3: Acta de originalidad

	ACTA DE SEGUNDO CONTROL DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN	Código:	F3.PP2-PR.02
		Versión:	02
		Fecha:	18/04/2024
		Hoja:	1 de 1

Yo, **Martha Olga Marruffo Valdivieso**, coordinadora de investigación del Programa de Estudios de derecho, he realizado el segundo control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de Pregrado según la Directiva de similitud vigente en USS; además certifico que la versión que hace entrega es la versión final del informe titulado: **EL DOXING Y SU NECESARIA INCORPORACIÓN EN LOS DELITOS INFORMÁTICOS**

Elaborado por el Bachiller **PUICAN ORDOÑEZ ANA LUCIA**

Se deja constancia que la investigación antes indicada tiene un índice de similitud del **11%**, verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN.

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación vigente.

Pimentel, 04 de setiembre de 2024

Mg. Martha Olga Marruffo Valdivieso
Coordinador de Investigación
Escuela Profesional de Derecho
DNI N° 43647439

Anexo 4: Matriz de consistencia

MATRÍZ DE CONSISTENCIA LÓGICA DE TRABAJO DE INVESTIGACIÓN					
Enfoque metodológico					
Titulo	**El Doxing y su necesaria incorporación en los delitos informáticos**				
Problema	**Hipótesis**	**Objetivo General**	**Objetivo Específico**	**Tipo de Investigación**	**Diseño de Investigación**
¿De qué manera el Doxing afecta el derecho a la intimidad?	Si se incorpora el Doxing como delito informático en la Ley 30096 entonces se protegerá el derecho a la intimidad	Incorporar el Doxing como delito informático en la Ley 30096 para proteger el derecho a la intimidad	a) Examinar la naturaleza del Doxing y su afectación al derecho a la intimidad b) Determinar si la falta de regulación del Doxing incide en los delitos informáticos c) Analizar la necesidad de regular el Doxing atraves de la legislación comparada	cualitativo	Diseño: analítico - descriptivo