Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

Tráfico ilegal de datos: necesidad de reforma del Código Penal peruano

Jadir Santos Yave Villar Feria

Para optar el Título Profesional de Abogado

Lima, 2024

Universidad Continental

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TESIS

A	:	Eliana Carmen Mory Arciniega. Decana de la Facultad de Derecho
DE	:	Gabriel Ravelo Franco Asesor de tesis
ASUNTO	:	Remito resultado de evaluación de originalidad de tesis
FECHA	:	29 de enero de 2024

Con sumo agrado me dirijo a vuestro despacho para saludarla y en vista de haber sido designado asesor de la tesis titulada: "Tráfico ilegal de datos: necesidad de reforma del Código Penal Peruano ", perteneciente al bachiller Jadir Santos Yave Villar Feria, de la E.A.P. de Derecho; se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 17% de similitud (informe adjunto) sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión bibliografía — SI [X] NO [ ]
- Filtro de exclusión de grupos de palabras menores (Nº de palabras excluidas: 15) — SI [X] NO [ ]
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [ ] NO [x]

En consecuencia, se determina que la tesis constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad.

Recae toda responsabilidad del contenido de la tesis sobre el autor y sobre el asesor recae la responsabilidad sobre el proceso de asesoría, en concordancia a los principios de legalidad, presunción de veracidad y simplicidad, expresados en el Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales – RENATI y en la Directiva 003-2016-R/UC.

Esperando la atención a la presente, me despido sin otro particular y sea propicia la ocasión para renovar las muestras de mi especial consideración.

Atentamente,

La firma del asesor obra en el archivo original
(no se muestra en este documento por estar expuesto a publicación)

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, JADIR SANTOS YAVE VILLAR FERIA, identificado(a) con Documento Nacional de Identidad No. 70756503, de la E.A.P. de Derecho de la Facultad de Derecho la Universidad Continental, declaro bajo juramento lo siguiente:

1. La tesis titulada: "TRÁFICO ILEGAL DE DATOS: NECESIDAD DE REFORMA DEL CÓDIGO PENAL PERUANO", es de mi autoría, la misma que presento para optar el Título Profesional de Abogado.
2. La tesis no ha sido plagiada ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas, por lo que no atenta contra derechos de terceros.
3. La tesis es original e inédita, y no ha sido realizado, desarrollado o publicado, parcial ni totalmente, por terceras personas naturales o jurídicas. No incurre en autoplagio; es decir, no fue publicado ni presentado de manera previa para conseguir algún grado académico o título profesional.
4. Los datos presentados en los resultados son reales, pues no son falsos, duplicados, ni copiados, por consiguiente, constituyen un aporte significativo para la realidad estudiada.

De identificarse fraude, falsificación de datos, plagio, información sin cita de autores, uso ilegal de información ajena, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

16 de enero de 2024.

La firma del autor obra en el archivo original
(no se muestra en este documento por estar expuesto a publicación)

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

Tesis Jadir Vilar

ORIGINALITY REPORT

17%	17%	3%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repositorio.ucv.edu.pe Internet Source	3%
2	hdl.handle.net Internet Source	2%
3	www.defensoria.gob.pe Internet Source	1%
4	cerac.unlpam.edu.ar Internet Source	1%
5	Submitted to Pontificia Universidad Catolica del Peru Student Paper	1%
6	repositorio.upn.edu.pe Internet Source	1%
7	www.coe.int Internet Source	<1%
8	www.informatica-juridica.com Internet Source	<1%
9	www.dspace.uce.edu.ec Internet Source	<1%

10	archive.org Internet Source	<1 %
11	documentop.com Internet Source	<1 %
12	qdoc.tips Internet Source	<1 %
13	issuu.com Internet Source	<1 %
14	blog.pucp.edu.pe Internet Source	<1 %
15	www.unodc.org Internet Source	<1 %
16	repositorio.uns.edu.pe Internet Source	<1 %
17	derecho-ntic.blogspot.com Internet Source	<1 %
18	www.repositorio.upla.edu.pe Internet Source	<1 %
19	revistas.pucp.edu.pe Internet Source	<1 %
20	1library.co Internet Source	<1 %
21	infotec.repositorioinstitucional.mx Internet Source	<1 %

22	www.dspace.uce.edu.ec:8080 Internet Source	<1 %
23	www.camara.cl Internet Source	<1 %
24	rchdt.uchile.cl Internet Source	<1 %
25	repositorio.upao.edu.pe Internet Source	<1 %
26	Submitted to ipn Student Paper	<1 %
27	Submitted to Universidad Tecnologica del Peru Student Paper	<1 %
28	"Nueva ley de datos personales para Chile : proyecto de ley para la modernización normativa en la protección de datos personales en Chile : análisis evaluativo y desafíos", Pontificia Universidad Catolica de Chile, 2020 Publication	<1 %
29	idoc.pub Internet Source	<1 %
30	derechojusticiasociedad.blogspot.com Internet Source	<1 %
31	es.slideshare.net Internet Source	

		<1 %
32	www.carey.cl Internet Source	<1 %
33	Submitted to Universidad Continental Student Paper	<1 %
34	derechodelared.com Internet Source	<1 %
35	repositorio.unjbg.edu.pe Internet Source	<1 %
36	Submitted to Universidad Nacional de Educación Student Paper	<1 %
37	dspace.unl.edu.ec Internet Source	<1 %
38	repositorio.unfv.edu.pe Internet Source	<1 %
39	repositorio.unp.edu.pe Internet Source	<1 %
40	Law Governance and Technology Series, 2014. Publication	<1 %
41	Submitted to Universidad Cesar Vallejo Student Paper	<1 %

42	intranet.uwiener.edu.pe Internet Source	<1 %
43	dokumen.pub Internet Source	<1 %
44	(11-22-02) http://148.244.220.100/latam/prensa/2000/ene/Interne Internet Source	<1 %
45	Gabriela Rosas-Lanas, Geoconda Pila-Cárdenas. "protección de datos personales en Ecuador", VISUAL REVIEW. International Visual Culture Review / Revista Internacional de Cultura Visual, 2023 Publication	<1 %
46	anuarioderechoprivado.uniandes.edu.co Internet Source	<1 %
47	negociosyautos.wordpress.com Internet Source	<1 %
48	ifai.org.mx Internet Source	<1 %
49	repositorio.uap.edu.pe Internet Source	<1 %
50	repositorio.unsa.edu.pe Internet Source	<1 %
51	www.rose-systemtechnik.com Internet Source	<1 %

52	es.scribd.com Internet Source	<1%
53	repositorio.unc.edu.pe Internet Source	<1%
54	www.coursehero.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	< 15 words
Exclude bibliography	On		

Dedicatoria

A Dios.

A mis padres, a quienes he visto trabajar desde que tengo uso de razón. Incluso cuando el empleo se acabó, ellos crearon el suyo para que la educación, el vestido y la alimentación nunca fueran carencias en casa. A mis hermanos, por sus palabras; ellos dicen admirarme, pero soy yo quien aprende constantemente de ellos. A mi abuela, a quien los años le otorgaron sabiduría para brindar las mejores palabras y consejos que he tenido el privilegio de escuchar.

Agradecimiento

A mis maestros, porque la docencia no solo se reduce a una cátedra. Se puede transformar vidas desde el Derecho. Gracias a todos aquellos docentes que, después de finalizar un ciclo, me brindaron palabras, ánimo y aliento para seguir continuando en esta carrera.

A mis padres, quienes, junto conmigo, son artífices de todo esto.

Finalmente, a cada institución y persona que, de una forma u otra, contribuyó a mi vida académica y profesional.

Resumen

El delito de tráfico de datos personales, en el contexto del tráfico ilegal de datos, es una preocupación legal creciente en la era digital. Este delito se centra en la obtención, venta, intercambio o uso no autorizado de datos personales de individuos, lo que constituye una grave violación de la privacidad y seguridad de las personas. El bien jurídico protegido por este delito es la intimidad (es de tipo instantáneo, común, de peligro y de mera actividad) y la confidencialidad de la información personal de los individuos. Es importante destacar que el desarrollo de leyes específicas para abordar el tráfico ilegal de datos personales, como en el caso de la Ley N°27309-2000 y su incorporación posterior en la Ley N°30096 (2013), refleja el reconocimiento por parte del legislador de la necesidad de adaptar la legislación penal a los desafíos y realidades de la era digital. En la legislación nacional no se contemplan cibercrímenes, sino ciberdelitos. La inclusión de este delito en la ley de delitos informáticos es coherente con la importancia que ha cobrado la protección de datos en el entorno tecnológico actual. Esta modificación legislativa y la creación de un delito informático indican una respuesta legislativa a la evolución de la tecnología y a los riesgos asociados con el uso indebido de datos personales en línea. El enfoque en la privacidad y protección de datos muestra la importancia de salvaguardar la información personal en un mundo cada vez más interconectado y digitalizado.

Palabras clave: protección de datos, datos personales, modificación normativa.

Abstract

The crime of trafficking in personal data, in the context of illegal data trafficking, is a growing legal concern in the digital age. This crime focuses on the unauthorized obtaining, sale, exchange or use of personal data of individuals, which constitutes a serious violation of people's privacy and security. The legal good protected by this crime is the privacy and confidentiality of the personal information of individuals. It is important to highlight that the development of specific laws to address the illegal trafficking of personal data, as in the case of Law No. 27309-2000 and its subsequent incorporation in Law No. 30096 (2013), reflects the recognition by the legislator of the need to adapt criminal legislation to the challenges and realities of the digital age. The inclusion of this crime in the cybercrime law is consistent with the growing importance of data protection in today's technological environment. This legislative change and the creation of a cybercrime indicate a legislative response to the evolution of technology and the risks associated with the misuse of personal data online. The focus on privacy and data protection highlights the importance of safeguarding personal information in an increasingly interconnected and digitalized world.

Keywords: data protection, personal data, regulatory modification.

Índice de Contenido

Dedicatoria ... ii
Agradecimiento ... iii
Resumen ... iv
Abstract ... v
Introducción ... 1
Capítulo 1: Planteamiento del Estudio ... 4
1.1 Tema de Investigación Delimitado ... 4
1.2 Justificación ... 11
1.2.1 Justificación práctica ... 11
1.2.2 Justificación legal ... 11
1.3 Planteamiento del problema ... 12
1.3.1 Problema general ... 12
1.3.2. Problemas específicos ... 12
1.4. Objetivos ... 13
1.4.1. Objetivo General ... 13
1.4.2. Objetivos específicos ... 13
Capítulo 2: Marco Teórico ... 14
2.1 Investigaciones Previas ... 14
2.1.1 Antecedentes Internacionales ... 14
2.1.2 Antecedentes Nacionales ... 15
2.2. Bases Teóricas ... 18
2.2.1 Desarrollo de los Delitos Informáticos ... 18
2.2.2 Tráfico Ilegal de Datos Personales ... 20
2.2.3 Tipificación del Delito de Tráfico Ilegal de Datos Personales ... 20
2.2.4 Teorías Específicas ... 21
2.3 Definición de Términos ... 22
2.4 Categorías de Análisis ... 24
Capítulo 3: Metodología ... 25
3.1 Explicación y Justificación del Tipo de Investigación Elegido ... 25

3.2. Población o Sujeto o Casos 25
3.3 Técnicas de Recojo de la Información 25
3.4 Instrumento de Recolección de Datos 26
3.5 Estrategias de Análisis de la Información 27
Capítulo 4: Resultados y Discusión 28
4.1. Resultados 28
4.2. Discusión 39
Conclusiones 51
Recomendaciones 53
Referencias 55

Lista de Tablas

Tabla 1 Comparación en función de los objetivos 29
Tabla 2 Comparación en función de la metodología 30
Tabla 3 Comparación en función al bien jurídico 32
Tabla 4 Comparación en función a los elementos típicos 34
Tabla 5 Comparación en función a las conclusiones 36
Tabla 6 Comparación en función de las recomendaciones 39

Introducción

El tráfico ilegal es un problema al que se enfrentan los usuarios de internet. Se refiere a la venta, compra o intercambio de información personal o privada sin contar con la autorización correspondiente. Este delito es una preocupación global, ya que los ciberdelincuentes pueden obtener información valiosa y confidencial, como dígitos de direcciones de correo electrónico, tarjetas de crédito, contraseñas y cualquier otro dato adicional.

En el Perú, el tráfico ilegal de datos personales es un delito contemplado en la ley penal, artículo 154-A, pero la legislación actual no está preparada para enfrentar los avances tecnológicos que vienen desarrollándose. Así, para evitar riesgos se plantea reformar el Código Penal peruano.

En las siguientes páginas se analizará el problema del tráfico ilegal de datos personales en el Perú, su repercusión en la esfera de la seguridad y la privacidad en la ciudadanía, y se planteará con ello diversas posibilidades de reforma del código penal para combatir este delito de manera más efectiva. Además, se propondrán medidas concretas que podrían implementarse para fortalecer la legislación peruana en este ámbito.

En concordancia con ello, el Perú es un país que ha experimentado, en estos tiempos, un crecimiento significativo con respecto a la incorporación de novedosas tecnologías (TIC). El aumento del uso de internet y la digitalización de los procesos empresariales y gubernamentales han generado una gigantesca cantidad de datos que se descubren en internet. Sin embargo, este contexto también ha dado lugar a nuevas formas de delitos cibernéticos.

El tráfico ilegal de datos personales en el Perú es una actividad ilícita que implica la obtención y venta de información personal o financiera, sin el consentimiento de los implicados. Este delito puede ser cometido por individuos, organizaciones criminales o grupos de *hackers*

que utilizan técnicas avanzadas para acceder a los sistemas informáticos y extraer información confidencial.

Este desarrollo investigativo se orienta a modificar el cuerpo penal del tráfico ilegal de datos regulado en la normativa penal, tomando como referencias las graves consecuencias para la privacidad y seguridad de los ciudadanos peruanos. La información obtenida por los delincuentes puede ser utilizada para cometer fraudes, estafas o extorsiones. Además, la filtración de datos privados puede generar daños y afectar la reputación de las personas, ya que la información podría ser utilizada para difamar o chantajear.

Tanto la privacidad como la seguridad de los datos conforman el bagaje de derechos reconocidos y, como tal, deben ser protegidos. Sin embargo, el comercio ilegal de datos cada vez es más frecuente y grave en todo el mundo, incluyendo el Perú. En este contexto, es fundamental que se realicen reformas al Código Penal peruano para brindar una mayor protección a los ciudadanos y combatir eficazmente este delito.

A continuación, se expondrán algunas de las razones por las cuales la reforma del Código Penal peruano es fundamental para plantear adecuadamente la problemática del tráfico ilegal de datos. La legislación peruana actual sobre el tráfico ilegal de datos es insuficiente para enfrentar las complejidades de los ilícitos cibernéticos actuales. La Ley de Delitos Informáticos, aprobada en el año 2000, define algunos delitos que guardan relación con el acceso a diferentes sistemas informáticos en la red, pero no contempla específicamente el tráfico ilegal de datos (Espinoza et al., 2018).

Así mismo, la necesidad de adaptarse a los avances tecnológicos ha permitido la evolución de este delito, adaptándose a las nuevas tecnologías y estrategias de ciberataque. Por lo tanto, es necesario que la legislación peruana se adapte y evolucione para combatir eficazmente

este tipo de delitos. La reforma del Código Penal peruano debe contemplar nuevas formas de comisión de dicho delito, como la obtención ilegal de datos a través de dispositivos móviles, la venta de datos en el mercado negro o la explotación de vulnerabilidades en las redes sociales (Villavicencio, 2014).

La reforma del Código Penal debe contemplar sanciones más gravosas para los sujetos que realicen este tipo de actuaciones, como los ataques a gran escala a empresas que manejan información sensible de los usuarios.

Por otra parte, se trata de proteger la privacidad y seguridad, ya que esta modalidad delictiva pone en riesgo los datos privados y personales. Por lo tanto, es fundamental que se tomen disposiciones a fin de proteger la privacidad y seguridad de los ciudadanos, y que se sancione de manera efectiva a los delincuentes que cometan este delito (Rodríguez, 2016).

La reforma del Código Penal peruano permitiría brindar una mayor protección a los ciudadanos frente al tráfico ilegal de datos, ya que contemplaría penas más severas para los delincuentes.

En definitiva, la exposición de esta pesquisa tiene como finalidad el análisis y la interpretación de la aplicación del tráfico ilegal de datos en la actualidad. Así mismo, clasificar los criterios de la política criminal que justifican el rango punitivo.

Capítulo 1: Planteamiento del Estudio

1.1 Tema de Investigación Delimitado

Teniendo en consideración el contexto situacional de la pandemia, se puede observar cierto impacto en la delincuencia común que se valía de esfuerzos físicos para poder perpetrar delitos contra el patrimonio, como hurto o robo, por citar algunos ejemplos. Bajo esa premisa, resulta imposible la idea de considerar que un delito común pueda efectuarse sin ese factor clave.

De esta manera, la delincuencia como fenómeno social se adaptó a las circunstancias de la nueva normalidad, que promovía un acercamiento acelerado al mundo de las tecnologías durante el aislamiento social. El teletrabajo, la modalidad de clases a distancia, el consumo masivo del *delivery*, el uso de aplicativos de banca móvil y banca por internet, y los servicios de *streaming* para el entretenimiento son algunos ejemplos de la nueva normalidad.

Dada estas condiciones, se desarrollan interacciones con otros individuos y se realizan actividades imprescindibles a través del ciberespacio. A su vez, la delincuencia hace lo propio, hallando nuevas modalidades de criminalidad a través del mundo digital, como la suplantación de identidad y el fraude informático.

De este modo, a partir del escenario que mostró el COVID 19, se hace evidente la necesidad de una reforma actual que prevenga dichos delitos. Los beneficiarios serían todos los usuarios del ciberespacio; sería la gran parte de la población porque, en la actualidad, todos se conectan a una sola red, y se exponen, así, a nuevos delitos cibernéticos.

Los órganos y auxiliares de la administración de justicia han advertido esta fenomenología delincuencial que se comprueba en un informe estadístico publicado por el Ministerio Público (2021), a partir del cual se señala que los informes difundidos por la DIVINDAT de la Policía Nacional del Perú muestran que:

Figura 1

Delitos conexos con la Ley 30096

Octubre de 2013-diciembre de 2020	Delitos conexos con la Ley 30096		
12.169 Delitos conexos con la Ley 30096	13 % Robo de identidad	6 % Delitos contra los datos, los sistemas informáticos	78 % (aprox.) Relacionados con la informática y la ciberdelincuencia

Nota: Delitos conexos con la Ley 30096.

De acuerdo con el Informe Defensorial N. 001-2023-DP/ADHPD (2023):

La adhesión de nuestro país al aludido convenio, la primera versión del Código Penal (publicado hace más de 30 años), en el que ya se mostraba un primer intento en regular los actos ilícitos realizados a través de la tecnología, como fue el tipificar el hurto telemático. Adicionalmente, tenemos que en el año 2011 ya había sido publicada la Ley N°29733, Ley de Protección de Datos Personales, y en el 2013 la Ley N.º 30096, Ley de Delitos Informáticos, instrumento normativo que –entre otros puntos– describe las conductas delictivas que afectan los sistemas y datos informáticos, así como también las protecciones a las libertades civiles en el ámbito de las comunicaciones. En el 2014, esta ley fue complementada con su modificatoria, efectuada por medio de la Ley N.º 30171. En igual contexto, en el Perú se ha continuado emitiendo normas de diferente naturaleza por parte de entidades de diferentes niveles y competencias. No obstante, aún existen marcados retos al respecto en aras de fortalecer el marco jurídico nacional existente sobre la materia, a la luz de los compromisos internacionales asumidos y a la propia realidad y necesidades que demandan una urgente protección de los derechos de las personas, urgente e indispensable de acuerdo al aumento de denuncias por delitos informáticos que anualmente recibe la Policía Nacional. (p. 23)

Por otro lado, según el informe del Ministerio Público (2021), “el delito con mayor cantidad de registros, dentro del fraude informático, corresponde a las operaciones y transferencias electrónicas y/o de fondos no autorizados, con el 86 % (8142)” (p. 20). Además, se puede observar, en registros penales, que han experimentado un aumento año tras año; por ejemplo, el registro del año 2020 representa un aumento del 13 % con respecto al 2017.

Sin soslayar lo expresado en los párrafos precedentes, la ciberdelincuencia ataca un bien jurídico en común: la información, a través de la cual se cometen otros delitos. Recientemente, se mostraron antecedentes de criminalidad organizada destinada a la realización de estos actos de ciberdelincuencia.

El 19 de mayo del 2022, la ASBANC hizo público que, el 28 de abril del 2022, identificó la comercialización de datos personales e información privada a través de las redes sociales y canales de mensajería instantánea. De acuerdo con ASBANC, esto fue reportado y comunicado a “diversas instancias del Estado” (Hiperderecho, 2022).

La información que se ofrece en estos canales incluye datos personales como nombre, dirección, teléfonos, datos de propiedades e, incluso, datos sensibles como aquellos relacionados a las AFP, calificación en centrales de riesgo y datos biométricos como las huellas dactilares (Hiperderecho, 2022).

Sin embargo, lo denunciado por la ASBANC no es nuevo y por muchos años este tipo de información ha sido de fácil acceso a través de distintos medios. Para sostener esta afirmación, solo se debe remontar al último antecedente con la página web Zorrito Run Run, donde se comercializaban datos personales, lo que fue borrado luego de ocurrido este escándalo. WhatsApp o Telegram serán las nuevas plataformas para vender estos datos robados (Infobae, 2022).

Dicha realidad ha despertado la preocupación de nuestros entes gubernamentales ante la vulneración, por parte de estos ciberdelincuentes, de las diversas medidas de seguridad adoptadas para acceder a información privada de millones de peruanos.

Cabe mencionar que la filtración de datos personales configuraba el acto ilícito de la transmisión ilegal de datos privados (Art. 6 – Ley 30096). Al respecto, Villavicencio (2014) menciona que: "Este delito sanciona la conducta de comercializar (comercializar, traficar, vender, promover, favorecer o facilitar) información no pública, independientemente si con estos actos se causa algún perjuicio" (p. 301). Además, se sanciona punitivamente, restringiendo la libertad por un plazo de entre tres y cinco años de cárcel. Asimismo, a diferencia de los demás delitos contra la invasión de la intimidad, este delito es de persecución pública.

Al respecto, Muñoz (2019) comenta la reciente Ley N.° 30171, que introduce el artículo 154-A en la norma penal y modifica el delito de "transacción" de datos personales. El establecimiento del presente delito como un nuevo "delito informático" fue posteriormente derogado e incorporado a la Ley N.º 30096; pero la última reforma derogó este artículo y lo restableció en el Código Penal, en esta ocasión manteniendo el mismo nombre que el delito de invasión de la intimidad.

En un informe periodístico se reveló un nuevo caso de crimen organizado en materia informática. A través del programa dominical Redacción Gestión (2022), se presentó "El club del Tarot", donde un joven, junto a sus cómplices, lograron ingresar al sistema de seguridad de la plataforma estatal SEACE con la finalidad de realizar la venta de información reservada a diversas empresas y recibir ofertas millonarias.

Asimismo, el informe de Punto Final menciona que: “Por ello, una vez ya obtenida la base de datos, estas eran enviadas a representantes de las constructoras para que ajustaran sus ofertas económicas (rebajan sus precios) y sean más atractivas” (p. 3).

A partir de ello, se debe sostener que el tratamiento jurídico que se le da los delitos informáticos sigue careciendo de una actividad legislativa eficiente que permita tipificar correctamente las conductas ilícitas que se desarrollan en el ciberespacio. Posteriormente, en cuanto a la delincuencia informática, es imperativo citar a Muñoz (2019), quien sostiene que el bien jurídico que se protege y ampara en los delitos informáticos está relacionado con la información de carácter general, y también con bienes jurídicos como la indemnidad sexual, intimidad personal, la honra, entre otros según el tipo de delito que se comete.

Aunque el tráfico ilegal de información de la persona está tipificado como un ilícito que sanciona a quien o quienes vulneren la intimidad de una persona, ello no desconoce su naturaleza informática ni que sus medios de comisión se dan a través de las tecnologías. Sin embargo, resulta importante definir o redefinir el concepto de intimidad. En consecuencia, se destaca lo que menciona Muñoz (2019), a saber, que “la intimidad está evolucionando y debe entenderse como una defensa de la información íntima de público conocimiento sobre nuestro control respecto de la información íntima que consideramos confidencial” (p. 41). El uso y desarrollo de la tecnología ha ido acompañado de una protección jurídica de la privacidad, que ha evolucionado a partir del resguardo de datos privados, íntimos, personales y sensibles.

Asimismo, es importante la definición de intimidad, pues también corresponde definir a los datos personales, cuya expresión textual obra en la descripción del delito. En ese sentido, cabe resaltar una conceptualización de Rivera (2019), quien menciona que los datos personales confidenciales son una categoría más limitada y sólo son relevantes para el contenido íntimo

personal; en cuanto al término "datos sensibles", este se refiere a cualquier información sobre una persona que pueda utilizarse para discriminarla, como información médica, opiniones religiosas y sexuales. Otro problema es el aspecto cultural, social o político del titular de estos datos sensibles. Esto se debe a que, independientemente de estos contextos, se considera la cantidad de información que es sensible.

De acuerdo a García (2007), el derecho a la intimidad es aquello que se considera más propio y oculto del ser humano; por lo que los datos personales y la aplicación de las nuevas tecnologías deben ser el contexto en el cual el legislador pueda consagrar el derecho fundamental a la protección de datos de carácter personal.

La reforma del Código Penal debe contemplar sanciones más gravosas para los sujetos que realicen este tipo de actuaciones, como los ataques a gran escala a empresas que manejan información sensible de los usuarios.

En el artículo 154-A del Código Penal se describe el *nomen juris* del delito tráfico ilegal de datos: se produce cuando se utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos.

En el debate académico se ha presentado esta dicotomía jurídica por establecer los límites para el reconocimiento de los derechos que goza una persona jurídica. El cuestionamiento consta en determinar si el derecho debería reconocer la protección de la intimidad de las personas jurídicas. Para ello, es importante el siguiente sustento de Pacheco (2016): el desarrollo de la ciencia requiere el uso de la terminología en un sentido unificado, que debe corresponder mejor a la realidad de las cosas y las personas; por lo tanto, por su propia personalidad y secretos

comerciales para las empresas, lo mejor es reservar una vida privada para una persona física; de esta manera se podrá avanzar hacia la formación de un verdadero reconocimiento a la privacidad de la vida de un individuo, que contenga tanto la privacidad de una persona física como la privacidad de una persona jurídica, como derechos básicos. Como parte del concepto general, ambos derechos deben ser complementarios y relacionados entre sí, pero no deben estar en perfecta concordancia.

La ciberdelincuencia en el Perú ha incrementado, afectando a personas naturales y jurídicas. Por su parte, los delitos informáticos hallan un bien jurídico en común: la información. Tras las modificaciones realizadas, la vulneración de datos personales abandonó el compendio de los delitos informáticos para ser incorporado al Código Penal. Ello no desconoce su naturaleza informática ni lo medios digitales a través de los cuales se pueda cometer este ilícito. Siendo imprescindible salvaguardar la información sensible de la ciudadanía, la prensa muestra que desde las entidades estatales se gestan organizaciones criminales destinadas a lesionar la intimidad y el patrimonio de los peruanos.

Por ende, corresponde cuestionarse: ¿existe tal efectividad al dar un tratamiento legislativo específico para el tipo penal del tráfico de delitos informáticos? Siendo un delito clave en la lucha contra la ciberdelincuencia, su tipificación aún es imprecisa y sus penas demasiado bajas para un delito que es fuente de demás delitos informáticos.

La presente investigación busca hallar formas de resolver esta problemática mediante la exposición de argumentos fácticos y jurídicos para sustentar una necesaria reforma en el tipo penal del injusto de tráfico de datos personales concernientes a la persona. En esa directriz, esta investigación busca que, mediante el delito en cuestión, la persecución fiscal sea eficaz y se

impongan penas a los ciberdelincuentes, ello sin dejar de reconocer la actividad investigatoria que precede y recae en los órganos policiales especializados en delitos de alta tecnología.

1.2 Justificación

A fin de hallar una solución eficaz para la reducción y prevención de la ciberdelincuencia, el presente estudio busca, desde la casuística, la estadística y la legislación comparada, una propuesta de modificación del tipo penal del delito de tráfico ilegal de datos privados a fin de frenar la delincuencia que agravia a la ciudadanía en el ciberespacio.

En lo que respecta a la importancia de las teorías mencionadas, estas serán de ayuda, ya que, a través de dichas teorías, se desarrollará el trabajo de investigación, mencionando, por ejemplo, el principio de protección de las garantías fundamentales de las personas.

1.2.1 Justificación práctica

La reforma de la legislación penal en el tema del intercambio ilegal de datos privados se basa en la necesidad de fortalecer la lucha contra este delito, el mismo que atenta contra la privacidad y seguridad de las personas, y contra la integridad de la información financiera y comercial. Incluir disposiciones sobre este delito y proporcionar sanciones basadas en su gravedad permitirá a las autoridades enjuiciar y castigar a los responsables del intercambio ilegal de datos. Además, este cambio permitirá al país cumplir con las leyes internacionales relativas al resguardo de los datos, y combatir el fraude en línea.

1.2.2 Justificación legal

La reforma penal peruana sobre tráfico ilegal de datos se fundamenta en la necesidad de realizar la adecuación de la legislación sobre la base de estándares nacionales e internacionales pertinentes ante las nuevas formar de delinquir. La imposición de sanciones proporcionales asegura también una respuesta adecuada a la gravedad del delito y la eficacia de la persecución y

sanción de ese tipo de delitos. Perú actualmente no tiene leyes específicas que rijan las telecomunicaciones ilegales. Sin embargo, ese delito está tipificado como delito contra la intimidad en el Código Penal y se castiga punitivamente con dos a seis años de cárcel. Además, la obra arroja luz sobre la situación legal en Colombia. La Ley 1581 (2012) establece medidas efectivas para prevenir y sancionar las transferencias ilícitas de datos personales en Colombia, garantizando los derechos de los ciudadanos. De acuerdo al artículo 296 f, violación de datos personales, "el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

De acuerdo al artículo anterior, se puede afirmar que es una disposición legal que establece las consecuencias legales para aquellas personas que, sin tener la autorización adecuada, obtengan, recopilen, roben, ofrezcan códigos personales o datos personales contenidos en archivos, bases de datos u otros medios similares, con el fin de obtener un beneficio propio o beneficiar a terceros.

1.3 Planteamiento del problema

1.3.1 Problema general

¿Es necesaria la modificación del tipo penal del tráfico ilegal de datos en el Código Penal peruano?

1.3.2. Problemas específicos

P.E.1 ¿Resulta idónea la descripción de la conducta típica del tráfico ilegal de datos personales?

P.E.2 ¿Cuáles son los criterios de la política criminal que justifican el rango punitivo

establecido en el artículo 154-A del Código Penal?

P.E.3 ¿Cuál es el alcance de la lesión del bien jurídico en el delito de tráfico ilegal de datos personales?

P.E.4 ¿Cuáles son los criterios que emplea el Estado de Colombia para la punibilidad del delito de tráfico ilegal de datos personales?

1.4. Objetivos

1.4.1. Objetivo General

Determinar si es necesario modificar el tipo penal del tráfico ilegal de datos en el Código Penal peruano.

1.4.2. Objetivos específicos

O.E.1.Determinar la idoneidad de la descripción de la conducta típica del tráfico ilegal de datos personales.

O.E.2.Clasificar los criterios de la política criminal que justifican el rango punitivo establecido en el artículo 154-A del Código Penal.

O.E.3.Identificar el alcance de la lesión del bien jurídico en el delito de tráfico ilegal de datos personales.

O.E.4. Analizar cuáles son los criterios que emplea el Estado de Colombia para la punibilidad del delito de tráfico ilegal de datos personales.

Capítulo 2: Marco Teórico

2.1 Investigaciones Previas

2.1.1 Antecedentes Internacionales

Fernández (2009), en su tesis *Defensa del Derecho a la Intimidad Frente al Poder Informático*, presentada para la Universidad Mayor de San Andrés (Bolivia), se trazó como objetivo principal proponer una norma que garantice y proteja los datos personales de las personas naturales y jurídicas, ello para garantizar el derecho a la intimidad de las personas. El autor arribó a la siguiente conclusión: la información que se mantiene en reserva equivale a un poder, por lo que la legislación boliviana no ofrece una condición de seguridad eficaz con respecto a los datos personales, generando de esta manera un vacío jurídico; por tanto, se exige una garantía para conservar aquellos datos de información personal con el propósito de impedir el tráfico ilícito y resguardar el derecho de quien fuere afectado.

De acuerdo con el párrafo anterior, se puede decir que la crítica a la legislación boliviana se sustenta porque no ofrece una condición de seguridad eficaz en lo que respecta a los datos personales. Esta crítica señala un problema importante y la necesidad de reformas legales para abordar el vacío jurídico, exigencia de garantías para conservar datos personales. El párrafo demanda la necesidad de garantías para conservar datos de información personal con el propósito de prevenir el tráfico ilícito de datos y proteger los derechos de quienes puedan verse afectados. Esta exigencia subraya la importancia de la regulación y la seguridad de los datos personales. En consecuencia, se establece un problema fundamental relacionado con la protección de datos personales y la intimidad en Bolivia. Se propone la necesidad de una norma legal más efectiva y la implementación de garantías para prevenir el tráfico ilícito de datos y resguardar los derechos de las personas afectadas. Esta tesis aborda una cuestión crucial en la era digital y destaca la importancia de la protección de la intimidad y los datos personales.

Trávez (2019) se propuso analizar las limitaciones de las leyes ecuatorianas en relación con los delitos informáticos y cómo estos vulneran los derechos constitucionales. La metodología utilizada fue de enfoque cuantitativo y el nivel de investigación fue exploratorio y descriptivo, con una población de 44 personas. Se concluyó que la tecnología ha evolucionado, lo que ha llevado a los delincuentes a perfeccionar sus métodos delictivos a través del uso de computadoras, incluyendo el acceso no autorizado a bases de datos empresariales y redes sociales, lo que afecta a la integridad personal, sexual, familiar y patrimonial de las víctimas. Se destacó que el ordenamiento jurídico ecuatoriano no ha previsto normativas adecuadas para abordar estos tipos de delitos, como el secuestro virtual, lo que deja a muchas de estas conductas en la impunidad. La investigación también subraya cómo los más jóvenes son especialmente vulnerables a estos delitos que atentan contra su intimidad y seguridad en línea.

2.1.2 Antecedentes Nacionales

Ferrero y Schutz (2013) analizaron cómo el tratamiento de datos personales se ha convertido en una práctica habitual en nuestros días y su comercialización en un negocio que mueve un inmenso caudal de dinero. De allí que cada vez más personas, naturales y jurídicas, se han abocado a la recolección, entrecruzamiento y transmisión de información confidencial. El caldo de cultivo de este floreciente negocio ha sido la presencia de una creciente demanda, es decir, personas, empresas, organizaciones, etcétera, dispuestos a desembolsar el dinero que sea necesario para obtener dicha información, sumado a una innumerable variedad de tecnologías que han sido colocadas a su servicio. La consecuencia directa e inmediata radica en la constante afectación de los derechos de las personas involucradas, quienes son, sin duda, las víctimas del tráfico de datos personales que constituye un fenómeno actual, cuyas múltiples implicancias se analizarán a continuación.

El autor concluye lo siguiente:

Normalización del tratamiento de datos personales: el párrafo señala que el tratamiento de datos personales se ha vuelto común en la sociedad actual, lo cual es un reflejo de la creciente digitalización y la recopilación de información personal en diversas plataformas y servicios.

Comercialización y negocio: el texto resalta que la comercialización de datos personales se ha convertido en un negocio rentable, lo cual implica que los datos personales tienen un valor económico significativo, y las empresas y organizaciones están dispuestas a pagar por acceder a esta información.

Recolección y transmisión de información confidencial: se menciona que muchas personas, tanto físicas como jurídicas, se dedican a la recolección, el cruce y la transmisión de datos confidenciales, lo cual es manifestación de la diversidad de actores involucrados en el tratamiento de datos personales.

Demanda y tecnología: el crecimiento de este negocio se atribuye a una creciente demanda de información personal y a una amplia gama de tecnologías que facilitan la recopilación y transmisión de datos, lo cual muestra la importancia de la tecnología en la expansión del tráfico de datos personales.

Afectación de los derechos de las personas: se destaca que la consecuencia inmediata de este tráfico de datos personales es la afectación constante de los derechos de las personas involucradas, lo cual implica que, en última instancia, son las personas las que sufren las consecuencias de la explotación de sus datos personales.

Tráfico de datos personales como fenómeno actual: el párrafo concluye aludiendo al tráfico de datos personales como un fenómeno contemporáneo, lo que sugiere que es un tema de relevancia actual que merece un análisis más profundo. Se comenta acerca de la normalización y

comercialización del tratamiento de datos personales, así como su impacto en los derechos individuales. También se sugiere que el análisis de este fenómeno es esencial para comprender sus implicaciones y desafíos en la sociedad actual.

Quevedo (2017) estudia el uso y trascendencia que tiene el internet y las nuevas formas de aparición de delitos informáticos. El autor aplica un enfoque cualitativo de revisión bibliográfica; tiene como objetivo demostrar que estos ciberdelitos exigen tomar estrictas medidas para prevenir y evitar la transgresión de los derechos. Se concluye que el uso de internet ha tenido un impacto significativo en la actividad delictiva, creando nuevas formas de delincuencia y como un medio para cometer otros delitos, así como una gama aún no caracterizada de posibles comportamientos relacionados con las redes y las computadoras.

El referido estudio difiere con los objetivos de la presente investigación dado que los vacíos normativos analizados, teniendo en cuenta -y como base- la normativa penal, no se encuentran tipificados en él, aunque sin dejar de destacar la importancia del ser humano, puesto que utilizan la red tecnológica de internet según su libre albedrío; mientras que en el trabajo de investigación de la autora se toman precauciones especiales para evitar entorpecer los esfuerzos de investigación o vulnerar los derechos fundamentales.

En la misma línea de investigación, Olivos (2020) señala que el derecho de protección a los datos personales se fundamenta bajo los preceptos de privacidad e intimidad, un poder personal de disposición y control de la información (derecho a la autodeterminación informativa) que busca proteger a la persona, teniendo el control sobre la información personal que le concierne y dejándola desarrollarse en un espacio de libertad, seguridad y justicia. Bajo esta perspectiva, los Estados deben brindar los mecanismos y elementos para su protección.

Dichos derechos se fundamentan en la privacidad e intimidad: el derecho de protección de datos personales se basa en los conceptos de privacidad e intimidad. Esto significa que las personas tienen un derecho fundamental a mantener su información personal confidencial y proteger su espacio íntimo de la intrusión no autorizada. Asimismo, se menciona el derecho a la autodeterminación informativa, un concepto clave en la protección de datos. Este derecho otorga a las personas el poder de decidir qué información personal desean compartir y controlar cómo se utiliza.

Protección de la persona en sí misma: el párrafo enfatiza que el derecho de protección de datos personales busca proteger a la persona en sí misma, lo cual significa que el enfoque está en la salvaguardia de la dignidad y los derechos individuales de cada persona, permitiéndoles desarrollarse en un entorno de libertad y seguridad.

Control sobre la información personal: se destaca que las personas deben tener el control sobre la información personal que les concierne, lo cual implica que las personas tienen el derecho de decidir quién puede acceder a su información, para qué fines y con qué limitaciones; en consecuencia, se argumenta que el derecho de protección de datos personales es esencial para preservar la privacidad, la intimidad y la autodeterminación informativa de las personas. Además, se enfatiza la responsabilidad de los Estados en garantizar la protección efectiva de este derecho fundamental.

2.2. Bases Teóricas

2.2.1 Desarrollo de los Delitos Informáticos

Banco de datos personales. Según el título preliminar de la Ley 29733, inciso 1, artículo 2, es un “conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso” (p. 2).

Banco de datos personales de administración privada. Acorde al inciso 2, artículo 2 de la Ley 29733, el "banco de datos personales, cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público" (p. 2).

Banco de datos personales de administración pública. Según el título preliminar de la mencionada ley, el Presidente de la República (2013), en el inciso 3, artículo 2, menciona que "la titularidad del banco de datos personales corresponde a una entidad pública" (p. 2).

Argumentos sobre la importancia y protección de datos personales. Según Aredo (2021), el *phishing* consiste en la violación al resguardo de datos personales en los delitos informáticos, los cuales se realizan como producto de los conocimientos técnicos que poseen los ciberdelincuentes. Por otro lado, Carriedo (2022) agrega que la censura a internet no resultaría ser una respuesta idónea ante el aumento de las conductas criminales a través de la red, sino que merece sanciones severas. No se trata de regular o no, sino de regular respetando los derechos humanos.

De la Puente (2020) menciona que "la vía que ha tomado la regulación pública consiste en cumplir ciertos parámetros para proteger la difusión de una información y que este acto no colisione con la protección a la intimidad y el secreto de las comunicaciones" (p. 121). Asimismo, Hidalgo (2020) complementa mencionando que, efectivamente, la existencia del internet contiene aspectos tanto positivos como negativos. Será negativo porque cualquier individuo podrá acceder a información de cada usuario debido a la sobreexposición de los datos personales en las redes sociales, por ejemplo.

Luna (2021) sostiene que debe promoverse una conciencia de protección de lo privado, de manera estricta. Asimismo, cada persona debe recibir y exigir información de manera transparente

y fiable respecto al uso de nuestros datos personales. No obstante, Muñoz (2019) refiere que toda persona posee la capacidad de establecer qué información se encuentra en el fuero íntimo, privado o público.

2.2.2 Tráfico Ilegal de Datos Personales

El tráfico ilegal de información personal implica la mercantilización de la información personal; por tanto, de conformidad con la directiva comunitaria, la sección 2(a) define los datos personales como:

Datos personales: "cualquier información relativa a una persona física identificada o identificable. Un individuo identificable es aquel cuya identificación es directa o se refiere a cualquier individuo que pueda establecerse indirectamente" (Montiel, s.f., p. 426)

Partiendo de lo citado, se debe afirmar, una vez más, que la información privada identifica a un ser humano que existe físicamente; por ello, deben ser protegidos frente al delito del tráfico ilegal de datos personales que, hoy en día, es un delito muy sonado en los medios de comunicación, y que debe ser sancionado severamente para evitar su aumento y la vulneración de un derecho.

2.2.3 Tipificación del Delito de Tráfico Ilegal de Datos Personales

Este delito se encuentra tipificado en el artículo 154 – A del Código Penal, "tráfico ilegal de datos personales", el cual menciona lo siguiente:

Artículo 154-A. Tráfico ilegal de datos personales

"El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar (…) sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años" (Congreso de la República, 1991).

Así mismo, estos autores indican que, “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 el párrafo anterior” (Congreso de la República, 1991).

2.2.4 Teorías Específicas

2.2.4.1 Bien Jurídico de la Intimidad. Este bien jurídico no solo se encuentra protegido por el Código Penal, también por la Norma Fundamental en el artículo 2, inciso 7, a partir del cual se habla del ilícito de transmisión ilegal de información de la persona. El bien jurídico lesionado es el derecho a la intimidad.

Cabe recalcar que, según Téllez (2015), el Código Penal peruano explica la inclusión de muchos delitos contra las libertades individuales, incluidos los delitos de violación del derecho a la privacidad. La justificación para hacer de la privacidad un bien legítimo a proteger es el reconocimiento de la universalidad de este derecho desde DUDH, que establece que la vida y el domicilio no pueden ser injeridos, ni puede dañarse el honor o la reputación.

En consecuencia, el delito afecta a la intimidad de diferentes maneras, según Téllez (2015) las más comunes son:

- Fugas de información personal: cuando nombres, direcciones, números de teléfono, información bancaria, etc., se intercambian ilegalmente, y pueden ser utilizados por malas personas para cometer estafas, robos de identidad u otros delitos. Esto perjudica a la intimidad y puede tener grandes consecuencias para las personas implicadas.
- Violación de confidencialidad: el tráfico de datos puede implicar la divulgación de información privada como secretos comerciales, planes de negocio, planes para fabricar nuevos productos o información gubernamental oculta. Estas filtraciones pueden perjudicar a empresas, organizaciones y gobiernos, y pueden dificultar que la gente

confíe en las instituciones.

- Espionaje y vigilancia ilegal: el tráfico ilegal de datos puede implicar la recopilación y distribución encubiertas de datos de vigilancia. Puede consistir en interceptar comunicaciones, obtener acceso no autorizado a cámaras de seguridad o vigilar actividades en línea en secreto. Estas prácticas violan la privacidad y pueden emplearse con fines de extorsión, coacción o cualquier otro fin ilegal.
- Exposición de información sensible: información como historiales médicos, historiales financieros, preferencias sexuales y otros detalles privados pueden incluirse en bases de datos comercializadas ilegalmente. Cuando este tipo de información sale a la luz, puede herir emocionalmente a las personas y arruinar su reputación en el ámbito laboral e incluso en la vida personal.
- Manipulación de datos: la transmisión ilegal de información también puede conllevar la manipulación de la información, como la falsificación de documentos o la alteración de registros electrónicos. El resultado puede ser la desinformación, perder o dudar de la confianza que puedan dar los sistemas de información, y la disposición de adoptar decisiones que se basen en datos inexactos o alterados malintencionadamente.

2.3 Definición de Términos

Datos personales

En el inciso 4, artículo 2, de la Ley 29733 se menciona que es “toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados” (p. 2).

Ley de protección de datos personales

Según Luna (2021), esta ley tuvo origen en el año 2011, pero entró en vigor en el año 2013. Ha tenido modificaciones en el año 2017.

Derechos arco

Conjunto de derechos que la ley recoge, en este caso, los interesados a solicitar la puesta a disposición, rectificación, supresión u oposición a la recogida y uso de sus datos a los organismos obligados a conservarlos**.** Según Bordachar (2022), estos son:

Acceso: se refiere a la capacidad de un interesado para solicitar la puesta a disposición, rectificación, supresión u oposición a la recogida y uso de sus datos al ente obligado en posesión de estos.

Rectificación: capacidad de las personas para rectificar cualquier información personal inexacta o incompleta que obre en poder de una organización. Si una persona descubre que su información personal es inexacta, obsoleta o insuficiente, tiene derecho a solicitar que se rectifique.

Cancelación: se define el derecho de cancelación como el derecho del titular de datos a solicitar y obtener del responsable, que suprima o elimine sus datos personales, de acuerdo con las causales previstas en la ley (Bordachar, 2022).

Oposición: condición de los sujetos a oponerse al procesamiento de sus datos personales. Esto incluye la capacidad de oponerse al uso de datos para marketing directo o procesamiento basado en intereses legítimos.

Derecho: el derecho es un sistema de reglas que regula la relación existente de la persona humana y la organización en una sociedad.

Protección de datos: se refiere al marco de leyes y políticas establecidas para salvaguardar el derecho de las personas a la reserva y al control sobre sus propios datos. Su objetivo es garantizar que la información personal no se maneje indebidamente, se divulgue o se acceda a ella de forma incompatible con el propósito original para el que fue recopilada y almacenada.

Derecho a la intimidad: es una garantía básica que permite la protección de los asuntos personales y domésticos. Indica que las personas tienen autonomía para gestionar y mantener en privado cualquier aspecto de su vida que consideren delicado. El derecho a la intimidad incluye la salvaguarda del hogar y la vida familiar, las comunicaciones escritas y electrónicas, la reputación y el aspecto físico.

La integridad: es la práctica de ser una persona honesta, respetuosa, adherirse a nuestros valores y tomar sistemáticamente decisiones positivas, incluso cuando nadie esté mirando. Mientras que la honestidad se refiere al acto de ser veraz, la integridad es el acto de actuar de acuerdo a los principios.

2.4 Categorías de Análisis

La necesidad de modificar el tipo penal del tráfico ilegal de datos en el Código Penal peruano.

Capítulo 3: Metodología

3.1 Explicación y Justificación del Tipo de Investigación Elegido

Este trabajo de investigación adoptó un enfoque cualitativo para interpretar el tráfico ilegal de datos y el potencial para la reforma del derecho penal. Esta no es una medida numérica o estadística. La profundidad también hace que el estudio sea descriptivo, ya que gira en torno a explicaciones en una sola categoría analítica.

El trabajo de estudio tiene como objetivo analizar las reformas del derecho penal relacionadas con el delito de tráfico de datos personales. A pesar de que existe un material bibliográfico limitado que analice el tema en discusión, muestra que la normativa se ha aplicado. Existen trabajos realizados en Sudamérica y en países de habla hispana que no califican a los hechos, necesariamente, de tráfico ilícito de datos personales. Con esto en mente, se analizan trabajos de Ecuador, Chile, Colombia y España, que trataron temas como privacidad, ciberdelincuencia y protección penal de datos personales.

3.2. Población o Sujeto o Casos

La población estuvo compuesta por tesis nacionales e internacionales, sumando un total de 18; de estas, 11 tesis son nacionales, y 10 de ellas pertenecen a la base de datos de Concytec y uno a Renati. Las seis tesis restantes son internacionales, una de Chile, tres de repositorios en Colombia y cuatro de un repositorio en Ecuador. Entre los criterios de inclusión se consideró la antigüedad de las investigaciones -cinco años como máximo- y todas aquellas relacionadas con la protección de datos y el tráfico ilegal de datos.

3.3 Técnicas de Recojo de la Información

La técnica empleada para la recopilación de la información es el análisis documental y observacional, sin ninguna interferencia por parte del tesista. Para acceder a estas tesis, se

ingresó a la base de Renati y Concytec, así como a repositorios institucionales de Colombia, Chile y Ecuador a través de la consulta en bibliotecas virtuales. Así mismo, los días específicos de la búsqueda de estos datos fueron el 9 de abril del 2023 para las once tesis nacionales, y el día 10 de abril se realizó la búsqueda en el repositorio de las universidades de Chile y Colombia.

Ahora bien, para la búsqueda se emplearon ejes temáticos teniendo como base la selección de fuentes relacionadas al tema de investigación. De igual forma, se consideraron las palabras claves para la búsqueda, que son: protección de datos, datos personales, delitos informáticos, fraude informático, y el *phishing*.

Finalmente, se consideraron aspectos espaciales, en virtud de los cuales se tomará en cuenta la legislación comparada con el fin de abordar el problema referido a los criterios que emplea el Estado de Colombia; para ello se analizará su normativa y su efectividad. Además de ello, se consideraron los aspectos temporales a efectos de que las tesis e investigaciones seleccionadas se hayan realizado entre los años 2018 y 2022, con el objetivo de recopilar información de calidad a efectos de analizar la naturaleza informática del delito de tráfico ilegal de datos. Todas las tesis han sido encontradas en idioma español, las mismas que son públicas por lo que no se requiere autorización alguna para poder ser revisadas.

3.4 Instrumento de Recolección de Datos

Se ha diseñado específicamente una herramienta de recopilación de datos, para reunir información relevante que permita el análisis y la interpretación del documento. Los detalles de esta herramienta es responsabilidad del tesista, teniendo en cuenta las especificaciones establecidas para el propósito general de la tesis. Al aplicar el presente instrumento de recolección de datos no se ha incluido tesis en inglés.

Después de realizar una indagación minuciosa, se encontraron 18 tesis, las mismas que se desarrollarán en los resultados de la investigación. Por ello, se ha clasificado en dos temáticas relevantes y la problemática penal reguladora de los datos personales. Siendo así, es preciso indicar que no se ha excluido ninguna investigación, ya que abordan problemáticas que serán materia de análisis en la presente tesis. Se indica, además, que el tiempo de publicación de estas investigaciones no excede los cinco años.

3.5 Estrategias de Análisis de la Información

A partir de las tesis obtenidas, se identificó el objetivo de cada tesis, el método empleado, el bien jurídico protegido, los elementos típicos empleados y, finalmente, el rango de la pena.

El tipo penal 154-A en Perú se refiere al "tráfico ilegal de datos personales". La tipicidad objetiva de este delito implica que se comete cuando alguien realiza actividades de tráfico ilegal de datos personales, es decir, la recopilación, transferencia, compra, venta o divulgación de información personal sin el consentimiento de la persona afectada. Esto puede incluir datos como nombres, números de identificación, direcciones, entre otros.

La tipicidad subjetiva se refiere a la intención o conocimiento del autor del delito. En el caso del tipo penal 154-A, la tipicidad subjetiva implica que el autor debe actuar con dolo, es decir, con conocimiento y voluntad de cometer la conducta ilícita. El autor debe ser consciente de que está traficando datos personales de manera ilegal y debe realizarlo de manera intencional.

En resumen, el delito de tráfico ilegal de datos personales en Perú implica la realización de actividades ilegales relacionadas con datos personales sin el consentimiento de la persona afectada, y el autor debe actuar con conocimiento y voluntad de cometer este acto ilícito.

Capítulo 4: Resultados y Discusión

4.1. Resultados

De acuerdo al análisis bibliográfico de revisión de literatura de trabajos de investigación nacionales e internacionales vinculados al tema de estudio, se precisan a continuación los resultados del presente trabajo.

Tabla 1

Comparación en función de los objetivos

Autor, año	Objetivo
(Aredo, 2021)	Comprobar si la figura del *phishing* vulnera o ataca los datos personales en los delitos informáticos (p. 2).
(Ccasa y Coila, 2021)	Determinar aquellos criterios que evidencian la defensa de un bien jurídico colectivo respecto a la integridad de los sistemas informáticos y su funcionalidad (p. 6).
(Berrio & Orellana, 2022)	Precisar cómo los datos personales y financieros son transgredidos por el tráfico de información digital en las plataformas de internet, Lima Este, 2022 (p. 4).
(Sosa, 2022)	Precisar si en la Ley N.° 30096 se encuentra de manera clara y expresa el *phishing* como una de las formas de los delitos informáticos (p. 13).
(Peralta, 2022)	Realizar el análisis respecto de los delitos informáticos y los datos en sistemas informáticos (p. 3).

Nota. La tabla establece la comparación de los objetivos de los diversos autores.

Tabla 2

Comparación en función de la metodología

Autor, año	Metodología
(Román, 2020)	La investigación fue no experimental, combinó métodos cualitativos y cuantitativos, y de tipo propositivo aplicado (en el sentido de que se elaboró una propuesta de legislación). Los abogados penalistas del Colegio de Abogados de Lambayeque y veinte investigadores de la División de Investigación de Delitos de Alta Tecnología conformaron la población y la muestra, respectivamente. Se emplearon métodos de observación, de campo, cuestionarios y métodos documentales, todo se documentó mediante una combinación de fichas de resumen, comentario, texto y fichas bibliográficas (pp. 41-46).
(Aredo, 2021)	El diseño del estudio que aquí se presenta es la teoría fundamentada, y el enfoque utilizado es de naturaleza cualitativa (análisis documental). Se recopiló documentación pertinente al tema de la investigación, la regulación del *phishing* en el país peruano, teniendo como eje principal el departamento de La Libertad. En el análisis participaron 10 expertos: cinco abogados penalistas y cinco ingenieros de sistemas, y dos expedientes. Dentro de la recopilación de los datos el autor empleó el análisis documental y su instrumento fue un formulario de recolección de datos (como detalles doctrinarios sobre *phishing*, delitos informáticos y casaciones). La técnica e instrumento utilizado fue la entrevista no estructurada (pp. 11-13).
(Londoño, 2021)	Se utilizó la hermenéutica, el enfoque cualitativo y la técnica sistemática para interpretar el artículo 12 de la Ley 1581 de 2012, que regulariza el procedimiento de información personal, así como las órdenes de la Constitución Política de Colombia. El estudio también utilizó el método de análisis de derecho comparado a través de documentos internacionales en forma de tabla, centrándose en los Convenios 108 de 1981, que actualizan los principios que rigen el tratamiento de datos personales (p. 7).
(Sanmartín, 2021)	El autor recopiló información a escala nacional y mundial que ayudó a diferenciar los numerosos componentes del delito. El nivel de estudio exploratorio considera el descriptivo y el explicativo. Tanto el Código Penal Orgánico Integral como el Convenio de Budapest tienen sus propias categorías

Autor, año	Metodología
	de delitos. Se utilizó el enfoque cualitativo a través del método histórico y la exégesis. La entrevista fue a ocho profesionales, entre abogados, jueces, fiscales y especialistas en derecho informático con gran experiencia en la investigación de la ciberdelincuencia y la defensa de casos de ciberdelincuencia en los tribunales nacionales.
(Sosa, 2022)	El diseño de la investigación fue documental a través de la legislación, doctrina y jurisprudencia relacionada con el tema; el nivel es documental descriptivo, de tipo básico. Se empleó un enfoque cualitativo porque integró doctrina especializada, su fin fue examinar si la tipificación del *phishing* como delito informático en la ley peruana N.º 30096 es deficiente. Dado que el *phishing* no se halla plasmado dentro de la normativa mencionada, se utilizó una combinación de enfoques analítico (análisis de la tipificación del *phishing*) y dogmático (doctrina vinculada al *phishing*), junto con un enfoque comparativo (internacional). Se consultaron diversos recursos primarios y secundarios, como internet, publicaciones especializadas, la ley de delitos informáticos, doctrina, artículos y medios de comunicación (p. 35).
(Peralta, 2022)	Se utilizó una metodología cualitativa y hermenéutica, y se analizaron documentos encontrados en libros, publicaciones periódicas, antecedentes preparatorios y una comparación de la Ley N.º 30096 del Perú con las de otros países. Además, se cuenta con la Sentencia Plena en el Área de Jurisprudencia: 1100/2020, documento N.º 01189-2019-PHC/TC (p. 20).
(Sinchiguano, 2022)	Dado que se buscó una reforma penal, se empleó un enfoque cualitativo. El autor obtuvo información y documentación, doctrina, hechos y leyes sobre el desarrollo y comercialización, acciones que no son propias ni están tipificadas en el Código Orgánico Integral Penal. La revisión documental (lectura, análisis de doctrina, libros, revistas, jurisprudencia y acuerdos internacionales) fue el método y la herramienta utilizada. En este caso, se comparó el Código Penal Integral chileno con el Convenio de Budapest. También se interrogó a abogados penalistas, constitucionalistas, jueces y fiscales de las provincias de Pichincha y Chimborazo, como expertos en la materia (pp. 42-46).

Nota. La tabla explica la comparación acerca de la metodología que utilizaron los autores.

Tabla 3

Comparación en función al bien jurídico

Autor, año	Bien jurídico
(Román, 2020)	Los bienes jurídicos en este contexto se refieren tanto a la información en sí como a la información que ha sido almacenada, procesada y transmitida utilizando diversos procedimientos computarizados de proceso de datos, así como los demás bienes jurídicos que se ven afectados por los delitos informáticos como la indemnidad sexual, la intimidad, entre otros (p. 31).
(Vicencio, 2020)	Se menciona que la constitución de Chile respeta y protege la vida privada, así como la honra tanto de la persona como de su familia, y la protección de los datos personales, ya que el tratamiento y protección de los mismos se realiza según lo que la ley establece; por tal motivo, si se vulnera lo que establece el artículo 20, se ocasionan actos u omisiones de privación o amenaza en el ejercicio legítimo del derecho a la protección de datos personales (p. 9).
(Aredo, 2021)	Dicho autor menciona la necesidad de proteger el bien jurídico de la intimidad informática, por lo que se requiere utilizar los medios pertinentes para su protección, ya que son vulnerados por personas inescrupulosas que tienen conocimientos en la informática (p. 27).
(Ccasa y Coila, 2021)	En este caso el bien jurídico protegido es la información (datos que se guardan, procesan y envían por medios electrónicos), y los complementarios (indemnidad sexual, privacidad, etc.) también son vulnerables a este tipo de delitos. Así mismo, un conjunto de bienes es afectado, teniendo la característica de un delito pluriofensivo (p. 32).
(Londoño, 2021)	El derecho a los datos personales está salvaguardado por la legislación 1581 de 2012, que establece en su artículo 2: quien recolecte dichos datos e información dentro del territorio colombiano debe cumplir con la ley colombiana (p. 17).
(Sanmartín, 2021)	Como bienes jurídicos se tiene a la seguridad informática, la integridad, confidencialidad, la disponibilidad de datos, los sistemas informáticos y, por último, la intimidad informática. El autor también menciona que la seguridad informática es el bien jurídico que tiene carácter colectivo e individual (p. 25).
(Berrio y Orellana, 2022)	En sentido estricto, como consecuencia de la tecnología en la información, se han incrementado los ataques a la seguridad de la información personal, que es el bien jurídico protegido (p. 1).

Autor, año	Bien jurídico
(Sosa, 2022)	En cuanto al bien jurídico protegido, el autor señala que no existe consenso al respecto y que, si bien se suele establecer en la totalidad de las leyes que estos delitos transgreden el patrimonio, adicionalmente se afirma, de cara a una posible reforma de la ley, que considere al bien jurídico protegido al orden económico, así como a la intimidad personal (p. 22).
(Peralta, 2022)	Según el autor, está incluido el derecho a la libertad de información y a la intimidad, los cuales corren peligro cada vez que las plataformas digitales que contienen diversos datos son objeto de ataques u objetivos de la delincuencia organizada en el Perú (p. 6).
(Sinchiguano, 2022)	Según el autor, estos delitos son pluriofensivos porque vulneran múltiples derechos a la vez, entre ellos los derechos a la intimidad o a la confidencialidad (daños individuales ofensivos) y a la seguridad patrimonial de los sistemas de comunicación e información (considerado un bien jurídico supraindividual) (p. 2).
(Huayca, 2022)	Según el autor, los bienes jurídicos más valioso en los delitos cibernéticos son los datos privados de las personas. El comercio ilegal de tecnología diseñada para salvaguardar la adquisición de datos puede conducir al robo de muchos tipos diferentes de propiedad legalmente protegida (pp. 2-3).

Nota. La tabla explica la comparación en función de los bienes jurídicos descritos por los autores.

Tabla 4

Comparación en función a los elementos típicos

Autor, año	Elementos típicos
(Román, 2020)	El autor precisa que el tipo penal describe un comportamiento que puede ser realizado por cualquier persona o un experto en conocimiento informático, que es el sujeto activo. Por otro lado, el sujeto pasivo está constituido por aquellos perjudicados por dicha conducta ilícita, los cuales pueden ser personas físicas o jurídicas (empresa pública o privada). El medio empleado es la informática, con el uso computarizado (pp. 26-28).
(Vicencio, 2020)	Como explica el autor, el propietario de la información privada es el sujeto pasivo, mientras que el sujeto activo puede ser cualquiera, porque toda persona puede efectuar el tratamiento de los datos personales de otros, pero la ley establece cuáles son esos límites (p. 10).
(Aredo, 2021)	En concreto el autor menciona el término *phishing* como una táctica engañosa empleada para robar información confidencial por e-mail, mensaje de texto o enlace a un sitio web, que es cometida por el sujeto activo; mientras que la información sobre la identidad de los usuarios, como nombres, direcciones, números de la seguridad social, cumpleaños y números de tarjetas de crédito, puede ser robada en un ataque de *phishing* (p. 2).
(Ccasa & Coila, 2021)	De acuerdo a los autores, el sujeto activo, mayoritariamente son los hackers, crackers y otros ciberdelincuentes, tiene al menos cierto nivel de conocimientos técnicos informáticos, lo que lo diferencia de los delincuentes más "tradicionales". Sujeto pasivo: cualquier entidad o persona natural. El *phishing* es un tipo de fraude mediante el cual se roba información personal sobre un usuario para acceder a sus cuentas de internet con el objetivo de comercializar esos datos o entrar a sus cuentas corrientes mediante su clave (pp. 26-28).
(Londoño, 2021)	Los sitios web de cookies recopilan información personal de propietarios y usuarios en internet, a veces sin el conocimiento del usuario y sus visitantes, aquí se hace mención al sujeto activo. Cualquier usuario que visite estos sitios, donde su información y datos privados pueden ser recogidos omitiendo su confidencialidad, se califica como sujeto pasivo (p. 3).

Autor, año	Elementos típicos
(Sanmartín, 2021)	Los sujetos activos que participan, según el autor, son las personas que realizan las conductas que están tipificadas en los tipos penales acerca de los tratamientos de los datos. Así mismo, estas personas poseen especialidades para realizar y utilizar sistemas informáticos. El sujeto pasivo incluye no sólo a las personas, sino también a las instituciones financieras, los gobiernos y las organizaciones internacionales (pp. 22-24).
(Berrio & Orellana, 2022)	La ciberdelincuencia actúa de distintas formas, entre ellas mediante la suplantación de páginas de empresas legales, lo que ocasiona pérdidas a los proveedores mediante supuestas compras que consisten es sustraer información de dichas empresas para generar desembolsos. Los medios que emplean son equipos como laptop y computadoras con el fin de vulnerar dichas páginas web (p. 2).
(Sosa, 2022)	En cuanto a sus elementos típicos, la acción suele consistir en dañar y destruir ordenadores a través de internet, así como por otros medios; el sujeto pasivo es la persona, sin importar que sea persona natural o persona jurídica, cuyo derecho a la confidencialidad se ve invadido; el sujeto activo que actúa puede ser un individuo o grupo de individuos que cuenten con saberes especializados en tecnología; y el medio empleado es el propio ordenador o los sistemas informáticos (p. 21).
(Peralta, 2022)	El autor explica que el sujeto activo es todo aquel que comete la acción que afecta al sujeto pasivo, cuya privacidad, intimidad o incluso patrimonio son vulnerados; los medios empleados son dispositivos computacionales dentro de los sistemas informáticos; y la conducta típica es la de carácter ilícito e ilegal, con el objetivo de destruir o manipular cualquier dispositivo tecnológico (pp. 12-13).
(Sinchiguano, 2022)	El autor se refiere al sujeto activo como aquel individuo que crea y vende *software* y que obtiene acceso no autorizado a un sistema de ordenadores, que podría ser declarado culpable de violar las leyes de privacidad en ambos casos. Cualquier persona cuyo derecho a la seguridad privada y/o informática se haya visto comprometido es el sujeto pasivo. El comportamiento típico, como se mencionó, es crear, vender y acceder ilegalmente a los sistemas informáticos (p. 20).

Autor, año	Elementos típicos
(Huayca, 2022)	Se refiere a los sujetos: sujeto pasivo pueden ser tanto las personas físicas como las jurídicas, incluidas cualquiera que tenga acceso a la información en cuestión, mientras que cualquiera puede ser sujeto activo. El robo de información mediante el acceso no autorizado a sistemas informáticos es el comportamiento típico (p. 3).

Nota. La tabla resalta la comparación en función a los elementos típicos de los diversos delitos informáticos.

Tabla 5

Comparación en función a las conclusiones

Autor, año	Conclusiones
(Román, 2020)	Según las investigaciones del autor, este tipo de delitos es cada vez más frecuentes en las comunidades en línea, donde actúan diversos mecanismos con efectos de gran alcance en la sociedad. Se requieren nuevos principios integradores para los delitos que causan daños informáticos, ya que la legislación vigente incluye lagunas legales que, con frecuencia, quedan impunes. Además, no incorpora una norma jurídica completa que explique cada tipo penal de estos delitos (p. 65).
(Vicencio, 2020)	Hay margen de mejora teniendo en cuenta todos los peligros cada vez mayores para la privacidad a los que la sociedad se enfrenta para mantener sus datos a salvo. El autor concluye que el proyecto de ley ayudará a crear el marco para resolver los desafíos que se muestren en el futuro. Los crecientes volúmenes de datos y las tecnologías más complejas plantean nuevos retos para la seguridad de los datos. Se reconoce que, debido al rápido crecimiento mundial de la tecnología y el proceso de la información, la legislación chilena de 1999 se está quedando obsoleta y se requieren ajustes (p. 31).
(Aredo, 2021)	A modo de conclusión, el autor menciona que, debido al amplio uso de las redes sociales, el *phishing* compromete la seguridad de la información personal con la ciberdelincuencia; además, como los ciberdelincuentes utilizan métodos técnicos sofisticados, puede resultar difícil identificarlos como participantes, causando daños materiales e invadiendo la privacidad (p. 30).
(Ccasa y Coila, 2021)	Se considera a los delitos informáticos como pluriofensivos mediante los cuales los bienes jurídicos tutelados se configuran conjuntamente. En primer

Autor, año	Conclusiones
	orden están los sistemas de información (base de datos) y los sistemas de gestión; en segundo orden están los bienes afectados contra la identidad e intimidad. También existe la afectación a un bien jurídico colectivo en el ámbito informático, que a la vez afecta bienes jurídicos individuales como el patrimonio y la identidad (p. 106).
(Londoño, 2021)	El autor concluye que la norma en base al tratamiento de datos personales debe ser implementada independientemente de los métodos, técnicas y tecnologías utilizadas en la recolección, utilización y tratamiento de dichos datos. Dado que las cookies se colocan en los dispositivos de los interesados con el objetivo expreso de recopilar parte de sus datos personales, cualquier tratamiento de dicha información debe cumplir con los requisitos de la Ley 1581 de 2012 y la normativa reglamentaria asociada (p. 35).
(Sanmartín, 2021)	A pesar de que el Convenio de Budapest o el Código Orgánico Penal de Ecuador tienen descripciones muy similares respecto de los delitos informáticos, se determinó que algunos de los delitos del convenio, como el uso indebido de dispositivos y la infracción de la propiedad intelectual, deberían incluirse en la legislación penal ecuatoriana (p. 86).
(Berrio & Orellana, 2022)	El tráfico ilegal de datos pone al descubierto el secreto bancario mediante el uso de programas informáticos legítimos y documentos de identidad y financieros falsificados, que presume una peligrosa amenaza para la intimidad de las personas (p. 35).
(Sosa, 2022)	En concreto, el autor tuvo como segunda conclusión que el *phishing* no está tipificado explícitamente en la Ley 30096. En cuanto a su tercera conclusión, es necesario que los legisladores amplíen el ámbito de la usurpación de identidad para incluir el *phishing*, a fin de que el Estado pueda castigar eficazmente la actividad delictiva y, al mismo tiempo, mantener la garantía fundamental de legalidad. Sin una tipificación previa, documentada, inequívoca, la actividad ilícita de *phishing* seguirá quedando impune o declarada ilegal (p. 48).
(Peralta, 2022)	En concreto, el autor concluyó que los ciberataques no solo intentan robar el patrimonio, sino también destruir los ordenadores de las víctimas. Estos son ejemplos de ciberataques que exponen datos. Los *hackers* que están detrás de estos asaltos no solo buscan robar patrimonio, también quieren acceder a datos

Autor, año	Conclusiones
	de la empresa y modificarlos potencialmente, lo cual pone de manifiesto la extrema exposición de la información digital en el Perú (p. 22).
(Sinchiguano, 2022)	En la sexta conclusión, el autor tuvo que acceder a un ordenador sin permiso del propietario, lo cual es ilegal en Ecuador y se encuentra tipificado, aunque no lo están las acciones de creación y comercialización necesarias para llevarlo a cabo. En cuanto a la séptima conclusión, se detalla que la solución mencionada en el párrafo anterior es la tipificación de la creación y comercialización sobre la comisión por el delito de accesibilidad no consentida a un sistema informático de comunicación electrónica, de modo que los fiscales y jueces puedan perseguir o condenar eficazmente a los individuos que cometen estos actos. Esto sería coherente con el Estado de derecho, el derecho a un proceso justo y la disuasión de la impunidad (pp. 84-85).
(Huayca, 2022)	El autor concluyó que una las deficiencias que existe en la normativa peruana es la falta de cambios normativos, ya que no se ha introducido ningún modelo nuevo ni se han tenido en cuenta las tecnologías en rápido desarrollo que dejan obsoletas las normas vigentes. Como tercera conclusión el autor sugiere actualizar las leyes que regulan los delitos de fraude informático o suplantación de identidad, ya que están obsoletas y han provocado inseguridad jurídica en la regulación informática y la proliferación de delitos adicionales como el *phishing*, el *malware* o el *skimming* (pp. 36-37).

Nota. La tabla trata sobre la comparación en función de las conclusiones dadas por los autores.

Tabla 6

Comparación en función de las recomendaciones

Autor, año	Recomendaciones
(Román, 2020)	El autor sugiere que, para proteger a la sociedad de la ciberdelincuencia, el sistema jurídico debe tener el peso adecuado. De este modo se garantizará la protección de la privacidad, la seguridad y la disponibilidad de los sistemas informáticos, los datos y las redes, al tiempo que se logra un justo equilibrio entre los intereses de la persecución penal y la estricta defensa de los derechos humanos fundamentales. Para combatir con éxito estos delitos, la Ley 30096 sobre delitos informáticos debería modificarse de conformidad con el Convenio de Budapest sobre ciberdelincuencia. Esto permitirá modificar los tipos penales que contiene (p. 67).
(Vicencio, 2020)	El autor sugiere que, a través de la propuesta del proyecto de ley, se abarque a nivel de toda la sociedad, ya que busca amparar los datos con el fin de generar un mayor conocimiento y educación al derecho a la privacidad y su protección constitucional (p. 28**).**
(Aredo, 2021)	El autor sugiere que el Congreso de la República revise las leyes que rigen los delitos informáticos, a la luz del hecho de que el número de tales delitos se disparó durante la emergencia nacional y persiste hasta el día de hoy, pero las penas existentes para tales delitos son, a menudo, demasiado débiles para disuadir a los autores de estos actos impunes. También sugiere que el congreso aumente el alcance, utilizando frases técnicas más precisas que ayuden a prevenir y perseguir delitos como el *phishing* (p. 31).
(Ccasa & Coila, 2021)	El autor sugiere el refuerzo en las capacitaciones tanto de fiscales como jueces en estos temas especiales como los delitos informáticos, a fin de mejorar en la persecución de los mismos, que son pluriofensivos porque protegen bienes jurídicos colectivos a fin de crearse fiscalías especializadas (p. 108).
(Londoño, 2021)	El autor sugiere que los encargados del manejo de información personal que se apoyen en cookies web para hacerlo, cumplan con sus obligaciones bajo el principio de transferencia; esto incluye conocer los requisitos del artículo 12 para la Ley 1581 de 2012, entre otros; y que es crucial emplear estrategias de responsabilidad demostrada sobre el tratamiento de información privada, e implementar un principio de confidencialidad por diseño (p. 36).

Autor, año	Recomendaciones
(Sanmartín, 2021)	Para reducir los peligros de los incidentes cibernéticos, debe establecerse un marco jurídico más uniforme y se debe contar con más herramientas para perseguir a los autores de delitos cibernéticos de acción local o efecto internacional, lo cual puede lograrse mediante la adhesión y ratificación del Convenio de Budapest por los organismos reguladores nacionales pertinentes (p. 87).
(Berrio & Orellana, 2022)	Los autores sugieren que el Poder Legislativo proponga y evalúe las normas sobre delitos digitales tomando en consideración las convenciones internacionales, sugiriendo una ley que establezca sanciones severas para los criminales que realicen contrabando con datos sensibles, y mencionando en la legislación los procedimientos de control requeridos en las organizaciones bancarias para evitar potenciales desastres financieros (p. 36).

Nota. La tabla trata sobre la comparación de las recomendaciones dada por los autores.

4.2. Discusión

Una vez determinadas las tablas, se prosigue con los resultados a través de una revisión de literatura. Para tal efecto se utilizaron diversos trabajos: antecedentes nacionales con base de datos de Concytec y Renati, y antecedentes internacionales con base de datos de repositorios digitales de las distintas universidades. Todos estos trabajos tienen un periodo de antigüedad que va desde 2018 hasta 2022. Están relacionados con el tema de investigación el tráfico ilegal de datos y la necesidad de una reforma en el Código Penal peruano.

Para dar respuesta al problema de investigación, se tuvo como objetivo general determinar si es necesario modificar el tipo penal del tráfico ilegal de datos en el Código Penal peruano. Se afirma que varios de los autores precisados en las tablas afirman que existe una imperiosa necesidad de una reforma que abarque ampliamente el tema de los delitos informáticos, por la deficiencia y ausencias de diferentes tipos penales nuevos.

De acuerdo a cómo se fueron elaborando los resultados, se describe la tabla 1 de objetivos, que brinda un aporte necesario al propósito de esta tesis, porque explica cómo los

distintos delitos informáticos, los que se encuentran establecidos en la norma y los que aún no se encuentran tipificados, requieren de una modificación normativa, lo cual guarda relación con el objetivo general del estudio, puesto que responde al problema principal que es la necesidad de una modificación normativa del tráfico ilegal de datos personales.

Autores como Vilca (2018), Carrillo y Montenegro (2018), Román (2020), Sosa (2022), Aredo (2021), Huayca (2022), Vicencio (2020) y Sanmartín (2021) coinciden en advertir que en la ley de delitos cibernéticos existen deficiencias legislativas; algunos de los delitos no se encuentran tipificados, mientras que otros no son claros. Dichos autores resaltan la utilidad que tiene la informática en la actualidad para la realización de actos de ciberdelincuencia, por lo cual surgen nuevas modalidades como el *phishing*, la suplantación de identidad y el fraude informático. Son motivos suficientes para sugerir cambios en la norma. Además, no solo sucede en Perú; en países como Chile y Ecuador se busca la creación de una ley a través de la adhesión al Convenio de Budapest, en aras de proteger los datos personales.

Por otro lado, autores como Moreno (2018) y Jacho (2018) discrepan del objetivo general, pues sus sugerencias abarcan más que una modificación normativa, enfatizan la preocupación acerca del amparo de los datos personales, específicamente de menores de edad. Si bien es cierto existe una regulación, se pretende analizar si la misma es suficientemente favorable para que no se afecten los derechos de los menores, ya sea porque no están tipificados o porque no son suficientes.

Del objetivo general, que es determinar si es necesario modificar el tipo penal del tráfico ilegal de datos en el Código Penal peruano, los autores descritos en la tabla 1 ofrecen respuesta al problema de investigación. La tesis de Román (2020) sugiere la modificación de la Ley N.º 30096 para que tengan eficacia dentro del ordenamiento jurídico peruano, esto en virtud de

contrarrestar la ciberdelincuencia. Asimismo, la tesis de Sosa (2022) señala que la ley no expresa de forma clara todos los delitos informáticos, como el *phishing*. Huayca (2022) pretende indicar aquellas insuficiencias que tiene la ley de delitos informáticos.

En tal sentido, hasta que no se modifique la ley de delitos informáticos, seguirán existiendo deficiencias, tales como la falta de cambios normativos en vista del desarrollo de medios informáticos. Además, no se han suscitados cambios nuevos o propuestas legislativas acerca de los delitos informáticos. Otra de las deficiencias es la falta de actualización de los delitos como la suplantación de identidad y el fraude informático; adicionalmente a ellos, figuras como el *phishing* o *maware* no se encuentran contemplados en la ley. Lo mencionado se relaciona con el delito de tráfico ilegal de datos, que también debería ser modificado por no mencionar las nuevas formas o modalidades mediante las cuales se cometen. Por lo tanto, también debería modificarse en el Código Penal y complementarse con los demás delitos informáticos.

Se necesita, por tanto, la modificación e integración de una ley específica que aclare todos los tipos penales de delitos informáticos, no solo el de tráfico ilegal de datos, sino también los nuevos delitos que surgen por la tecnología. Es un motivo suficiente para una adecuada regulación de la normativa, ya que no se puede vulnerar los datos personales de ninguna persona, sobre todo los más expuestos como son los menores de edad.

Como siguiente punto, se tiene la tabla 2 sobre “metodología”. Se resaltan los distintos enfoques que han tenido los autores para tener un estudio sobre los delitos informáticos. Se enfatiza el análisis documental que guarda relación con el objetivo específico uno, acerca de la descripción del tipo penal que conllevó al resultado del mismo en cada uno de esos estudios.

La información de la tabla se relaciona con las investigaciones de Vilca (2018) y Sosa (2022), que coinciden en haber utilizado como técnica el análisis documental. Asimismo, se utilizó la doctrina y la jurisprudencia que sirvieron para analizar las actuaciones delictivas de los delitos informáticos, a través del código penal, libros, revistas, la Ley N.º 30096, etc. Así, los resultados de Sosa (2022), a través de la interpretación de las normativas relacionadas a los tipos penales de delitos informáticos, guardan relación con el objetivo específico uno, que es analizar la idoneidad de la descripción de la conducta típica del tráfico ilegal de datos personales.

Además, Román (2020) utiliza el tipo propositivo a fin de elaborar una propuesta de legislación. Ccasa y Coila (2021) entablan un estudio jurídico-doctrinal que tiene el fin de dilucidar las condiciones que pueden justificar la preservación de un determinado bien jurídico. Lo establecido por los autores tiene relevancia para el estudio, puesto que se utiliza un análisis documental con el fin de analizar si es necesaria la modificación de delitos informáticos.

Los autores discrepan en el sentido de utilizar como técnica la entrevista o la encuesta, en especialistas como abogados, fiscales y jueces que tuvieron experiencia en la ciberdelincuencia, a través de enfoques mixtos como los que fueron utilizados en investigaciones como las de Jacho (2018), Román (2020) y Sanmartín (2021). De esta manera, no guarda relación con nuestro estudio de investigación, ya que la técnica a la que se refieren los autores no fue utilizada.

Respecto al aporte crítico, se necesita un análisis documental que pueda relacionarse con la actividad del tráfico ilegal de datos personales, a fin de realizar un análisis exhaustivo para comprender mejor esta figura delictiva. A pesar de existir distintos enfoques de estudio, el fin inicial es conocer sobre los delitos informáticos, si requieren una modificación normativa y cómo está descrita la conducta típica.

Siguiendo con la discusión, se hace referencia a la tabla 3 que refiere el "bien jurídico tutelado". Brinda aportes al propósito de este estudio, puesto que señala y describe los bienes jurídicos afectados cuando se comete un delito informático; no solo se afecta un bien jurídico, sino varios. Tienen la característica de ser pluriofensivos; es lo que se puede destacar de la mencionada tabla. Además, se relaciona con el objetivo específico tres. A modo general, el bien jurídico afectado es la información personal y la intimidad privada de la persona afectada. Para poder determinar el alcance de la lesión del bien jurídico tutelado en el delito de tráfico ilegal de datos, fue importante analizar cada uno de los bienes jurídicos señalados por los autores.

Al respecto, autores como Blossiers (2018), Vilca (2018), Moreno (2018) y Peralta (2022) coinciden en señalar que el bien jurídico más afectado es la intimidad de las personas y la información privada, así como el tráfico ilegal de datos. Esto se debe a la interacción que tienen las personas al compartir sus datos a través de las redes. Otro grupo de autores coindice en señalar que la lesión de bienes jurídicos se destaca por ser pluriofensiva. Sinchiguano (2022) sostiene que son pluriofensivos porque vulneran la intimidad y la seguridad patrimonial. Reyes (2020) tiene como bien jurídico a la información y los bienes que son afectados, señalando que existen dos clases de intimidad personal: la territorial y la informacional, este último involucra los medios digitales. Román (2020) y Ccasa y Coila (2021) afirman los mismos bienes jurídicos, la información, cuando haya sido almacenada o procesada, y otros como la intimidad o indemnidad sexual.

Dichos discrepan al mencionar que el bien jurídico tutelado no solo es la información. Sanmartín (2021) señala como bien jurídico a la seguridad informática, esta puede ser tanto colectiva como individual. Berrio y Orellana (2022) indican que es la seguridad de la información personal. Por último, Carrillo y Montenegro (2018) conciben que el acceso, la

funcionalidad e integridad de un sistema informático es el bien jurídico, lo cual significa que el bien jurídico que se debe tutelar es la seguridad informática.

El objetivo específico 3, identificar el alcance de la lesión del bien jurídico en el delito de tráfico ilegal de datos personales, da respuesta a las tesis de Blossiers (2018), que indica que la ley de delitos informáticos establece penas cuando se trata de delitos como el tráfico ilegal de datos, donde el bien jurídico lesionado es la privacidad, es decir, la intimidad de las personas.

En ese sentido, Reyes (2020) concibe que el bien jurídico tutelado es la intimidad personal, mediante la cual se protege la invasión de cualquier tercero en la esfera privada y familiar de la persona afectada, y explica que existe la intimidad informacional, aquella que se da con el uso de la tecnológica. De tal modo que el tipo de delito de tráfico ilegal de datos lesiona el bien jurídico tutelado de la intimidad personal, el cual es vulnerado por los *hackers* informáticos o por cualquier persona que tenga a su alcance la información privada del sujeto pasivo. Se vulnera de varias formas, una de ellas es accediendo ilegalmente a la información privada de la persona, natural o jurídica, lo cual pone al descubierto los secretos bancarios mediante el uso de la intimidad informacional que se revela a través de programas computacionales.

De lo señalado y a modo de crítica se puede afirmar que los delitos informáticos tienen un gran grupo de bienes jurídicos que son afectados, no solo los individuales, sino también los colectivos, entre los cuales está la información, lo cual daña en gran magnitud la intimidad de las personas. A diferencia del otro grupo que defiende que el bien jurídico es la seguridad informática.

De la misma forma, los descrito en la tabla 4, elementos típicos, aporta al propósito del estudio, puesto que ayuda a comprender las diferentes conductas típicas. Se hace referencia al tipo objetivo, que indica quién es el sujeto activo, el sujeto pasivo y el objeto material del mismo.

En el tipo subjetivo, se señala el dolo, ya que existe una intencionalidad. Todo ello enriquece el tema y se relaciona con el objetivo específico 1, acerca de la idoneidad de la descripción de la conducta típica del tráfico ilegal de datos personales.

Los autores Carrillo y Montenegro (2018), y Blossiers (2018), coinciden en señalar que el sujeto pasivo es aquel a quien se vulnera su intimidad, aquel que es propietario de la información o titular del sistema informático. De la misma forma, se refieren al sujeto activo como aquel que tiene conocimiento en la informática para causar daños delictivos. Otro aspecto importante es la tipicidad subjetiva, el dolo, porque existe la intencionalidad de acceder o frustrar el adecuado funcionamiento del sistema informático. Sinchiguano (2022) y Huayca (2022) coinciden al decir que el sujeto activo crea y vende *software* por tener acceso sin autorización a varios sistemas informáticos. Por lo tanto, el comportamiento típico es crear, vender y acceder ilegalmente a los sistemas informáticos. Peralta (2022) manifiesta que la conducta típica tiene carácter ilícito, porque el objetivo es destruir y manipular cualquier medio tecnológico.

Por otro lado, Carrillo y Montenegro (2018) discrepan respecto de lo mencionado por otros autores, porque el sujeto activo no tiene que ser fundamentalmente una persona que conozca o tenga cualidades especiales relacionadas con la informática; en otras palabras, puede tratarse de cualquier persona natural que expongan los datos de las personas. Román (2020) también afirma que el sujeto activo puede ser cualquier persona o alguien que tenga un grado de conocimiento; recalca que el sujeto pasivo puede ser una persona natural o jurídica. Sanmartín (2021) y Sosa (2022) sostienen que el sujeto activo debe poseer especialidades sobre el tratamiento de los datos. Además, también se refieren al sujeto pasivo como aquella persona natural, instituciones financieras, organizaciones y gobiernos. La conducta típica es dañar o destruir ordenadores de internet.

De acuerdo a lo descrito se tiene el objetivo específico 1: determinar la idoneidad de la descripción de la conducta típica del tráfico ilegal de datos personales. Autores como Cassa y Coila (2021) indican que el sujeto activo en los delitos informáticos es, en la gran mayoría, el *hacker*, *cracker* y otros ciberdelincuentes que tienen cierto nivel de conocimientos técnicos informáticos. Por otro lado, el sujeto pasivo puede ser una entidad o persona natural. En el *phishing* se roba información personal sobre un usuario para acceder a sus cuentas de internet con el objetivo de comercializar esos datos. Blossiers (2018) afirma que los elementos subjetivos constituyen el dolo porque quieren frustrar el funcionamiento de un sistema. Para Sinchiguano (2022) el comportamiento típico es crear, vender y acceder ilegalmente a los sistemas informáticos.

En consecuencia, otros delitos informáticos como el *phishing* y el acceso no autorizado en los sistemas informáticos, entre otros, se relacionan con el delito de tráfico ilegal de datos personales, porque acceden a información privada con el objetivo de comercializarla ilegalmente. Vender esa información vulnera el derecho de la intimidad de las personas. Existe idoneidad en cuanto a la conducta típica, pero aun así el tipo penal descrito no es suficiente, porque en la descripción misma menciona “el que comercializa o ilegítimamente vende información”, pero no dice a través de qué medios; y sobre la pena, que es no menor a dos ni mayor a cinco años, no refleja el daño que puede ocasionar la vulneración a la privacidad.

De lo mencionado, el aporte crítico es aludir que el solo acceso no autorizado a un sistema informático que tiene un titular vulnera al sujeto pasivo. Cuando se trata de vender esa información, se vulnera el derecho a la intimidad; en cuanto al tráfico ilegal de datos, se trata de comercializar dicha información. Además, no solo se da en personas naturales, sino también en personas jurídicas.

La tabla 5 de conclusiones aporta al estudio porque pretende mostrar cómo en el Perú y en otros países no se encuentran debidamente establecidas las normas relativas a la protección a los datos y delitos informáticos. Varias de las conductas típicas no se encuentran detalladas, otras conductas no se encuentran tipificadas en el Código Penal. Además, esta tabla guarda relación con el objetivo principal, dado que logra comprender la necesidad de regular una norma que detalle de manera concisa todos los delitos informáticos.

Los autores coinciden en varios aspectos: primero, la ley de delitos informáticos es insuficiente porque solo describe el problema, resaltando que varios de esos delitos no se encuentran regulados con precisión, como es el caso del delito de atentar contra la seguridad de los sistemas informáticos, el *phishing*, y actualizar las leyes. Vilca (2018) y Román (2020) afirman que la ley de delitos informáticos es insuficiente y deficiente, pues requiere de principios que integren las lagunas legales en aquellos delitos que quedan impunes. Para Carrillo Montenegro (2018) la cantidad de delitos tecnológicos existentes no se encuentran adecuadamente abordados por el sistema judicial peruano. Sosa (2022) se refiere también a la modificación del apartado de suplantación de identidad, con cualquiera de las formas en las que se roben los datos, con el fin de causar un perjuicio con el contenido de sus datos privados. Estos delitos deben estar sujetos a la misma pena.

Blossiers (2018) muestra su desacuerdo ante una normativa especial porque que, si bien la legislación sobre los delitos informáticos es insuficiente para proteger los intereses de las entidades financieras, no es necesario que se establezca una normativa concreta porque esto debilitaría la seguridad de acciones legales que pueden realizarse con regímenes estrictos. Lo mencionado por el autor no guarda relación con nuestro objetivo general ni con los específicos, ya que no se pretende modificar la normativa, lo cual perjudicaría los sistemas bancarios.

Según el objetivo general: determinar si es necesario modificar el tipo penal del tráfico ilegal de datos en el Código Penal peruano, varios autores incentivan la modificación de la norma. Vilca (2018) indica que, en el Perú, la regulación de los delitos informáticos es insuficiente, ya que solo proporcionan una amplia descripción del problema caracterizando a la ley como deficiente. Esto hace imposible llevar a cabo una investigación forense exhaustiva de los delitos informáticos en el Perú. Según Huayca (2022), una de las deficiencias que existe en la normativa peruana es la falta de cambios normativos, ya que no se ha introducido ningún modelo nuevo ni se han tenido en cuenta las tecnologías que se han desarrollado y que dejan obsoletas las normas vigentes.

Por ello, una modificación de los delitos informáticos conllevaría suplir todas aquellas deficiencias de la ley de delitos informáticos, como la del tráfico ilegal de datos. Por ende, es necesaria la modificación porque estos tipos penales están cambiando constantemente en la sociedad. No existen cambios normativos, la ley necesita ser actualizada. Surgen nuevas formas de delitos que están pasando desapercibidas.

El aporte crítico que se puede dar es que, si bien se necesita una modificación normativa respecto a los delitos informáticos, esto no debe dejar ningún vacío normativo, se tienen que contemplar todos los nuevos delitos que aparezcan a partir de una ley, con el fin de proteger la información y los datos personales de las personas en general.

Por último, se tiene la tabla 6 que se refiere a las recomendaciones. Fue un gran aporte, ya que guarda relación con los objetivos específicos 2 y 4, ofreciendo ideas para una posible solución, a través de políticas criminales y cuáles serían los posibles criterios para la persecución del injusto penal. Si bien el estudio se basa en el tráfico ilegal de datos, es importante señalar qué

aspectos se tienen que tomar en cuenta, como una sección especial en el Código Penal que establezca los delitos informáticos y no solo el tráfico ilegal de datos.

Blossiers (2018) y Vilca (2018) coinciden en modificar la normativa, pero en un solo apartado, es decir, unificado en el Código Penal, y no en diferentes normas, porque los delitos informáticos se actualizan conforme al avance de la tecnología, y esto solo sería posible a través de una sección especial que especifique todos los tipos de delitos informáticos.

Respecto al objetivo específico 2: clasificar los criterios de la política criminal que justifican el rango punitivo establecido en el artículo 154-A del Código Penal, la tesis de Berrio y Orellana (2022) ofrecen una perspectiva interesante, ya que no orientan solo a establecer políticas criminales nacionales, sino que sugieren que el Poder Legislativo cree normas enfocadas en las convenciones internacionales, con el objetivo de establecer sanciones severas para las personas que cometen estos actos delictivos, sobre todo cuando existe un grado mayor, es decir, contrabando de datos sensibles. Asimismo, Moreno (2018) sugiere que se diseñen políticas de calidad contra los peligros que trae el internet. Por tal motivo, también precisa que es necesario una legislación que mantenga el control de los sistemas bancarios.

De acuerdo a los criterios de la política criminal que deberían darse, se resalta que el Poder Legislativo debe acoplarse o ceñirse a las convenciones internacionales, como el Convenio de Budapest, al que Colombia se ha adherido para combatir la ciberdelincuencia y prevenir todo tipo de criminalidad informática. Sería un gran aporte para Perú, en aras de la modificación de los delitos informáticos, para definir los nuevos tipos penales, ya que las penas no son tan severas a pesar de que existe vulneración de bienes jurídicos fundamentales. En consecuencia, se busca exigir sanciones más severas cuando se vulneran datos sensibles.

Así mismo, respecto al objetivo específico 4: describir los criterios procedimentales establecidos por la justicia peruana para la persecución del injusto penal de tráfico ilegal de datos personales, Huayca (2022) menciona que la ley de delitos informáticos debe actualizarse cada año, sobre todo respecto de la multa y el tipo penal para que la actuación del fiscal sea más eficaz. Reyes (2020) sostiene que la fiscalía debe impartir programas o cursos de formación que enseñan a cómo lidiar con estos delitos en sus nuevas modalidades. Para Peralta (2022) los operadores de justicia tienen que capacitarse constantemente acerca de los delitos informáticos, en cuanto se refiera a delitos de alta complejidad, con el fin de utilizar los procedimientos necesarios para la recolección de pruebas informáticas. Por lo tanto, para que la actuación fiscal en materia procedimental sea eficaz, debe actualizarse la ley de delitos informáticos, puesto que estos necesitan de un equipo especializado para contrarrestarlos: el tráfico ilegal de datos, la suplantación de identidad, el secreto de las comunicaciones, el *phishing*, entre otros delitos que utilizan a la tecnología para llevarse a cabo. Los constantes cambios motivan la modificación de la mencionada ley, pues el acceso no consentido a los propios correos, cuentas personales y bancarias es recurrente en estos casos, robando información para el uso ilegal. Se necesita, por tanto, una investigación a profundidad para descubrir si se trata de una organización criminal.

Conclusiones

Primera: según el objetivo general, resulta imperativo modificar el tipo penal de tráfico ilegal de datos actualmente establecido y tipificado en el Código Penal. Para lograr esto de manera efectiva, es necesario actualizar la Ley de Delitos Informáticos, dado que presenta deficiencias al no contemplar cambios normativos que aborden de manera renovada los delitos informáticos tales como la suplantación de identidad, el fraude informático y las nuevas modalidades de ciberdelincuencia como el *phishing*. Estas conductas tienen en común la intrusión en la información personal de las personas, aspecto que guarda estrecha relación con el delito de tráfico ilegal de datos, del cual no se hace mención en cuanto a la descripción de estas nuevas formas de conducta.

Segunda: en relación con el primer objetivo específico, se observa que el tipo penal del tráfico ilegal de datos no está descrito de manera suficiente. Las conductas típicas se limitan a la venta o comercialización ilegal de datos privados, sin abordar de manera exhaustiva las nuevas modalidades que han surgido en la actualidad, especialmente aquellas vinculadas al uso de sistemas informáticos. Este delito guarda una estrecha relación con otros, como el *phishing* y el acceso no autorizado a sistemas informáticos. Además, la penalización actual no se ajusta proporcionalmente al daño causado, y la normativa carece de claridad en cuanto a la forma de sancionar la vulneración de datos en menores de edad, aspecto que podría requerir una pena más severa para garantizar una adecuada protección.

Tercera: en relación al segundo objetivo específico, se destaca la importancia de la política criminal en un Estado, especialmente en el ámbito de los delitos informáticos. De este objetivo se desprende la necesidad de que Perú se adhiera a convenciones internacionales en materia penal, siendo el Convenio de Budapest uno de ellos, con el propósito de contrarrestar la

delincuencia informática. Al referirse a las organizaciones o bandas criminales involucradas en este tipo de actividades, se alude a los sujetos activos, buscando imponer sanciones más severas debido a la gravedad que constituye vulnerar datos e información privada, especialmente cuando se trata de menores de edad. Este enfoque tiene como objetivo garantizar los intereses de las personas mediante la protección de los datos, sin comprometer su derecho a la intimidad.

Cuarta: de acuerdo al tercer objetivo específico, el bien jurídico lesionado en el tráfico ilegal de datos es la intimidad, circunscribiéndose en la intimidad informacional, que es aquella en la cual se utilizan medios informáticos. Por ello, se busca proteger los datos privados. El alcance de la lesión de este bien jurídico primordial alcanza al sujeto pasivo, a través de diversas formas, como acceder a su información personal, familiar, etc. Así mismo, a las personas jurídicas, siendo los *hackers* informáticos los responsables, que en la actualidad son más comunes.

Quinta: con base en el cuarto objetivo específico, que abordan los criterios procedimentales para la persecución del injusto penal. Es esencial considerar la reforma de la Ley de Delitos Informáticos para garantizar la eficacia de la vía procedimental. Se hace necesario contar con un equipo especializado adecuado para la investigación de delitos como el tráfico ilegal de datos, la suplantación de identidad y el acceso no autorizado a las comunicaciones. Estos delitos presentan diversas modalidades, a menudo ejecutadas por organizaciones criminales, lo que representa una amenaza para la información personal. Un ejemplo común de estas prácticas es el *phishing*, un tipo de ataque que intenta obtener información y fondos a través del envío de correos electrónicos fraudulentos, lo cual afecta a cualquier persona.

Recomendaciones

Primera: se sugiere al Poder Legislativo la formulación de una propuesta de ley destinada al análisis y abordaje de los delitos informáticos, que englobe de manera integral tanto las infracciones recientemente identificadas como aquellas ya consagradas en la legislación existente. Esta iniciativa se materializaría en una única disposición legal, específicamente en el Código Penal, con el propósito de ofrecer una estructura clara y comprensible. Se propone la inclusión de una sección especial dedicada a los delitos que afectan el derecho a la intimidad de las personas, bajo el título "Delitos contra la Integridad Informática". Cada subsección y subtítulo abordaría detalladamente las distintas categorías de delitos, brindando así una mayor claridad y coherencia en la normativa.

Segunda: se sugiere considerar no solo la vulneración de la intimidad del público en general, sino también la afectación a las personas jurídicas. En este contexto, las entidades financieras deben fortalecer sus medidas de resguardo y seguridad ante posibles ataques, dada la frecuente participación de organizaciones criminales en estos incidentes. La comercialización ilícita de información, una práctica común en la actualidad, donde se destacan las conductas típicas de venta de datos con el fin de obtener beneficios ilegales, subraya la urgencia de reforzar las salvaguardias en el ámbito financiero.

Tercera: se sugiere que, en el proceso de análisis, el Poder Legislativo considere la relevancia del Convenio de Budapest, del cual Colombia es signatario. Esta recomendación se basa en la contribución que dicho convenio podría aportar para combatir la ciberdelincuencia, especialmente en la definición de un marco punitivo proporcional a la afectación del bien jurídico, que en este caso son los datos personales, en aras de proteger la intimidad de los ciudadanos. Además, es crucial destacar que los menores de edad que utilizan el navegador se

encuentran particularmente expuestos al riesgo de que sus datos sean vulnerados, lo cual hace evidente la necesidad de abordar esta vulnerabilidad de manera integral.

Cuarta: asimismo, se insta al Estado Peruano a otorgar la debida importancia a los delitos informáticos, con el fin de salvaguardar el derecho a la intimidad de los ciudadanos. En la actualidad, se observa una proliferación constante de hackeos que resultan en el robo de cuentas personales, comprometiendo la seguridad de la información de los individuos. En este contexto, resulta recomendable la implementación de un programa destinado a comprender la naturaleza de estos actos delictivos, los cuales se han vuelto cotidianos en la vida diaria debido al amplio uso de internet, incluso con fines de búsqueda de información.

Quinta: es imperativo que tanto el Ministerio Público como el Poder Judicial reciban instrucción específica acerca de los actos delictivos innovadores relacionados con la ciberdelincuencia. A diferencia de otros tipos de delitos, estos surgen en el ámbito de la navegación, de los sistemas informáticos y los datos alojados en la nube e internet. Se hace necesaria la formación de equipos especializados capaces de rastrear a los ciberdelincuentes, permitiendo así la adopción de medidas procedimentales adecuadas a la complejidad de la materia.

Referencias

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos*. [Tesis de pregrado, Universidad César Vallejo]. Repositorio Institucional – UVC. https://repositorio.ucv.edu.pe/handle/20.500.12692/80920

Berrio, E., & Orellana, I. (2022). *El Tráfico Ilegal de Información Digital y Vulneración de los Datos Personales, Patrimoniales, Financieros en las Plataformas de Internet, Lima Este 2022*. [Tesis de grado, Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/112006

Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria* [Tesis de maestría, Universidad Nacional Federico Villarreal]. https://alicia.concytec.gob.pe/vufind/Record/RUNF_081cc155bc9a16d2bf68de65923017eb

Bordachar, M. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO. *Revista Chilena de Derecho y Tecnología, 11*(1), 397-412. https://doi.org/10.5354/0719-2584.2022.67205

Carriedo, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México.* [Tesis de maestría, Infotec]. Infotec Repositorio. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Carrillo, C., & Montenegro, A. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos* [Tesis de grado, Universidad Señor de Sipán]. https://alicia.concytec.gob.pe/vufind/Record/USSS_dd939f09de3b53b6bb7e02999d97d62b

Ccasa, V & Coila, R. (2021). *El tratamiento de los bienes jurídicos colectivos en los delitos informáticos*. [Tesis de pregrado, Universidad Nacional de San Agustín]. https://alicia.concytec.gob.pe/vufind/Record/UNSA_33efc9bd447bc99a5bd92ced71ba30df

Cerezo, A., y & García, R. (2020). La ciberdelincuencia en España: Un estudio basado en las estadísticas policiales. *Revista Peruana de Ciencias Penales, 1*(34), 91-106. https://rpcp.pe/index.php/RPCP/article/view/3

De la Puente, J. (2020). *La intercepción y difusión de las comunicaciones privadas y las libertades comunicativas en el proceso de judicialización peruano. Ponderación, límites e interés público.* [Tesis de maestría, Universidad Nacional de San Marcos]. Repositorio de Tesis – UNMSM. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/15611/DelaPuente_mj.pdf?sequence=1&isAllowed=y

Díaz, C. (2019). *La aplicación de la Ley N°.30096-Ley de delitos informáticos respecto a su regulación en el derecho penal peruano.* [Tesis de grado, Universidad Cesar Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/51569

Espinoza, M., Salinas, A., Santos, M., & Villegas, A. (2018). Breve análisis del delito de tráfico de drogas en la legislación peruana. *Ius et Tribunalis*, *1*(1), 89-107. http://journals.continental.edu.pe/index.php/iusettribunalis/article/view/707

Fernández, P. (2009). *Defensa del Derecho a la Intimidad Frente al Poder Informático.* (Tesis de grado, Universidad Mayor de San Andrés). https://repositorio.umsa.bo/handle/123456789/19915

Ferrero, E., & Schutz, A. (2013). Tráfico de datos personales: su afectación a los derechos personalísimos. *Perspectivas, 3*(2). https://repo.unlpam.edu.ar/handle/unlpam/4113

García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de derecho comparado, 40*(120), 743-778. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003&lng=es&tlng=es.

Hidalgo, Y. (2020). *El paradigma del derecho global para la protección de datos personales en redes sociales.* [Tesis de grado, Universidad Católica Santo Toribio de Mogrovejo]. https://tesis.usat.edu.pe/bitstream/20.500.12423/2808/1/TL_HidalgoZamoraYuriko.pdf

Hiperderecho. (2022). Identificó la comercialización de datos personales. ASBANC.

Huarcaya, L. (2021). *La influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro -2020*. [Tesis de grado, Universidad Peruana de las Américas]. http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1267/HUARCAYA%20BORDA.pdf?sequence=1&isAllowed=y

Huayca, H. (2022). *Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos*. [Tesis de grado, Universidad Cesar Vallejo]. https://alicia.concytec.gob.pe/vufind/Record/UCVV_bbf9c6d62acf415ad061eb2a04f929ec

Infobae. (2022, mayo). *'Zorrito Run Run': Esta es la plataforma que filtró y ofertó los datos personales de los peruanos*. [Infobae.com]. https://www.infobae.com/america/peru/2022/05/20/zorrito-run-run-la-plataforma-que-filtra-y-oferta-los-datos-personales-de-los-peruanos/

Jacho, S. (2018). *Ciberbullying como delito informático en el Derecho Penal Ecuatoriano.* [Tesis de grado, Universidad Central del Ecuador]. http://www.dspace.uce.edu.ec/handle/25000/16601

Londoño, A. (2021). *Tratamiento de datos personales a través de web cookies: análisis bajo la legislación colombiana de protección de datos personales*. [Tesis de maestría, Universidad de los Andes]. https://repositorio.uniandes.edu.co/handle/1992/53613

López, E. (2019). *El delito de narcotráfico en la Deep Web: Una visión desde la Legislación* Ecuatoriana. [Tesis de grado, Universidad San Francisco de Quito]. https://repositorio.usfq.edu.ec/handle/23000/8945

Luna, E. (2021). Preguntas y respuestas varias sobre la protección de datos personales en el Perú. *Advocatus,* (039), 253–264. https://doi.org/10.26439/ADVOCATUS2021.N39.5133

Malatesta, D. (2020). *Las nuevas tecnologías de la información y la vulneración del derecho a la intimidad protegido por el Habeas Data*. [Tesis de maestría, Universidad Andina del Cusco]. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/3584/RESUMEN.pdf?sequence=1&isAllowed=y

Ministerio Publico. (2021). Ciberdelincuencia: Pautas Para Una Investigación Fiscal Especializada. In Oficina de Análisis Estratégico contra la Criminalidad. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1667473-ciberdelincuencia-en-el-peru-pautas-para-su-investigacion-fiscal-especializada

Montes, D. (2021). A vueltas con el terrorismo e internet: hacia una definición de ciberterrorismo. *Revista De Derecho De La UNED (RDUNED),* (27), 697–738. https://doi.org/10.5944/RDUNED.27.2021.31102

Montiel, J. (s.f.). Los Datos Personales y su Protección Durante la Averiguación Previa. http://ru.juridicas.unam.mx/xmlui/handle/123456789/27725

Morales, M. (2020). Los delitos contra la intimidad y la protección de datos personales: la responsabilidad penal del personal de la universidad. *El Criminalista Digital*, (8), 1-29. http://revistaseug.ugr.es/index.php/cridi/article/view/20894

Moreno, D. (2018*). Protección de datos, un juego de niños: reflexiones sobre los derechos de menores a la luz de la protección de datos personales.* [Tesis de grado, Universidad de los Andes de Colombia]. https://repositorio.uniandes.edu.co/handle/1992/40373

Muñoz, L. (2019). *Protección penal de la intimidad personal en las redes sociales*. [Tesis de pregrado, Universidad Nacional del Altiplano]. https://renati.sunedu.gob.pe/handle/sunedu/3226875

Olivos, M. (2020). El derecho a la protección de datos personales en el Perú: 27 años desde su incorporación en la Constitución Política de 1993. *IUS, 9*(1).

Pacheco, L. (2016). ¿Derecho a la intimidad o privacidad empresarial? Gaceta Constitucional y Procesal Constitucional. *Repositorio Institucional PIRHUA,* (101), 33–37. https://pirhua.udep.edu.pe/bitstream/handle/11042/5906/Derecho_intimidad_privacidad_empresarial.pdf?sequence=1&isAllowed=y

Peralta, R. (2022). *Los delitos informáticos y los datos en sistemas informáticos* [Tesis de pregrado, Universidad Peruana de Las Américas]. https://alicia.concytec.gob.pe/vufind/Record/ULAS_6a65ab27a045123f9286a35fe4fea9b6

Presidente de la República. (2013, 22 de marzo). Decreto Supremo 003-2013-JUS. Reglamento de la Ley de Protección de Datos Personales. Normas Legales, 491320. Diario Oficial El Peruano. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf.pdf?v=1643315587

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

Redacción Gestión. (2022). OSCE: denuncian espionaje informático a favor de constructoras chinas. *Gestión*. https://gestion.pe/peru/politica/espionaje-en-osce-habria-permitido-que-constructoras-chinas-ganen-millonarios-contratos-con-el-estado-rmmn-noticia/

Reyes, C. (2020). *Los delitos informáticos y su influencia en la integridad personal, distrito de Chorrillos, Lima metropolitana, 2019*. [Tesis de pregrado, Universidad Peruana de Las Américas]. https://alicia.concytec.gob.pe/vufind/Record/ULAS_d961417a88debe53ee883645e3b62a51

Rivera, B. (2019). Realidad sobre la privacidad de los datos personales en Costa Rica. *E-Ciencias de la Información. 9*(2), 1-13. https://doi.org/10.15517/ECI.V9I2.37503

Rodríguez, R. (2016). ¿Qué seguridad? Riesgos y amenazas de internet en la seguridad humana. *Araucaria, 18*(36), 391–415.

Román, E. (2020). *Modificación legislativa de la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo.* [Tesis de grado, Universidad Señor de Sipán]. https://alicia.concytec.gob.pe/vufind/Record/USSS_87c1d5b262cd4ba551d1ef78bd7dafc1

Sanmartín, W. (2021). *Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest*. [Tesis de grado, Universidad Central del Ecuador]. http://www.dspace.uce.edu.ec/handle/25000/25177

Sinchiguano, J. (2022). *Las acciones típicas de desarrollo y comercialización de programas informáticos, para el cometimiento del delito de acceso no consentido a un sistema de información y comunicación*. [Tesis de grado, Universidad Central de Ecuador]. http://www.dspace.uce.edu.ec/bitstream/25000/28508/1/FJCPS-CD-SINCHIGUANO%20JEFFERSON.pdf

Sosa, O. (2022). *Phishing como modalidad de delitos informáticos: A propósito de la suplantación y robo a los beneficiarios del Bono Universal en el Perú*. [Tesis de grado, Universidad Nacional de Piura]. https://alicia.concytec.gob.pe/vufind/Record/RUMP_13672070317d092739dbd2259a3c80eb

Téllez, C. (2015). Nuevas tecnologías y nueva privacidad en el Código Penal peruano. *Foro Jurídico,* (14), 126–131. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/13756/14380

Trávez, N. (2019). *La vulneración de los Derechos Constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación (TICs).* (Tesis de grado, Universidad Central de Ecuador).

Vera, M., & Vivero, M. (2019). ¿Vida privada o muerte a la privacidad?: Protección de datos personales en la relación empresa-cliente en Ecuador. *USFQ Law Review*, 6(1), 233–256. https://doi.org/10.18272/LR.V6I1.1397

Vicencio, N. (2020). *Nueva ley de datos para Chile: Proyecto de ley para la modernización normativa en la protección de datos personales en Chile: análisis evaluativo y desafíos*. [Tesis de posgrado, Pontificia Universidad Católica de Chile]. https://repositorio.uc.cl/handle/11534/52687

Vilca, G. (2018). *Los hackers delito informático frente al código penal peruano*. [Tesis de pregrado, Universidad Nacional Santiago Antúnez de Mayolo]. https://alicia.concytec.gob.pe/vufind/Record/RUNM_73d3678c5046384ec6a0a8d6f799353a

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS,* (49), 284–304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, (053), 95–110. https://doi.org/10.26439/IUSETPRAXIS2021.N053.