UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE DERECHO

ESCUELA DE DERECHO

Normativa penal en la protección de datos personales: criterios para prevenir delitos informáticos en el Perú

TESIS PARA OPTAR EL TÍTULO DE

ABOGADO

AUTOR

Renzo Miguel Chicoma Calderon

ASESOR

CinthyaCrisa Dunyoli Gastulo Muro

https://orcid.org/0000-0002-8905-4333

Chiclayo, 2025

Normativa penal en la protección de datos personales: criterios para prevenir delitos informáticos en el Perú

PRESENTADA POR

Renzo Miguel Chicoma Calderon

A la Facultad de Derecho de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

ABOGADO

APROBADA POR

Elky Alexander Villegas Paiva
PRESIDENTE

Renzo Paul Taboada Diaz
SECRETARIO

CinthyaCrisa Dunyoli Gastulo Muro
VOCAL

Dedicatoria

Dedico esta tesis a mi familia, por su amor y apoyo incondicional en cada etapa de mi vida. En especial, a mi hermana Anyela, cuya fortaleza y ejemplo han sido mi mayor inspiración. Este logro también forma parte de ellos.

Agradecimientos

Agradezco profundamente a mi asesora de tesis, CinthyaCrisa Gastulo Muro, por su guía y compromiso durante este proceso, y a mi profesora de titulación, Ana María Llanos, por su constante apoyo e inspiración. Este logro no habría sido posible sin la confianza y el respaldo de ambas.

ARTICULO FINAL

INFORME DE ORIGINALIDAD

5%	6%	5%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	cybertesis.unmsm.edu.pe Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%
3	Submitted to Universidad Andina del Cusco Trabajo del estudiante	1%
4	repositorio.ucv.edu.pe Fuente de Internet	<1%
5	habeasdatacolombia.uniandes.edu.co Fuente de Internet	<1%
6	www.informaticaforense.com.co Fuente de Internet	<1%
7	tesis.usat.edu.pe Fuente de Internet	<1%
8	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
9	iij.ucr.ac.cr	

Índice

Resumen

La investigación buscó proponer criterios técnicos y jurídicos para fortalecer la infraestructura regulatoria de protección de datos personales en el Perú, con el fin de prevenir y mitigar la incidencia del cibercrimen. Para ello, se establecieron tres objetivos: primero, analizar los criterios esenciales para la efectiva regulación de los delitos informáticos; segundo, comparar la legislación peruana con los marcos normativos de Chile y Colombia; y tercero, establecer medidas normativas concretas para mejorar la respuesta penal e institucional frente a las amenazas digitales. Metodológicamente, el estudio tuvo un enfoque cualitativo, con diseño descriptivo y análisis documental de legislación, doctrina, jurisprudencia y fuentes científicas. Los principales resultados establecen que, a pesar de contar con un marco normativo formal, el Perú presenta serias deficiencias estructurales como la falta de tipificación de delitos emergentes, ausencia de tribunales especializados y baja operatividad de la autoridad de control. Se proponen criterios para la actualización de la legislación, la cooperación con los proveedores de Internet, la creación de órganos especializados y la armonización con tratados internacionales como el Convenio de Budapest. Estos criterios reforzarán la respuesta institucional a la ciberdelincuencia, promoviendo la seguridad digital y garantizando el derecho a la intimidad en el entorno cibernético.

Palabras clave: derecho penal, protección de datos, delitos informáticos, seguridad digital.

Abstract

The research sought to propose technical and legal criteria to strengthen the regulatory infrastructure for the protection of personal data in Peru, in order to prevent and mitigate the incidence of cybercrime. To this end, three objectives were established: first, to analyze the essential criteria for the effective regulation of cybercrime; second, to compare Peruvian legislation with the regulatory frameworks of Chile and Colombia; and third, to establish concrete regulatory measures to improve the criminal and institutional response to digital threats. Methodologically, the study had a qualitative approach, with descriptive design and documentary analysis of legislation, doctrine, jurisprudence and scientific sources. The main results establish that, despite having a formal regulatory framework, Peru has serious structural deficiencies such as the lack of typification of emerging crimes, absence of specialized courts and low operability of the control authority. Criteria are proposed for updating legislation, cooperation with Internet providers, the creation of specialized bodies and harmonization with international treaties such as the Budapest Convention. These criteria will strengthen the institutional response to cybercrime, promoting digital security and guaranteeing the right to privacy in the cyber environment.abstract

Keywords: criminal law, data protection, computer crimes, digital security.

Introducción

A lo largo de la historia, la humanidad ha perseguido incansablemente el crecimiento, la innovación, alcanzando avances tecnológicos que se han vuelto indispensables en múltiples aspectos de la vida cotidiana. Sin embargo, esta dependencia tecnológica también presenta riesgos significativos, ya que puede generar problemas de seguridad y facilitar el robo de información. La proliferación de la tecnología digital ha incrementado la vulnerabilidad ante la ciberdelincuencia, exponiendo a individuos y organizaciones a ataques cibernéticos, fraudes y otras amenazas que comprometen su privacidad y seguridad.

En el mundo, la globalización y el avance tecnológico han traído herramientas útiles, pero también nuevos tipos de delitos, dentro de ellos los delitos informáticos. Los cuales, debido a su naturaleza y especialización, son difíciles de perseguir e investigar. La preocupación principal radica en cómo estas acciones afectan la convivencia social. Por lo que, hay una seria necesidad de adaptar el derecho penal a los retos que plantea el mundo digital en la actualidad. (Leyva Serrano, 2021)

En América Latina, la protección de datos personales ha sido una preocupación creciente, especialmente con el aumento del uso de tecnologías digitales. Varios países de la región, influenciados por estándares internacionales como el Reglamento general de protección de datos (RGPD) de la Unión Europea, han promulgado leyes específicas para regular el tratamiento de la información personal. Aunque algunos países han mostrado avances significativos en este ámbito, otros enfrentan desafíos en la implementación efectiva y el cumplimiento de estas leyes. (Enríquez Álvarez, 2019)

En el Perú, la protección de datos personales está regulada por la Ley N° 29733, influenciada por el marco europeo. Esta ley garantiza el derecho a la autodeterminación informativa, permitiendo a los individuos controlar su información. No obstante, la protección efectiva enfrenta desafíos debido a la creciente incidencia de delitos informáticos. (Franco García & Quintanilla Perea, 2020)

Por lo que, la problemática principal radica en una protección débil de los datos personales, que se traduce en una exposición constante a riesgos de ciberataques. Simultáneamente, la dificultad en la identificación de los infractores complica la imposición de sanciones, creando un ambiente de impunidad y debilitando la eficacia de las leyes penales.

Las causas de esta es que las leyes no están lo suficientemente actualizadas para abordar adecuadamente los delitos informáticos y la protección de datos en el ámbito penal. Aunque existan leyes que regulen la protección de datos y la prevención de delitos informáticos, su aplicación y cumplimiento pueden ser deficientes debido a limitaciones en los recursos, falta

de capacitación de las autoridades responsables, infraestructura tecnológica insuficiente y falta de inversión en ciberseguridad, etc.

Asimismo, la falta de conocimiento sobre nuevas tecnologías y la desinformación trae como consecuencia el aumento de la vulnerabilidad ante delitos informáticos, resultando en la pérdida de datos personales. Por otro lado, la falta de conciencia sobre los riesgos tecnológicos facilita el acceso no autorizado a información personal, comprometiendo su protección. Finalmente, la evolución constante de los delitos cibernéticos agrava la dificultad de proteger los datos personales adecuadamente al tener una estructura débil en la ley. (Arapa Ticona y otros, 2024)

En este contexto, se plantea la pregunta problema: ¿Qué criterios deberán considerarse en la regulación de los delitos informáticos para la protección de datos personales en el Perú? Por lo que, si se implementan estos criterios para identificar, rastrear y sancionar a los infractores de la protección de datos, junto con campañas de concientización sobre seguridad cibernética, es probable que se reduzca la incidencia de ataques cibernéticos y la vulnerabilidad de la información personal en línea.

En función a esta problemática, se planteó como objetivo general: Establecer criterios técnicos y legales necesarios para fortalecer la infraestructura normativa y legal sobre la protección de datos personales en el Perú con respecto a la ley delitos informáticos, con el fin de prevenir y mitigar delitos informáticos. Asimismo, se establecieron como objetivos específicos: analizar criterios esenciales para la regulación de los delitos informáticos en el Perú, con el fin de prevenir y mitigar su incidencia, garantizando la seguridad y privacidad de la información de los ciudadanos y comparar la legislación chilena tomando en cuenta la ley 21459, la ley 1273 colombiana sobre delitos informáticos con la normativa peruana en especial la ley 30096 de delitos informáticos.

La justificación de esta investigación sobre la normativa penal en la protección de datos y la prevención de delitos informáticos en el Perú se sustentó en la necesidad de adaptar el marco legal nacional a los desafíos actuales del entorno digital, caracterizado por la proliferación de conductas ilícitas que vulneran la privacidad y seguridad de los ciudadanos. A pesar de la existencia de normas como la Ley N.º 29733 y la Ley N.º 30096, estas presentan vacíos técnicos, tipológicos y operativos que impiden una respuesta penal efectiva y oportuna.

De este modo, esta investigación tiene como aporte contribuir al fortalecimiento de la normativa penal en la protección de datos personales en el Perú, elaborando criterios para identificar, rastrear y sancionar a los infractores, así como la promoción de la conciencia pública sobre la importancia de proteger la información personal en línea.

I. Revisión de la literatura

1.1. Antecedentes

1.1.1. Nacionales

Los antecedentes en una investigación son los trabajos previamente realizados por otras personas que están relacionados con el tema que se está investigando actualmente. Estos sirven como punto de partida, proporcionando un contexto y una base de conocimiento sobre el objeto de estudio de la investigación. (Arispe Alburqueque y otros, 2020, pág. 33)

Palacios Cuba (2021) en su tesis, *"Los Delitos Informáticos contra Datos, y su vulneración al Derecho de la Intimidad Personal, en la Ciudad de Ayacucho, 2020"*, la tesis se centra en cómo los delitos informáticos afectan el derecho a la intimidad personal en Ayacucho, destacando los daños psicológicos que generan al vulnerar la privacidad y crear inseguridad en el uso de tecnologías digitales. Analiza específicamente el rol de las redes sociales en la obtención de información personal, lo que aumenta la gravedad de estos delitos. Además, los análisis sobre cómo estos delitos vulneran derechos fundamentales en un contexto local (Ayacucho) y la necesidad de actualizar normativas podrían complementar comparaciones con las leyes de Chile, Colombia y Perú, especialmente en lo relacionado con la protección de datos y la seguridad informática.

Ventura (2021) en su tesis titulada *"La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020",* se centra en la necesidad de adaptar la legislación penal peruana a las nuevas modalidades de ciberdelitos, específicamente el phishing (suplantación mediante correos electrónicos), smishing (engaños a través de mensajes de texto) y vishing (fraudes mediante llamadas telefónicas), la autora propone su tipificación como delitos autónomos dentro de la Ley 30096 y su modificatoria, para combatir la creciente ciberdelincuencia y garantizar la seguridad jurídica en un entorno digital cada vez más complejo. En este sentido, esta tesis es altamente relevante para tu investigación, ya que se alinea con el objetivo de fortalecer la normativa penal en el ámbito de los delitos informáticos en Perú, su enfoque en modalidades concretas y su impacto en derechos fundamentales y patrimoniales aporta una base sólida para reforzar las propuestas de prevención y tipificación en nuestro trabajo.

Ccama (2021) en tesis su titulada *"El Delito contra Datos Informáticos Personales en el Derecho Fundamental a la Intimidad Personal en la Corte Superior de Justicia de Puno 2020"*, analiza el impacto de los delitos informáticos relacionados con datos personales en el derecho fundamental a la intimidad personal, según la perspectiva de los operadores de justicia en Puno. El estudio evalúa cómo estas infracciones afectan distintas dimensiones del derecho a la

intimidad, como la confidencialidad, la integridad de los sistemas informáticos, la privacidad y la reserva, destacando las correlaciones y porcentajes de afectación de cada una de estas dimensione. Por lo que, esta tesis contribuye proporcionando un análisis empírico sobre el impacto de los delitos informáticos en el derecho a la intimidad personal en el contexto peruano.

Rivera (2022) en su tesis titulada *"En búsqueda del equilibrio entre la protección de datos personales, el deber de transparencia y el derecho de acceso a la información pública"*, investiga cómo balancear estos tres derechos fundamentales en Perú, basándose en la evolución histórica y normativa de la protección de datos en Europa, Estados Unidos y Latinoamérica. Además, analiza casos específicos y jurisprudencia peruana donde estos derechos entran en conflicto. Propone criterios para que las autoridades competentes en Perú logren un equilibrio razonable entre la privacidad de los datos personales y la transparencia del Estado, considerando también la aplicación del derecho al olvido y los métodos de ponderación jurídica. Esta tesis ayudará en nuestra investigación debido a que, toma derechos indispensables no solo en el plano social, sino en el espacio socio-digital, asimismo, ofrece ejemplos prácticos y metodologías jurídicas, como principios, que son útiles para establecer criterios técnicos y legales para fortalecer la protección de datos y prevenir delitos informáticos.

Ocupa (2023) , en su tesis titulada *"Aplicación del convenio de Budapest y delitos informáticos en el Perú, 2022"*, analiza cómo el Estado peruano ha implementado el Convenio de Budapest para sancionar delitos informáticos. Esta se enfoca en cómo este tratado ha mejorado la cooperación internacional y el fortalecimiento de la legislación peruana en la tipificación de delitos como el fraude, acceso ilícito a sistemas y la suplantación de identidad. Además, examina cómo el convenio ha impulsado mejoras en las técnicas investigativas y en la coordinación entre países, con el fin de enfrentar los ciberdelitos. Ocupa concluye que el Convenio ha sido clave para fortalecer la legislación peruana, facilitando la persecución de estos delitos y protegiendo la seguridad de la información y la privacidad. Esta tesis puede ser de gran ayuda para nuestra investigación sobre la normativa penal en la protección de datos personales en Perú, ya que proporciona un análisis detallado de cómo un tratado internacional ha influido en la legislación local.

Carrero (2024) por su parte en su tesis titulada *"Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos"*, analiza el incremento de esta modalidad de ciberdelito en Perú, destacando la insuficiencia de la Ley 30096 para tipificar claramente este delito. Propone la incorporación del phishing como modalidad específica en el artículo 8 de dicha ley, argumentando que ello fortalecería el marco normativo, facilitaría la persecución penal y disminuiría la incidencia de estos delitos, siendo esta tesis relevante al aportar un análisis

detallado de un tipo específico de ciberdelito y su impacto en la seguridad de los datos personales, siendo su propuesta importante como ejemplo para integrar criterios específicos que fortalezcan el marco legal peruano, alineando su protección de datos con estándares internacionales. Además, refuerza la importancia de adaptar la legislación a las nuevas formas de criminalidad informática, objetivo que ambos compartimos.

1.1.2. Internacionales

Gómez (2014) en su tesis titulada "Ciber-criminalidad: Nuevos Retos para la Seguridad Pública", aborda los desafíos que la cibercriminalidad plantea a la seguridad pública, enfocándose en los delitos informáticos, la evidencia digital y el rol de la policía cibernética en México. Analiza también la legislación sobre delitos informáticos y los retos que enfrenta la policía cibernética en su implementación y eficacia. Por lo que, esta tesis aporta un análisis profundo sobre los delitos informáticos y el rol de la policía cibernética, lo cual puede contribuir a nuestro estudio sobre cómo la normativa penal en Perú podría fortalecerse para prevenir y mitigar estos delitos. Además, ofrece una perspectiva sobre la recolección de evidencia digital, un tema que puede ser útil para establecer criterios en la legislación peruana para proteger datos personales.

Sánchez (2019) en su tesis titulada *"La tipificación del delito de acceso ilícito a sistemas y equipos de informática en México"*, analiza cómo este delito vulnera el bien jurídico de la información y si la normativa mexicana es adecuada frente a los estándares internacionales. Su estudio permite contrastar con la legislación peruana (Ley 29733 y Ley 30096), evaluando si esta cubre de forma suficiente el acceso no autorizado y otros delitos informáticos. Además, los vacíos normativos identificados en México sirven como referencia para detectar posibles deficiencias similares en el Perú que limiten la sanción efectiva de estas conductas. Asimismo, examina cómo el acceso ilícito, hacking y sabotaje informático afectan bienes jurídicos fundamentales, como la privacidad, lo que servirá para resaltar cómo los delitos informáticos vulneran el derecho a la protección de datos personales en Perú.

La tesis de Peña (2023), titulada *"Delitos Cibernéticos",* trata sobre el impacto creciente de los delitos cibernéticos en el sector financiero, analizando la responsabilidad de las entidades bancarias y las debilidades del sistema judicial en Colombia frente a la protección de los usuarios. Se discuten la falta de seguridad en las transacciones en línea, la necesidad de un marco normativo más robusto, y la importancia de ajustar los protocolos de seguridad a estándares internacionales para combatir eficazmente la ciberdelincuencia. La tesis de Peña contribuirá a nuestra investigación con respecto a que ofrece un análisis sobre la

responsabilidad de las entidades bancarias en Colombia por no implementar medidas de seguridad adecuadas, lo que es relevante para proponer criterios legales claros en Perú que asignen responsabilidad en la protección de datos personales. Además, el estudio analiza la falta de desarrollo jurisprudencial en Colombia sobre delitos informáticos, lo que podría servir para identificar vacíos normativos en la legislación peruana y plantear mejoras en la interpretación judicial.

Cornejo (2023), en su tesis titulada "La investigación de delitos informáticos y su prueba en materia penal", aborda principalmente el papel de la policía en la investigación de los delitos informáticos, un área en crecimiento debido al aumento del uso del ciberespacio. El trabajo examina la evolución histórica de los delitos informáticos, las normativas internacionales y chilenas, y las técnicas de investigación utilizadas para perseguir estos delitos. También se centra en la Ley 21.459 de Chile, que tipifica los delitos informáticos, y destaca las atribuciones de la policía para mejorar la recolección de pruebas en casos penales. Ello ayudará en mi investigación debido a que proporciona una base sobre las técnicas de investigación en delitos informáticos, lo cual es útil para analizar la implementación de mejores mecanismos en la normativa penal peruana. Además, ofrece un análisis comparado de la legislación chilena en ciberseguridad, que podría usar para comparar con las leyes peruanas en protección de datos y delitos informáticos. Por último, expone las facultades de la policía en la persecución de delitos cibernéticos, lo que puede inspirar criterios para mejorar la respuesta en Perú frente a estos crímenes.

Cuellar & Astaiza (2023), en su tesis titulada *"Análisis Dogmático de los Delitos Informáticos o Ciberdelitos en Colombia",* se centran en un análisis exhaustivo de los ciberdelitos desde una perspectiva penal en Colombia. El trabajo analiza cómo la Ley 1273 de 2009 reformó el Código Penal para abordar los ciberdelitos, enfocándose en delitos como el acceso no autorizado a sistemas informáticos, la interceptación de datos, el fraude informático y el daño a sistemas. La tesis se organiza en torno a tres objetivos principales: explicar la génesis de los ciberdelitos en Colombia, describir los mecanismos normativos vigentes para proteger contra estos delitos, y explorar los límites y alcances del marco legal en su aplicación. Esta tesis también discute las dificultades que enfrenta la justicia en la lucha contra los ciberdelitos, como la adaptación de la ley a la rápida evolución tecnológica, las limitaciones de recursos y capacidades técnicas de las autoridades, y la creciente complejidad de los ataques cibernéticos. Esto ayudará a nuestro trabajo de investigación debido a que proporciona un marco legal colombiano que será usado como referencia para comparar la Ley 1273 de Colombia y la Ley 30096 de delitos informáticos en Perú.

1.2. Bases teóricas

1.2.1. Delito informático y la criminalidad informatica

1.2.1.1. Concepto delito informático y criminalidad informatica

El delito informático es todo acto humano culpable ejecutado con empleo de herramientas informáticas, que lesiona bienes jurídicamente protegidos los cuales están amparos por la ley, y que se encuentra tipificado y sancionado en el marco legal vigente. (Narvaez Montenegro, 2015). Asimismo, se reconoce que cualquier persona con acceso a medios informáticos puede cometer delitos en este ámbito, independientemente de su experiencia técnica, no se requiere un conocimiento especializado para ser considerado un autor de delitos informáticos, ampliando así las técnicas de tipificación. (Carbajal Camones, 2022)

Carrillo & Montenegro (2018) señalan que el delito informático se refiere a acciones que afectan bienes jurídicos específicos relacionados con la seguridad y confidencialidad de datos almacenados, transmitidos o procesados digitalmente. Es decir, se trata de actividades que comprometen la integridad y el acceso legítimo a información sensible en entornos digitales, poniendo en riesgo la privacidad y la seguridad tanto de individuos como de organizaciones.

Asimismo, el delito informático se refiere a las infracciones que se cometen utilizando sistemas informáticos o el ciberespacio. Algunas personas consideran más apropiado el término "ciberdelitos", ya que resalta el enfoque en el ciberespacio como escenario principal de estas conductas. Estas acciones pueden tener lugar desde cualquier ubicación física y afectar a diversos bienes jurídicos simultáneamente. (Millán López, 2023)

Estos a su vez son llamados delito cibernético o ciberdelito y son toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Además, poseen un carácter transfronterizo, los cuales puede ser realizados por un solo sujeto o en conjunto más personajes u organizaciones criminales dentro y fuera de un determinado país. (Cornejo Contreras, 2023)

Con lo expuesto anteriormente, entendemos que los delitos informáticos son conductas ilícitas realizadas por criminales cibernéticos haciendo empleo de la tecnología para conseguir de esta forma vulnerar y lesionar un bien jurídico relevante como los datos personales de las personas, los cuales son empleados a favor de estos ciberdelincuentes para generar un mayor agravio en los derechos de las personas afectadas.

Por otro lado, los delitos informáticos están relacionado con la criminalidad informática que son aquellas actividades que buscan evadir o romper las barreras de seguridad en dispositivos tecnológicos. Esto incluye el acceso no autorizado a computadoras, correos electrónicos o sistemas de datos al emplear contraseñas o claves de acceso sin permiso. Lo esencial de estas

conductas es que dependen de la tecnología para llevarse a cabo, es decir, no se pueden realizar sin el uso de herramientas tecnológicas. (Villavicencio Terreros, 2014)

Asimismo, también llamada delincuencia informática se refiere a cualquier acto o conducta ilegal y criminal que tenga como objetivo alterar, socavar, destruir o manipular un sistema informático o cualquiera de sus componentes, con la intención de causar daño o poner en peligro cualquier bien jurídico. (Acurio Del Pino, 2016)

La criminalidad informática, entonces, es entendida como el uso ilegal de la tecnología con el propósito de infiltrarse en sistemas informáticos protegidos, acceder a datos personales o confidenciales de manera no autorizada, manipulando y dañando estos sistemas con la intención de causar perjuicio o poner en riesgo la seguridad y la integridad de individuos, organizaciones o infraestructuras digitales.

1.2.1.2. Características de los delitos informáticos

Los delitos informáticos se destacan por involucrar actividades ilícitas que aprovechan el entorno digital, lo que los convierte en un fenómeno único dentro del mundo del crimen. Su naturaleza digital no solo amplía el alcance y la velocidad con la que pueden ocurrir, sino que también los dota de una serie de características que los diferencian de los delitos tradicionales. Estas particularidades no solo permiten identificarlos de manera más clara, sino que también presentan desafíos específicos para su prevención y persecución.

Una de las características principales de estos delitos es que son actividades ilícitas que se efectúan en entornos digitales, empleando herramientas electrónicas como computadoras, redes y sistemas informáticos, el cual está regulado en la ley N° 30096 y es sancionado por el código penal peruano (Urdanegui Rangel, 2023, pág. 14)

Por otro lado, los delitos informáticos pueden ser perpetrados de forma masiva y automática. Se menciona a la automatización ayudada por el computador a poder procesar y transferir de forma automatizada estos datos, asimismo, los atacantes pueden utilizar programas que replican los ataques repetidamente sin una intervención constante del mismo. (Acurio Del Pino, 2016)

Otra característica y de las más complejas es el anonimato, la posibilidad de actuar de forma anónima o utilizando identidades falsas en línea es una característica frecuente en los delitos informáticos, lo que dificulta la identificación de los autores lo que se traduce a que muchos de estos casos suelen quedar impunes. (Estrada Salvador Ramirez, 2024)

Por último, esta la trasnacionalidad la cual gracias al internet permite que estos puedan ocurrir en varias jurisdicciones simultáneamente, o pueden realizarse en un país y tener sus consecuencias o resultados en otro. (Temperi, 2018)

De este modo entendemos que los delitos informáticos destacan por aprovechar las características únicas del entorno digital, lo que permite su ejecución masiva y automática, y facilita el anonimato y la trasnacionalidad. Por lo que estas particularidades dificultan la identificación y persecución de los autores, planteando desafíos específicos para la legislación y las autoridades.

1.2.2. Datos personales y su protección

1.2.2.1. Concepto de datos personales y el derecho a ser protegidos

El dato personal se refiere a información que identifica o hace identificable a una persona. Incluye datos no sensibles, con acceso al público y datos sensibles. La distinción radica en que los datos sensibles requieren una mayor protección debido a su potencial para afectar la privacidad y la dignidad de las personas. (Córdova Abregú, 2023)

Por otro lado, son definidos como cualquier información que posibilite relacionar o identificar a una persona. Esto incluye no solo datos que por sí solos son claramente personales, sino también aquellos que, aunque individualmente podrían no ser considerados personales, al ser combinados o analizados junto con otros, pueden revelar la identidad de una persona. (Mubarak Aguad, 2020, pág. 209)

De este modo, a criterio personal, el dato personal es toda información que permita identificar a una persona mediante su vinculación con esta. Estos pueden públicos y privados, de estos últimos destaca su carácter sensible, al ser información confidencial que de filtrarse sin autorización generaría un perjuicio en la persona.

Los delitos informáticos a su vez vulneran un derecho como la protección de los datos personales, el cual es un derecho fundamental que permite a las personas controlar cómo se utilizan sus datos personales, oponiéndose a usos no autorizados y protegiendo su dignidad y derechos. Asimismo, este derecho asegura que los datos no sean manipulados de forma ilícita y que cada individuo tenga el poder de decisión sobre su información persona. (Polo Roca, 2021, pág. 215)

Este derecho es la facultad que otorga a las personas la capacidad de salvaguardar su información privada y de decidir sobre su uso, esto incluye el control sobre quién puede acceder a la información, el control del contenido y la posibilidad de restringir su uso el cual tenga diferentes fines. (Olivos, 2020)

Entendemos así que, el derecho de protección de datos personales es un derecho fundamental que permite a las personas controlar el uso y la gestión de su información personal, otorgándoles la capacidad de decidir quién puede acceder a sus datos, qué tipo de información se puede recopilar, cómo se puede utilizar y los fines con los que serán utilizados. Además, implica

proteger la integridad y la confidencialidad de los datos personales con el propósito de prevenir su uso indebido, su manipulación ilegal o su divulgación no autorizada.

1.2.2.2. Consecuencias de la vulneración de los datos personales

Las consecuencias de los delitos informáticos son amplias y afectan diversos aspectos de la vida personal y profesional. Estos crímenes no solo ponen en riesgo la seguridad de los datos, sino que también generan repercusiones económicas, legales y sociales. Además, pueden impactar la confianza en las instituciones y servicios digitales, que cada vez son más esenciales en nuestra sociedad. Es por ello, que Arapa & otros (2024) nos menciona las siguientes consecuencias:

1. **Económicas**: Abarcan las pérdidas financieras que sufren las víctimas, ya sean individuos, empresas o entidades públicas y privadas. Estas pérdidas pueden provenir de fraudes, robos de información, o extorsiones.
2. **Reputacionales**: Los delitos informáticos pueden dañar la reputación de personas y empresas, generando desconfianza tanto en los clientes como en los socios comerciales.
3. **Psicológicas y emocionales**: Afectan principalmente a usuarios que no están familiarizados con los sistemas informáticos, como personas mayores o jóvenes que suelen ser más confiados, lo que puede generar ansiedad, estrés o miedo ante el uso de la tecnología.
4. **Robo de información confidencial**: Los ciberdelitos pueden comprometer la seguridad de datos personales o empresariales, afectando la privacidad y seguridad de las víctimas

Por otro lado, desde el punto de vista financiero, las pérdidas son millonarias, afectando tanto a empresas como a individuos. A nivel social, los delitos informáticos generan inseguridad e incertidumbre, pues afectan a todas las clases de la sociedad, sin importar el nivel económico o el perfil de las personas. Jurídicamente, estos delitos plantean desafíos para la regulación, ya que su carácter técnico dificulta la identificación de responsables y la aplicación de sanciones adecuadas. (Valencia Álvarez, 2020)

En este sentido, los delitos cibernéticos impactan en el ámbito financiero, generando pérdidas económicas para personas, empresas y gobiernos; en el emocional y psicológico, al causar miedo e inseguridad; y en el social, debilitando la confianza en los sistemas digitales. Estos ataques afectan a todos, mostrando que nadie está completamente seguro en el entorno digital.

1.2.3. Regulación de los delitos informáticos en el derecho comparado y en el Perú

1.2.3.1. Normativa latinoamericana, Perú, Chile y Colombia

Las leyes de delitos informáticos en Perú, Colombia y Chile presentan diferencias importantes en términos de alcance y actualización. En Colombia, la Ley 1273 de 2009 fue pionera en la región, al añadir un capítulo específico sobre la protección de datos y sistemas informáticos en el Código Penal. En comparación, Chile, con su Ley N° 21.459 de 2022, actualizó su normativa para alinearla con el Convenio de Budapest, un estándar internacional para combatir ciberdelitos.

Un aspecto clave en las diferencias es la protección de los datos personales. La legislación colombiana destaca por incluir penas claras por la violación de datos, imponiendo sanciones a quienes accedan, manipulen o utilicen información sin autorización, lo que le da un enfoque de protección integral. Chile, por otro lado, introduce el concepto de receptación de datos, penalizando el almacenamiento y comercialización de información obtenida ilícitamente. En Perú, la protección de los datos personales está regulada de manera complementaria a la Ley de Delitos Informáticos mediante la Ley N° 29733 de Protección de Datos Personales. Esta ley peruana se enfoca en garantizar el derecho de los ciudadanos a la privacidad, estableciendo sanciones severas para quienes accedan, manipulen o divulguen información personal sin consentimiento. A diferencia de Colombia, donde la protección de datos está integrada en la Ley 1581.

Las agravantes específicas en cada país también difieren notablemente. En Colombia, las penas por delitos informáticos se agravan si afectan sistemas estatales o financieros, o si se cometen con fines terroristas. (Sanchez Castillo, 2017). En Chile, las sanciones son más severas si los delitos afectan servicios de utilidad pública, como electricidad o telecomunicaciones, lo que refleja una preocupación por proteger infraestructuras críticas. En cambio, Perú tiene una normativa general sin un enfoque específico en sectores esenciales, lo que supone una limitación. En cuanto a la cooperación internacional, Chile ha avanzado más que Perú contra los ciberdelitos, al adecuar su Ley N.º 21.459 al Convenio de Budapest, lo que le permite una mejor coordinación con otros países, Perú también sigue estos principios con la Ley N.º 30096 y la Ley N.º 29733, pero aún presenta limitaciones técnicas y normativas que afectan la efectividad de dicha cooperación.

1.2.3.2. Protección de los datos personales en el ámbito digital: Principios del RGPD

El RGPD se ha convertido en un estándar internacional, reconocido en más de 160 países, reflejando lo que algunos llaman el "efecto Bruselas", en el que la Unión Europea establece estándares globales. Esto ha transformado las políticas de privacidad y ha instaurado una cultura

de protección de datos, tanto entre los responsables del tratamiento como entre los ciudadanos. Es por ello, que Barrio (2024) menciona los siguientes principios esencial de RGPD:

- **Legitimidad**: Este principio asegura que los datos personales se utilicen solo para fines legales y legítimos, respetando el derecho de las personas a la intimidad. Esto exige que el procesamiento sea justo, lícito y basado en una base legal específica, y que las empresas no se consideren propietarias de los datos, sino administradoras responsables que deben proteger la privacidad.
- **Proporcionalidad**: Los tratamientos de datos deben limitarse a lo estrictamente necesario para cumplir con sus fines específicos. Este principio implica la minimización de datos y la limitación en el tiempo de su almacenamiento, garantizando que no se utilicen datos personales en exceso o fuera de los propósitos iniciales.
- **Empoderamiento**: Los interesados tienen el derecho de controlar sus datos personales mediante el acceso, la rectificación y la eliminación de sus datos cuando lo deseen. Esto da a los ciudadanos la capacidad de decidir sobre el uso de su información y el poder de oponerse a tratamientos que puedan vulnerar su privacidad.
- **Transparencia**: Este principio garantiza que los individuos reciban información clara sobre quién está tratando sus datos, cómo se usan y cuáles son sus derechos, permitiéndoles comprender completamente el impacto de ese tratamiento en su privacidad.
- **Responsabilidad Proactiva**: Exige a los responsables del tratamiento implementar medidas preventivas y mantener registros actualizados que demuestren el cumplimiento del RGPD. Este enfoque implica un cambio de responsabilidad, donde los encargados deben asegurar, de forma activa, que los datos personales se traten adecuadamente y puedan justificar su cumplimiento.
- **Seguridad**: Los responsables del tratamiento deben aplicar medidas técnicas y organizativas adecuadas para proteger los datos contra el acceso no autorizado, pérdidas o destrucción accidental. Este principio incluye la seudonimización y el cifrado como herramientas para garantizar la seguridad y la resiliencia de los sistemas de tratamiento de datos, y establece protocolos para notificar a las autoridades en caso de una violación de seguridad significativa

Por otro lado, el RGPD no solo se limita a definir los datos personales desde un punto de vista netamente informático sino también después un punto medico definiendo los datos de

salud de manera amplia, incluyendo información genética y biométrica. Estos datos, como códigos únicos o muestras biológicas, pueden identificar a una persona y, por ello, se consideran "especialmente protegidos". Esto significa que los datos deben tratarse bajo una protección rigurosa debido a su naturaleza delicada y su potencial para revelar información de salud presente, pasada y futura de los individuos. (Beltrán Aguirre, 2018)

Estos principios han ayudado en la normativa peruana con la Ley de Protección de Datos Personales (Ley N° 29733) y su reglamento, vigentes desde 2013, que establecen los principios, derechos y obligaciones sobre el tratamiento de datos personales. En 2017, se fortaleció el marco con el Decreto Legislativo 1353, lo cual mejoró las capacidades de la Autoridad Nacional de Protección de Datos Personales (ANPD), encargada de supervisar y sancionar las prácticas de manejo de datos en entidades públicas y privadas. Sin embargo, aun hay retos en la aplicación práctica y en la consolidación de una cultura de protección de datos entre empresas y ciudadano. (Luna Cervantes, 2021)

1.2.3.3. Evolución de delitos informaticos y nuevas amenazas

La ciberdelincuencia ha evolucionado en respuesta a los avances tecnológicos y cómo esto plantea nuevas amenazas y desafíos. Originalmente, los delitos informáticos se limitaban a acciones como accesos no autorizados o daños simples a sistemas informáticos. Sin embargo, la expansión del ciberespacio ha creado un ambiente donde las amenazas pueden extenderse rápidamente a nivel global, comprometiendo redes y sistemas informáticos en múltiples jurisdicciones, creando así nuevos retos y amenazas.

Acurio (2016) nos señala que los delincuentes organizados aprovechan los avances tecnológicos, especialmente en las comunicaciones, que les permiten operar de forma más flexible, rápida y global. De esta forma, las redes criminales usan el internet y herramientas de comunicación avanzadas para cometer fraudes en línea y para coordinar sus actividades sin importar las distancias.

Por otro lado, Pérez (2021) señala que entre las nuevas amenazas destaca el uso de botnets (redes de dispositivos infectados controlados de manera remota), que permiten ataques masivos y simultáneos, como los de denegación de servicio (DDoS), y pueden utilizarse para actividades delictivas como el fraude, la extorsión o el ransomware mejor entendido como el secuestro de datos.

Asimismo, el crecimiento del uso de la tecnología es evidente en especial el uso de redes sociales las cuales nos permiten comunicarnos con diferentes personas e interactuar en un mundo social cibernético, sin embargo, los menores están cada vez más expuestos a delitos como el grooming, el sexting, el ciberbullying y el ciberacoso, donde los delincuentes

aprovechan su falta de experiencia para manipularlos y obtener su información personal. En el grooming, los agresores se ganan la confianza de los menores con fines sexuales; mientras que, en el sexting, las víctimas comparten contenido íntimo que puede ser difundido sin su consentimiento. Tanto el ciberbullying como el ciberacoso los exponen a humillaciones, chantajes y amenazas. Estos delitos son difíciles de controlar por el anonimato en internet y el acceso sin supervisión. (Jiménez Rozas, 2022)

En este sentido, vemos como la ciberdelincuencia ha avanzado juntamente con los avances tecnológicos los cuales suponen nuevas alternativas para vulnerar sistemas de seguridad, así como la creación de nuevos delitos o formas de ataques a estos sistemas, ampliando el alcance y complejidad de sus amenazas, desde accesos no autorizados hasta fraudes masivos y ransomware. Además de la exposición de menores a delitos como el grooming, sexting, ciberbullying y ciberacoso, aprovechando su vulnerabilidad y el anonimato en línea.

II. Materiales y métodos

El paradigma interpretativo promueve una visión holística y flexible del conocimiento, que integra la subjetividad humana y considera la diversidad cultural como un elemento fundamental. Además, destaca la influencia de factores históricos, culturales y sociales en la configuración de estas experiencias. Asimismo, sugiere que el conocimiento es un proceso humano en constante evolución, que se transforma y se abre a nuevas posibilidades epistemológicas. (Miranda Beltrán & Ortiz Bernal, 2020). En este sentido, esta investigación tiene como punto de flexión el paradigma interpretativo pues, explica una realidad problemática que ha sido causada del constante cambio en la tecnología. Este enfoque interpretativo también permite explorar las múltiples perspectivas, tales como los grupos afectados por los delitos informáticos, así como por las medidas de protección de datos.

Por otro lado, se ha utilizado el enfoque cualitativo como menciona Salazar (2020) este enfoque destaca la importancia de la vida cotidiana como escenario fundamental para comprender y desarrollar las diferentes dimensiones del mundo humano, poniendo énfasis en su carácter único, multifacético y dinámico. En este sentido, esta investigación emplea este enfoque porque permite analizar la problemática actual relacionada con la creciente incidencia de delitos informáticos en el Perú, especialmente en un contexto donde la normativa penal sobre protección de datos personales enfrenta desafíos como la falta de claridad en su aplicación, la insuficiente capacitación de los operadores de justicia y las limitaciones tecnológicas para su implementación. A través del análisis cualitativo, se busca comprender cómo estos factores interactúan en la práctica y afectan la efectividad de las estrategias preventivas, con el fin de

proponer criterios específicos que respondan a esta realidad y contribuyan a un sistema penal más robusto frente a los delitos informáticos

Este trabajo es de tipo básica explicativa, Nicomedes (2018) menciona que esta representa un nivel avanzado de investigación que se centra en la verificación de hipótesis causales o explicativas en el ámbito científico-social. Su objetivo principal es descubrir nuevas leyes científico-sociales o micro teorías que expliquen las relaciones causales entre las propiedades o dimensiones de los hechos, eventos y procesos sociales. De este modo, esta investigación responde al tipo básica explicativa, ya que, examina las relaciones causales entre la legislación existente y la efectividad en la prevención de delitos informáticos. Además, se investiga cómo la aplicación de la normativa penal influye en la disminución o aumento de los delitos informáticos en el país.

Ahora, en cuanto a las técnicas de investigación, Medina & otros (2023) mencionan que son procedimientos sistemáticos utilizados para recopilar y analizar datos con el objetivo de resolver problemas o responder preguntas de investigación. Por lo tanto, las técnicas empleadas durante la presente investigación fue la investigación de documentos para la investigación, ya que permite examinar leyes, casos judiciales y documentos legales relevantes para entender cómo se aplican y cumplen las regulaciones relacionadas con la protección de datos en el país, si como también el uso de fichas que es indispensable para reunir y organizar información relevante de distintas fuentes, las cuales aportan de forma significativa en las cuestiones que aborda esta investigación.

Con respecto a las fuentes de información se ha usado el tipo de fuente documental tal como menciona Maranto & González (2015) son cualquier recurso que proporciona datos que permiten reconstruir hechos o ampliar el conocimiento sobre un tema específico los cuales son fundamentales para el proceso de búsqueda y acceso a la información. Por lo tanto, para esta investigación resulta más viable el usar fuentes bibliográficas que permitan un mejor entendimiento y comprensión para el desarrollo de esta tesis.

Por último, en cuanto a la recolección de datos, se han usado diez (10) tesis, de las cuales cinco (5) son de origen nacional y cinco (5) internacional. Estas investigaciones han sido fundamentales para ampliar la comprensión sobre la normativa penal vinculada a la protección de datos personales y su papel en la prevención de delitos informáticos en el Perú. A través del análisis de estos trabajos, se ha logrado obtener un panorama más claro sobre el contexto, los retos y las medidas necesarias para regular y prevenir este tipo de actividades ilícitas, constituyendo una base clave para el desarrollo de este proyecto de investigación.

Por otro lado, las revistas y artículos científicos han jugado un papel importante en la construcción de las bases teóricas y las categorías conceptuales de este estudio. Se utilizaron dieciséis (27) artículos especializados en delitos informáticos y protección de datos personales, de alcance nacional e internacional. La información recopilada de estas fuentes guarda una estrecha relación con los conceptos fundamentales de la investigación, aportando un sustento sólido y confiable. Estos materiales también han facilitado un análisis más exhaustivo y detallado de las teorías y conceptos esenciales, fortaleciendo el marco teórico y garantizando que las categorías conceptuales estén claramente definidas y respaldadas por la literatura.

III. Resultado y discusión

En el presente capitulo se muestran los resultados y la discusión de estos apartados, teniendo en cuenta los objetivos que sustentarán la propuesta y aporte del trabajo. En primer lugar, se analizaron criterios propuestos por diferentes autores en relación con los delitos informáticos emergentes y las medidas necesarias para fortalecer su persecución penal. Asimismo, se comparó la legislación peruana, particularmente la Ley N.º 30096 sobre delitos informáticos y las normativas de Chile (Ley N.º 21.459) y Colombia (Ley N.º 1273), identificando buenas prácticas, avances normativos, evaluando así el grado de adecuación de la legislación peruana frente a los estándares y enfoques adoptados en la región. Finalmente, se propusieron criterios esenciales para la regulación de la protección de datos personales en el Perú con el fin de prevenir y mitigar la incidencia de delitos informáticos.

Análisis de los criterios esenciales para la regulación de la protección de datos personales en el Perú, con el fin de prevenir y mitigar la incidencia de delitos informáticos, garantizando la seguridad y privacidad de la información de los ciudadanos.

En estas líneas, se analizó los criterios propuestos por distintos autores, lo cual permitió identificar los factores normativos e institucionales que incidieron positiva y negativamente en la efectividad de dichos mecanismos. Ello se fundamentó en la Teoría de la Ciberseguridad Penal Preventiva, la cual propone anticipar, mitigar y disuadir los delitos informáticos mediante estrategias normativas, institucionales y técnicas enfocadas en la protección del ciberespacio como nuevo escenario delictivo. Trujillo (2024) en su artículo “Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en el Perú” hace uso de esta teoría implícitamente analizando los retos que enfrenta el país en materia de ciberseguridad y proponiendo estrategias preventivas desde el ámbito penal para enfrentar la cibercriminalidad, alineándolas con los principios de anticipación y prevención en la legislación penal frente a los delitos informáticos. En este sentido, los criterios considerados por la doctrina son los siguientes:

1. **Delimitación del uso de tecnologías de vigilancia**

Zamudio (2021) aborda la falta de regulación específica sobre el tratamiento de datos personales de los trabajadores, especialmente en relación con tecnologías como la geolocalización GPS, además, propone la aplicación del principio de proporcionalidad y la adecuación de la normativa interna de las empresas para garantizar los derechos fundamentales de los empleados. En este sentido, la protección de datos en el ámbito laboral es crucial para evitar abusos y garantizar la privacidad de los trabajadores. En el Perú, la ausencia de una regulación específica en esta materia deja un vacío que puede ser explotado por empleadores sin escrúpulos, en este sentido, establecer normas claras que delimiten el uso de tecnologías de vigilancia y protejan los derechos de los empleados contribuiría a un entorno laboral más justo y respetuoso de la privacidad. Es por ello que esto abarca más allá del ámbito penal, y se relaciona con una cuestión de derechos fundamentales en el ámbito del trabajo. De ello se desprende que, la falta de regulación específica sobre el tratamiento de datos personales de los trabajadores no solo puede dar lugar a abusos en términos de control y vigilancia, sino que también afecta a la autonomía personal de los empleados y su derecho a la privacidad.

2. **Activación de los pilares del tratamiento adecuado de información**

Además, Zamudio (2021) identifica los principales desafíos que enfrenta el Perú en la garantía del derecho fundamental a la protección de datos personales, señala la necesidad de activar los tres pilares del tratamiento adecuado de la información: el responsable del tratamiento, la autoridad de control y el titular del dato, para consolidar un Estado Constitucional de Derecho en materia de protección de datos. En este caso, la implementación efectiva de la protección de datos personales en el Perú requiere de un enfoque integral que involucre a todos los actores antes mencionados. Por lo que, es necesario fomentar la responsabilidad de quienes manejan datos, fortalecer las capacidades de la autoridad de control y empoderar a los ciudadanos para que ejerzan sus derechos, solo mediante una colaboración coordinada y comprometida se podrá garantizar una protección adecuada de los datos personales en el país.

3. **Incorporación del derecho a la portabilidad de datos personales**

Gabriela Bolaños (2022) por su parte, analizó la necesidad de incorporar el derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano. Su investigación propone mecanismos legales y técnicos que permitan a los titulares reutilizar sus datos en el entorno digital, fortaleciendo así su autodeterminación informativa. En este sentido, la portabilidad de datos es esencial en la era digital, donde los usuarios interactúan con múltiples plataformas y servicios. En este sentido, la implementación de este derecho en el Perú permitiría a los

ciudadanos tener un mayor control sobre su información personal y facilitaría la competencia entre proveedores de servicios. No obstante, su adopción requiere de una infraestructura tecnológica adecuada y de una normativa clara que establezca los procedimientos y responsabilidades de las partes involucradas.

4. **El principio de seguridad como protector de los datos personales**

Asimismo, Vásquez (2022) resalta el principio de seguridad como un pilar en la protección de datos personales. Este principio implica la implementación de medidas proactivas y reactivas que preserven la confidencialidad, integridad y disponibilidad de la información, siendo esencial para la prevención de delitos informáticos. En este contexto, la seguridad de los datos personales es fundamental para prevenir accesos no autorizados y posibles delitos informáticos. Sin embargo, muchas organizaciones en el Perú carecen de políticas y procedimientos adecuados para garantizar esta seguridad. Es necesario promover una cultura de seguridad de la información, capacitar al personal y establecer sanciones efectivas para quienes incumplan con las medidas de protección establecidas.

5. **El derecho al olvido**

Por último, Franco & Quintanilla (2020) exploran el reconocimiento del derecho al olvido en el Perú, en consonancia con los estándares internacionales del Sistema Interamericano de Derechos Humanos, analizando las limitaciones y retos que enfrenta este derecho en el contexto peruano, especialmente en relación con la libertad de expresión y la privacidad. En este sentido, el derecho al olvido permite a los individuos solicitar la eliminación de información personal que ya no es relevante o que afecta negativamente su reputación, por lo que su implementación en el Perú debe equilibrar adecuadamente el derecho a la privacidad con la libertad de expresión y el acceso a la información.

El análisis desarrollado permitió concluir que, pese a los avances formales de la normativa peruana en protección de datos personales, persistían limitaciones estructurales y operativas que impedían su eficacia como mecanismo preventivo frente a delitos informáticos emergentes. Se constató que la ausencia de criterios claros sobre portabilidad, seguridad de la información y control efectivo por parte de la autoridad de protección, evidenciaban un rezago frente a estándares internacionales. Asimismo, quedó demostrado que incorporar un enfoque de Ciberseguridad Penal Preventiva no solo resulta pertinente, sino urgente para anticipar riesgos y fortalecer la resiliencia digital del Estado peruano.

Comparación de la legislación chilena tomando en cuenta la ley 21459 y la ley 1273 colombiana sobre delitos informáticos con la normativa peruana en especial la ley 30096 de delitos informáticos.

Se analizó de manera comparativa la normativa penal vigente en Perú, Chile y Colombia en materia de delitos informáticos, tomando como referencia la Ley N.º 30096 del Perú, la Ley N.º 21.459 de Chile y la Ley 1273 de Colombia, constatando que ambos países han logrado incorporar mecanismos más eficaces de cooperación internacional, tipificación penal especializada y fortalecimiento institucional en la persecución de delitos cibernéticos, elementos que aún presentan un déficit en el ordenamiento peruano.

Desde la perspectiva de la Teoría del Derecho Penal Adaptativo, esta situación evidencia que el Perú necesita transitar desde un modelo penal reactivo hacia un modelo proactivo, capaz de anticipar y disuadir nuevas formas de criminalidad digital. Esta teoría sostiene que el derecho penal debe evolucionar para responder a los cambios sociales y tecnológicos, actuando no solo como un mecanismo de castigo, sino como una herramienta de prevención adaptativa. Asimismo, Agustina (2022) menciona que el ciberespacio ha transformado la forma en que se cometen los delitos, generando nuevas oportunidades delictivas que desafían el principio de territorialidad, la tipicidad clásica y los mecanismos tradicionales de persecución penal. Propone que el derecho penal debe dejar de ser "autopoyético" (cerrado en sí mismo) y abrirse a una visión interdisciplinaria, incorporando conocimientos de criminología, sociología, tecnología y comunicación para comprender la nueva realidad delictiva.

Asimismo, se advierte que la Ley N.º 21.459 de Chile y la Ley 1273 de Colombia ofrecen enfoques complementarios en la regulación de delitos informáticos, destacándose por elementos innovadores que podrían ser adaptados al contexto peruano. En el caso chileno, esta legislación se alinea con el Convenio de Budapest, promoviendo la cooperación internacional y definiendo con precisión los delitos relacionados con la infraestructura crítica, como el sabotaje informático. Según Bascur & Peña (2022), la Ley 21.459 actualiza la normativa relativa a los delitos informáticos en Chile, estableciendo nuevos tipos penales, reglas de sanción y procesales, lo que representa un avance significativo en la adecuación de la legislación nacional a los estándares internacionales. Por su parte, la normativa colombiana se enfoca en la protección integral de los datos personales, estableciendo agravantes cuando se afectan sistemas estatales o financieros. Guarnizo (2020) destaca que la Ley 1273 de 2009 incorporó al Código Penal colombiano la protección de la información y los datos como bienes jurídicos, permitiendo tipificar y penalizar delitos cometidos contra estos, aunque señala que el avance tecnológico requiere una actualización constante de la legislación para abordar nuevas formas de criminalidad digital.

En contraste, la Ley N.º 30096 del Perú se limita a una enumeración básica de delitos informáticos, sin abordar de manera exhaustiva las nuevas modalidades delictivas que emergen

con los avances tecnológicos. Alcántara (2024) señala que existen vacíos u omisiones legales dentro de la presente ley, lo que permite a los ciberdelincuentes aprovecharse de estas deficiencias. Por ejemplo, mientras que las leyes chilena y colombiana contemplan sanciones específicas para el acceso no autorizado a sistemas y la interceptación de datos, la normativa peruana carece de un desarrollo similar, lo que dificulta la identificación y persecución de estas conductas.

Asimismo, Cornejo (2023) en su tesis titulada *"La investigación de delitos informáticos y su prueba en materia penal"*, analiza la legislación chilena a partir de la Ley 21.459, destacando la importancia de modernizar los marcos normativos y dotar de mayores facultades investigativas a la policía especializada en delitos cibernéticos. A diferencia de Perú, que aún no cuenta con unidades especializadas ampliamente operativas ni con formación avanzada para jueces en esta materia, Chile ha avanzado en la creación de sistemas técnicos de recolección de evidencia digital y protocolos de investigación ajustados a los estándares del Convenio de Budapest.

Del mismo modo, Cuellar y Astaiza (2023) en su tesis *"Análisis dogmático de los delitos informáticos o ciberdelitos en Colombia"*, explican cómo la Ley 1273 reformó el Código Penal colombiano para incorporar una tipificación más clara y detallada de conductas delictivas como la interceptación de datos, el sabotaje informático y la manipulación de sistemas. A diferencia del marco peruano, que carece de especificidad en estos delitos, la normativa colombiana incluye agravantes cuando estos afectan al sistema financiero o instituciones del Estado, elevando las penas y priorizando su persecución.

Por otro lado, Peña (2023) en su tesis *"Delitos Cibernéticos"*, analiza los desafíos que enfrenta el sistema judicial colombiano frente a la cibercriminalidad, y resalta la necesidad de juzgados especializados para enfrentar con mayor eficacia los delitos digitales. Esta propuesta encuentra eco en la necesidad peruana de implementar órganos judiciales especializados, algo que ya forma parte de la política criminal chilena. Peña enfatiza que la falta de una respuesta institucional robusta contribuye a la impunidad, situación también presente en el Perú, donde las fiscalías y juzgados no siempre cuentan con formación técnica en criminalidad informática

Asimismo, Mejía**,** Hurtado & Grisales (2023) señala que a pesar de haber firmado el Convenio de Budapest, no ha desarrollado adecuadamente un marco jurídico que permita su implementación eficaz. A diferencia de Chile y Colombia, que cuentan con normativa nacional coherente con dicho tratado internacional, el Perú aún mantiene vacíos normativos sobre delitos como el acceso indebido a sistemas, la suplantación de identidad o la comercialización de datos personales. Mientras qué, Colombia ha integrado las disposiciones del Convenio en su

legislación nacional a través de la Ley 1273 de 2009 y la Ley 1928 de 2018, fortaleciendo la protección de la información y los datos personales, y estableciendo mecanismos de cooperación internacional. Es por ello, que Perú debe ampliar la tipificación de delitos informáticos para incluir todas estas conductas descritas en el Convenio de Budapest. Según Huamán (2020), la Ley N.º 30096 no abarca completamente las disposiciones del Convenio, lo que limita la capacidad del país para cooperar eficazmente en la lucha contra la ciberdelincuencia. En contraste, Chile ha avanzado en la implementación del Convenio mediante la promulgación de la Ley N.º 21.459 en 2022, que actualiza y amplía la tipificación de delitos informático, conforme a las normas internacionales, además se ha implementado la formación de sistemas técnicos para la recolección de pruebas digitales y protocolos de investigación acorde a los estándares del Convenio de Budapest. (Novoa Toledo & Venegas Cruz, 2020)

Finalmente, se concluyó que los marcos normativos de Chile y Colombia presentaban criterios clave para la regulación efectiva de la criminalidad digital, tales como la incorporación de agravantes cuando se afectan infraestructuras críticas, la consideración de la responsabilidad penal de personas jurídicas, y la adopción de estándares de cooperación internacional en la persecución y recolección de evidencia digital. Estos elementos permiten no solo mejorar la respuesta punitiva del Estado, sino, desde una perspectiva preventiva, anticipar y disuadir conductas delictivas en el entorno digital. Por tanto, se evidenció que para que el Perú logre una regulación adecuada de los delitos informáticos y de protección de datos personales, resulta indispensable incorporar estos criterios, modernizar la tipificación penal, fortalecer las capacidades técnicas de los operadores de justicia y adecuar sus normas a los estándares del Convenio de Budapest, superando así la brecha existente con las legislaciones de sus países vecinos.

Criterios técnicos y legales necesarios para fortalecer la infraestructura normativa y legal sobre la protección de datos personales en el Perú, con el fin de prevenir y mitigar delitos informáticos.

En el desarrollo del presente estudio, se advirtió la problemática relacionada con la insuficiencia normativa y estructural del marco penal peruano en lo referente a la protección de datos personales frente a la creciente amenaza de los delitos informáticos. En esta sección se establecieron los criterios técnicos y legales necesarios para robustecer la infraestructura normativa y legal que regula la protección de datos personales en el Perú, como estrategia preventiva frente al avance de los delitos informáticos. Para ello, se evaluaron tanto las debilidades existentes en el marco legal vigente como las oportunidades de mejora,

considerando la rápida evolución del entorno digital y las nuevas formas de criminalidad asociadas al uso indebido de la información personal. El estudio partió del reconocimiento de que los datos personales constituyen un bien jurídico especialmente vulnerable en la era digital, cuya protección requiere no solo de normas claras y actualizadas, sino también de mecanismos institucionales eficaces, cooperación interinstitucional e internacional, así como de operadores jurídicos capacitados para enfrentar los desafíos técnicos de esta nueva criminalidad.

Ante esta problemática constatada, se planteó la siguiente pregunta problema de investigación, orientada a guiar el desarrollo del presente objetivo: ¿Qué criterios deberán considerarse en la regulación de los delitos informáticos para la protección de datos personales en el Perú? Esta interrogante surge de la constatación de que, aunque existen normas como la Ley N.º 29733 y la Ley N.º 30096, su efectividad se ve limitada por la falta de actualización legislativa, operatividad institucional y articulación internacional.

Desde este enfoque adaptativo**,** la Teoría de la Responsabilidad Penal Informática propone adaptar el derecho penal tradicional a la realidad digital, considerando las particularidades técnicas del ciberespacio. Esta teoría resalta que el delito informático requiere una imputación que contemple no solo la conducta típica, sino también el entorno virtual, las herramientas tecnológicas y la intencionalidad del agente. En este sentido, Montano (2024) sostiene que los delitos informáticos no necesariamente constituyen una nueva categoría de delitos, sino que son formas innovadoras de cometer ilícitos tradicionales, lo cual plantea desafíos interpretativos importantes para el sistema penal. En el Perú, la Ley N.º 30.096 no tipifica adecuadamente delitos emergentes como el *phishing* o el *ransomware*, lo que dificulta su sanción. Por ello, esta teoría hace referencia a la capacidad del derecho penal para sancionar a aquellos que cometen delitos utilizando medios electrónicos, informáticos o virtuales, como el acceso no autorizado a sistemas, el robo de datos, el fraude electrónico, el ciberacoso, entre otros. en delitos complejos y en constante evolución. En este sentido, propongo estos criterios con el fin de prevenir delitos informáticos:

1. **Tipificación de nuevos delitos emergentes**

Los delitos cibernéticos emergentes, como el phishing, el ransomware y otros más, representan una amenaza significativa en el entorno digital contemporáneo. Sin embargo, la Ley N° 30.096 del Perú presenta vacíos en la tipificación de estas conductas, lo que complica su identificación y sanción. La normativa actual no abarca de manera adecuada las nuevas modalidades delictivas, limitando la capacidad de las autoridades para actuar con eficacia y generando un ambiente de impunidad en el ámbito cibernético. Este desfasaje legislativo

debilita la protección de datos personales y facilita la proliferación de ataques cibernéticos que afectan tanto a individuos como a organizaciones.

Asimismo, la evolución de las tecnologías de la información ha impulsado la aparición de nuevas modalidades delictivas que desafían los marcos legales tradicionales. En esta misma línea, la investigación de Carrero (2024), destaca con urgencia la necesidad de incluir nuevas modalidades como el phishing de forma expresa en la legislación penal peruana, debido a su alta frecuencia y al impacto devastador que produce sobre los usuarios menos informados tecnológicamente. Asimismo, advierte que la ambigüedad normativa actual obstaculiza la persecución penal, por lo que la tipificación clara no solo fortalecería la sanción, sino también la prevención. Este criterio es relevante porque permite visibilizar conductas que afectan directamente la privacidad y seguridad de los datos personales. Sin embargo, su adopción implica afrontar desafíos técnicos y políticos, como definir los elementos objetivos del tipo penal sin vulnerar el principio de legalidad o criminalizar en exceso conductas digitales.

2. **Cooperación de los proveedores de servicio de internet**

Otro eje fundamental para reforzar la infraestructura normativa está vinculado a la cooperación regulada con los proveedores de servicios de internet (ISP). En el entorno digital, estos actores ocupan una posición estratégica, dado que administran la infraestructura de red sobre la que circulan los datos personales y, por ende, pueden colaborar en la identificación de usuarios, en la retención de metadatos y en la preservación de evidencia digital. Establecer mecanismos de colaboración técnica entre las autoridades judiciales y los ISP permitiría agilizar investigaciones penales complejas y rastrear con mayor precisión las rutas cibernéticas del delito. Rivera de la Cruz (2025), sostiene que esta cooperación es indispensable en la actualidad, especialmente si se estructura con garantías jurídicas claras que equilibren la eficacia penal con la protección de los derechos fundamentales. En efecto, este criterio es importa porque refuerza la trazabilidad digital y mejora la capacidad de respuesta del sistema penal frente a ciberataques. No obstante, también es cierto que puede generar tensiones con el derecho a la privacidad y la confidencialidad de las comunicaciones, por lo que su implementación debe estar sujeta a autorizaciones judiciales rigurosas y a límites proporcionales.

3. **Fortalecimiento de fiscalías existentes y creación de juzgados especializados en delitos informáticos**

En paralelo, se identifica como criterio clave la creación de juzgados y el fortalecimiento de fiscalías especializadas en delitos informáticos. Esta medida busca responder a la creciente complejidad técnica que caracteriza a este tipo de criminalidad, la cual exige conocimientos específicos en redes, sistemas, algoritmos, blockchain, análisis de metadatos, y otras

herramientas digitales. La especialización permitiría que jueces y fiscales interpreten adecuadamente las pruebas electrónicas, valoren informes periciales tecnológicos y resuelvan casos con una visión técnica y jurídica coherente. Carbajal Camones (2022), en su estudio sobre el fortalecimiento de fiscalías especializadas, concluye que estas unidades constituyen un mecanismo eficaz para contrarrestar los factores que actualmente dificultan el juzgamiento del fraude informático, tales como la dispersión de competencias o la falta de peritos adecuados. La especialización judicial, por tanto, no solo acelera los procesos, sino que también eleva la calidad del razonamiento jurídico en materia de cibercrimen. A pesar de sus ventajas, esta propuesta enfrenta limitaciones prácticas como la escasez de presupuesto, la falta de personal capacitado y la necesidad de actualizar constantemente los conocimientos técnicos de los operadores.

4. La cooperación internacional

Finalmente, un aspecto que no puede soslayarse es la armonización normativa con los estándares internacionales. La reciente adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia en diciembre de 2024 representa un hito en esta materia, constituyendo un avance en la armonización normativa internacional, al establecer principios para el intercambio de evidencia digital, asistencia legal mutua y definiciones delictivas (Naciones Unidas, 2024). Sin embargo, uno de los principales problemas en la política criminal peruana frente a la cibercriminalidad pura es la fragmentación normativa y la insuficiente articulación internacional, por lo que la adopción de marcos globales resulta estratégica. Si bien esta armonización es deseable, también implica desafíos de implementación, como la adecuación de normas procesales, la capacitación de operadores en estándares internacionales y la reforma legislativa en aspectos claves como la jurisdicción digital. (Llano Carrera, 2022)

En resumen, la propuesta de estos criterios técnicos y legales necesarios para fortalecer la infraestructura normativa y legal sobre la protección de datos personales en el Perú evidencia la necesidad de implementar la Ley N.º 30096 para adecuarla a los delitos cibernéticos emergentes, adoptar un enfoque penal adaptativo, consolidar la cooperación con los ISP bajo controles judiciales, especializar los órganos jurisdiccionales y armonizar el ordenamiento jurídico nacional con tratados internacionales como la Convención de la ONU. Estas medidas, si bien enfrentan obstáculos técnicos y operativos, son indispensables para enfrentar con eficacia el fenómeno delictivo digital y garantizar una tutela efectiva del bien jurídico de los datos personales.

Conclusiones

- Si bien el Perú cuenta con una normativa básica sobre protección de datos personales en caso de delitos informáticos, esta presenta serias limitaciones en cuanto a la implementación de criterios técnicos como la seguridad, la portabilidad y el derecho al olvido. La ausencia de capacidades institucionales, sumada a la escasa formación de los operadores jurídicos, limita su aplicación efectiva, lo que impide anticipar o responder adecuadamente ante delitos informáticos.
- En comparación con la Ley N.º 21.459 de Chile y la Ley N.º 1273 de Colombia, la Ley peruana N.º 30096 evidencia una clara desactualización frente a las exigencias del contexto digital actual, donde las legislaciones extranjeras no solo han incorporado figuras delictivas modernas como el sabotaje informático y el phishing, sino que han establecido mecanismos de cooperación internacional y agravantes diferenciadas.
- Finalmente, se determinó que la infraestructura jurídica peruana carece de una articulación adecuada entre tecnología, operadores especializados y normas procesales eficaces. El país aún no ha consolidado unidades policiales ni juzgados especializados en ciberdelincuencia, ni cuenta con protocolos homologados para el tratamiento de evidencia digital, lo que dificultan una respuesta penal efectiva.

Recomendaciones

- Se recomienda que la Autoridad Nacional de Protección de Datos Personales, en coordinación con el Ministerio Público y el Poder Judicial, elabore y difunda protocolos técnicos operativos que integren estándares mínimos de seguridad, directrices sobre portabilidad y lineamientos para la aplicación efectiva de estos criterios en investigaciones por delitos informáticos.
- Se recomienda que el Ministerio de Justicia y Derechos Humanos promueva la modificación de dicha ley mediante una nueva propuesta legislativa que contemple tipos penales autónomos para delitos informáticos emergentes, además de establecer mecanismos de cooperación penal internacional efectivos, en línea con las disposiciones del Convenio de Budapest.
- El Ministerio del Interior, junto con el Ministerio Público y el Poder Judicial, debe implementar unidades de investigación digital, fiscalías y juzgados especializados en ciberdelitos. Además, se deben establecer programas de formación continua en cibercriminalidad y tecnologías emergentes para operadores de justicia.

Referencias

Acurio Del Pino, S. (2016). *Delitos Informáticos: Generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Agustina Sanllehí, J. (2022). La inmersión del derecho penal en la era de la "postmodernidad tecnológica": Retos en la adaptación del sistema jurídico-penal ante un cambio de paradigma. En J. Pérez Collados, J. A. Pérez Juan, & F. J. Sanjuán Andrés, *La cultura jurídica en la era digital* (págs. 219-246). Editorial Aranzadi.

Alcantara Diaz, F. E. (2024). Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022. *[Tesis para optar el titulo profesional de abogado]*. Universidad Señor de Sipan, Pimentel. https://hdl.handle.net/20.500.12802/12384

Arapa Ticona, J. C., Cari Calcina, K. M., Laura Lipe, J. J., Laura Valero, M., Merma Cabrera, R. M., Tarapa García, H. L., & Condori Parí, N. (2024). Causas y consecuencias del incremento de los delitos informáticos en la ciudad de Puno 2023. *Revista de Derecho de la Universidad Nacional del Altiplano de Puno, 9*(1). https://doi.org/https://doi.org/10.47712/rd.2024.v9i1.262

Arellano Cruz, J. L., & Mendivil Cortez, C. V. (2020). Teoría del delito y teoría del caso. *Revista de Investigación Académica sin Frontera*(33), 1-43. https://doi.org/https://doi.org/10.46589/rdiasf.vi33.308

Arispe Alburqueque, C. M., Yangali Vicente, J. S., Guerrero Bejarano, M. A., Lozada de Bonilla, O. R., Acuña Gamboa, L. A., & Arellano Sacramento, C. (2020). *La investigación cientifica: una aproximación para los estudios de posgrado.* Guayaquil: Universidad Internacional del Ecuador. https://repositorio.uide.edu.ec/handle/37000/4310

Barrio Andrés, M. (2024). Los principios estructurales del Reglamento General de Protección de Datos. *Actualidad Jurídica Iberoamericana*(20), 1322-1341. https://hdl.handle.net/10550/100390

Bascur, G., & Peña, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte. *Revista De Estudios De La Justicia*(37). https://doi.org/ttps://doi.org/10.5354/0718-4735.2022.67885

Beltrán Aguirre, J. L. (2018). Reglamento general de protección de datos: Novedades. Adaptación de la normativa española: El proyecto de LOPD. *Derecho y Salud, 28*, 74-96.

Bolaños Vainstein, G. G. (2022). La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano. *[Tesis para optar el Título Profesional de Abogado]*. Universidad de Lima, Lima, Perú.

Carbajal Camones, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen [Tesis para optar el grado académino de maestra en Derecho en Ciencias Penales]*. Universidad de San Martin de Porres, Lima. https://hdl.handle.net/20.500.12727/11398

Carrero Perez, J. S. (2024). Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos. *Incorporación de la modalidad del Phishing en la Ley de Delitos Informáticos [Tesis de licenciatura, Universidad Católica Santo Toribio de Mogrovejo]*. Universidad Católica Santo Toribio de Mogrovejo, Chiclayo. http://hdl.handle.net/20.500.12423/7300

Carrillo Díaz, C. F., & Montenegro Dávila, A. N. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos [Tesis para optar el titulo profesional de abogado]*. Universidad Señor de Sipán, Pimentel.

Ccama Centeno, M. E. (2021). *El delito contra datos informáticos personales en el derecho fundamental a la intimidad personal en la Corte Superior De Justicia de Puno 2020 [Tesis para optar el titulo profesional de Abogado]*. Universidad Privada San Carlos, Puno, Perú. http://repositorio.upsc.edu.pe/handle/UPSC/116

Córdova Abregú, A. F. (2023). *Tratamiento de datos personales en marco a la atención de las solicitudes de acceso a la información pública [Tesis para obtener el grado académico de Maestra en Derecho Administrativo]*. Pontificia Universidad Catolica del Perú, Lima.

Cornejo Contreras, A. (2023). La investigación de delitos informáticos y su prueba en materia penal. *[Memorias para optar el grado de licenciado en ciencias juridicas y sociales]*. Universidad de Chile, Santiago de Chile.

Cornejo Contreras, A. (2023). *La investigación de los delitos informáticos y su prueba en materia penal.* Universidad de Chile, Santiago de Chile.

Coronel Carvajal, C. (2023). Los objetivos de la investigación. *Revista Archivo Médico de Camagüey*. http://scielo.sld.cu/pdf/amc/v27/1025-0255-amc-27-e9591.pdf

Cuellar Quintero, V., & Astaiza Morales, P. A. (2023). Análisis dogmático de los delitos informáticos o ciberdelitos en Colombia. *[Proyecto de grado presentado para optar al*

título de Abogado]. Universidad libre seccional Cali, Santiago de Cali. https://hdl.handle.net/10901/29295

Enríquez Álvarez, L. (2019). La Visión de América Latina sobre el Reglamento General de Protección de Datos. *Comentario Internacional: Revista del Centro Andino de Estudios Internacionales*(19), 99-112. https://revistas.uasb.edu.ec/index.php/comentario/article/view/1546/1316

Estrada Salvador Ramirez, C. T. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. *Ius Vocatio, 3*(9), 91-115. https://doi.org/https://doi.org/10.35292/iusVocatio.v7i9.928

Franco García, D., & Quintanilla Perea, A. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*(84), 271-299. https://doi.org/https://doi.org/10.18800/derechopucp.202001.009

García Granizo, J. J. (2022). *La política criminal implementada por el Estado Peruano y la persecución de los delitos de robo en la ciudad de Huancayo, 2019 – 2020 [Tesis para optar el grado académico de Maestro en Derecho y Ciencias Politica].* Universidad Peruana los Andes, Huancayo.

Gómez Martínez, M. (2014). Ciber-criminalidad: Nuevos Retos para la Seguridad Pública. *[Tesis para optener el titulo de licenciado en Derecho].* Universidad de Sonora, Hermosillo, Sonora. http://hdl.handle.net/20.500.12984/1275

Guarnizo Portela, M. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia.* Universidad Nacional, Abierta y a Distancia, Ibagué. https://repository.unad.edu.co/handle/10596/41392

Huamán Cruz, M. Y. (2020). Los delitos informáticos en Perú y la suscripción del Convenio de Budapest. *[Tesis para optar el título profesional de abogado].* Universidad Andina del Cusco, Cuzco. https://hdl.handle.net/20.500.12557/4116

Jiménez Rozas, J. (2022). Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y nuevas problemáticas. *Curso de adaptación al grado en criminologia.* Universidad de Salamanca, Salamanca. http://hdl.handle.net/10366/150144

Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris Et Investigatio*(1), 29-47. https://doi.org/https://doi.org/10.15381/lucerna.v0i1.18373

Llano Carrera, L. R. (2022). Análisis de la política criminal peruana frente a la cibercriminalidad pura. *[Tesis para obtener el título de Abogado que presenta el bachiller].* Pontificia Univesidad Católica del Perú, Lima, Perú.

Luna Cervantes, E. J. (2021). Preguntas y respuestas varias sobre la protección de datos personales en el Perú. *Advocatus*(039), 253-264. https://doi.org/https://doi.org/10.26439/advocatus2021.n39.5133

Maranto Rivera, M., & González Fernández, M. (2015). *Fuentes de información*. Universidad Autónoma del Estado de Hidalgo: https://repository.uaeh.edu.mx/bitstream/123456789/16700

Medina Romero, M., Rojas León, R., Bustamante Hoces, W., Loaiza Carrasco, R., Martel Carranza, C., & Castillo Acobo, R. (2023). Metodología de la investigación: Técnicas e instrumentos de investigación. *Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú*. https://doi.org/https://doi.org/10.35622/inudi.b.080

Mejía Lobo, M., Hurtado Gil, S., & Grisales Aguirre, A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista De Ciencias Sociales, 29*(2), 356-372. https://doi.org/https://doi.org/10.31876/rcs.v29i2.39981

Millán López, E. (2023). *Delitos informáticos: situación actual, acceso ilícito y responsabilidad penal de las personas jurídicas.* Universidad de Valladolid, Valladolid. https://uvadoc.uva.es/handle/10324/66985

Miranda Beltrán, S., & Ortiz Bernal, J. A. (2020). Los paradigmas de la investigación: un acercamiento teórico para reflexionar desde el campo de la investigación educativa. *11*(21). https://doi.org/https://doi.org/10.23913/ride.v11i21.717

Montano, P. (2024). Responsabilidad penal e informática. *Revista de Derecho Penal*(13). https://revistas.fcu.edu.uy/index.php/penal/article/view/3725

Mubarak Aguad, L. (2020). El Internet, el Big Data y el tratamiento de los datos personales. *Advocatus*(036), 205-223. https://doi.org/10.26439/advocatus2018.n036.4753

Naciones Unidas. (2024). *Convención de las Naciones Unidas contra la Ciberdelincuencia; Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión.* Asamblea general. https://documents.un.org/doc/undoc/gen/n24/426/77/pdf/n2442677.pdf

Narvaez Montenegro, D. B. (2015). El delito informático y su clasificación. *Revista Uniandes Episteme*, 158-173. https://dialnet.unirioja.es/servlet/articulo?codigo=6756355

Nicomedes Teodoro, E. N. (2018). Tipos de investigación. *Repositorio: Universidad Santo Domingo de Guzmán*. https://core.ac.uk/outputs/250080756/

Novoa Toledo, I., & Venegas Cruz, L. (2020). Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. *[Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales]*. Universidad de Chile, Santiago de Chile. https://repositorio.uchile.cl/handle/2250/176344

Ocupa Sánchez, B. S. (2023). Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022. *[Tesis para obtener el grado de maestro en derecho penal y procesal penal]*. Universidad Cesar Vallejo, Tarapoto. https://hdl.handle.net/20.500.12692/119930

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: Revista de investigación de la Facultad de Derecho, 9*(1). https://doi.org/https://doi.org/10.35383/ius-usat.v9i1.338

Palacios Cuba , E. F. (2021). *Los Delitos Informáticos contra Datos, y su vulneración al Derecho de la Intimidad Personal, en la Ciudad de Ayacucho [tesis para optar el titulo profesional de abogado]*. Universidad Cesar Vallejo, Lima. https://hdl.handle.net/20.500.12692/74705

Peña Peña, M. E. (2023). Delitos Cibernéticos. *[Trabajo de investigación para optar al título de Magister en Derecho Penal]*. Universidad Libre de Colombia, Bogotá D.C. https://hdl.handle.net/10901/24774

Pérez Arias, J. (2021). Cibercriminalidad: hacia la nueva realidad -virtual- del derecho penal. *Revista internacional de doctrina y jurisprudencia, 26*, 175-193.

Polo Roca, A. (2021). Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. *Estudios de Deusto, 69*(1), 211-240. https://doi.org/https://doi.org/10.18543/ed-69(1)-2021pp211-240

Rivera Prado, M. (2022). En búsqueda del equilibrio entre la protección de datos personales, el deber de transparencia y el derecho de acceso a la información pública. *[Trabajo de investigación para optar el Grado Académico de Maestro en Derecho Empresarial]*. Repositorio Institucional de la Universidad de Lima, Lima. https://hdl.handle.net/20.500.12724/19020

Salazar-Escorcia, L. S. (2020). Investigación Cualitativa: Una respuesta a las Investigaciones Sociales Educativas. *Cienciamatria: Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, VI*(11), 101-110. https://doi.org/https://doi.org/10.35381/cm.v6i11.327

Sanchez Castillo, Z. N. (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia.* Universidad nacional abierta y a distancia, Chiquinquirá.

Sánchez Sánchez, I. (2015). *Cronograma de actividades*. Universidad Autónoma del Estado de Hidalgo: https://repository.uaeh.edu.mx/bitstream/123456789/16696

Sánchez Villa, K. K. (2019). La tipificación del delito de acceso ilícito a sistemas y equipos de informatica en Mexico. *[Tesis para obtener el grado de maestro en ciencias del derecho].* Universidad Autónoma de Sinaloa, Culiacán.

Siche Jara, R. (2020). *Proyecto de investigación*. Retrieved 7 de Junio de 2024, from Universidad Nacional José Faustino Sánchez Carrión: https://www.unjfsc.edu.pe/investigacion/wp-content/uploads/2020/01/Proyecto-de-Investigacion.pdf

Temperi, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. En R. Parada, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet* (págs. 49-69). Erreius.

Trujillo Vega, E. G. (2024). Desafios y estrategias de seguridad digital para combatir la cibercriminalidad en el Perú. *Dialógica Revista Multidisciplinaria, 21*(2), 130-147. https://doi.org/https://doi.org/10.56219/dialgica.v21i2.3327

Urdanegui Rangel, A. (2023). *Los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en lima metropolitana [Tesis para obtener el titulo de abogada].* Universidad Autónoma del Perú, Lima.

Valencia Álvarez, A. (Abril de 2020). Impacto de los delitos informáticos en la sociedad actual. *Publicación semestral*(2), 1-14.

Vásquez Rodríguez, R. (2022). La Responsabilidad Proactiva en la Normativa Peruana de Protección de Datos Personales. *YachaQ: Revista De Derecho*(13), 25-37. https://doi.org/https://doi.org/10.51343/yq.vi13.913

Ventura Quijano, M. A. (2021). La Tipificación del Phishing, Smishing y Vishing en nuestro Sistema Penal Peruano, para la lucha contra la Ciberdelincuencia en Lima, 2020. *La Tipificación del Phishing, Smishing y Vishing en nuestro Sistema Penal Peruano, para la lucha contra la Ciberdelincuencia en Lima, 2020 [Tesis para optar el titulo profesional de abaoga].* Universidad Privada del Norte, Lima, Perú. https://hdl.handle.net/11537/28942

Villavicencio Terreros, F. (2014). Delitos informaticos: cybercrimes. *Revista ius et veritas*(49), 284-304.

Villavicencio Terreros, F. (2019). *Derecho penal básico.* Lima: Pontificia Universidad Católica del Perú, Fondo Editorial.

Zamudio Salinas, M. (2021). El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del Sistema De Geolocalización GPS. Límites y propuestas. *[Tesis para optar el grado academico de magister en Derecho].* Pontificia Universidad Catolica del Perú, Lima, Perú. http://hdl.handle.net/20.500.12404/20150

Anexos

Anexo 01: Matriz de consistencia

<table>
<tr><td colspan="2">Línea de investigación: Ordenamiento jurídico nacional</td></tr>
<tr><td colspan="2">Título del proyecto de investigación: Normativa Penal en la Protección de Datos: criterios para prevenir delitos informáticos en el Perú</td></tr>
<tr><td colspan="2">Problema de investigación: ¿Qué criterios deberán considerarse en la regulación de la protección de datos personales para la prevención de delitos informáticos en el Perú?</td></tr>
<tr><td colspan="2">Realidad problemática: Radica en una protección débil de los datos personales, que se traduce en una exposición constante a riesgos de ciberataques. Simultáneamente, la dificultad en la identificación de los infractores complica la imposición de sanciones, creando un ambiente de impunidad y debilitando la eficacia de las leyes penales. Esto evidencia una necesidad urgente de revisar y fortalecer la normativa penal en relación con la protección de datos personales</td></tr>
<tr><td>Tesista: Renzo Chicoma Calderón</td><td>Asesor(a): Cinthyacrisa Gastulo</td></tr>
<tr><td>Variables (categorías conceptuales)</td><td>Objetivos</td></tr>
<tr><td rowspan="4">1. Delitos informáticos
2. Derecho de protección de datos personales
3. Criminalidad informática
4. Dato personal</td><td>General</td></tr>
<tr><td>Analizar y establecer los criterios esenciales para la regulación de la protección de datos personales en el Perú, con el fin de prevenir y mitigar la incidencia de delitos informáticos, garantizando la seguridad y privacidad de la información de los ciudadanos.</td></tr>
<tr><td>Específicos</td></tr>
<tr><td>1. Identificar y analizar los criterios técnicos y legales necesarios para fortalecer la infraestructura normativa y legal sobre la protección de datos personales en el Perú, con el fin de prevenir y mitigar delitos informáticos.
2. Comparar la legislación chilena tomando en cuenta la ley 21459. Así como la ley 1273 colombiana sobre delitos informáticos con la normativa peruana, ley 29733 de datos personales y la ley 30096 de delitos informáticos.</td></tr>
</table>

Aporte: al derecho penal peruano al identificar brechas en la protección de datos personales frente a delitos informáticos, proponiendo criterios legales y técnicos para fortalecer la normativa vigente. También contribuirá a la tipificación más precisa de estos delitos y promoverá el uso de tecnologías avanzadas para mejorar el rastreo y sanción de ciberdelincuentes. Además, fomentará la concientización pública sobre ciberseguridad, ayudando a prevenir delitos y proteger los derechos en el entorno digital.

Anexo 02: Aprobación de asesor