Lucerna Iuris Et Investigatio
n.º 7 - 2024, pp. 89 - 118
https://doi.org/10.15381/lucerna.n7.28141

ISSN: 3028-9726 (En línea)
2788-6689 (Impreso)
Facultad de Derecho y Ciencia Política UNMSM

INVESTIGACIONES NACIONALES

Tipificación de los delitos informáticos en la legislación peruana

Classification of Cybercrimes in Peruvian Legislation

Miguel Andrés Osmar Tapia Cornejo

Universidad Nacional Mayor de San Marcos, Lima, Perú

https://orcid.org/0009-0005-9200-4053

miguel.tapia5@unmsm.edu.pe

Presentado: 23/05/2024 - Aceptado: 02/12/2024 - Publicación: 31/12/2024

Resumen

El objetivo general del artículo fue determinar si la Ley 30096 ofrece una tipificación que abarca los delitos cibernéticos actuales. Desde el plano metodológico, se tomó en consideración la investigación básica, enmarcada en un modelo cualitativo, mediante el empleo del método inductivo cuyas técnicas de recolección de datos se basó en la recopilación de fuentes relacionadas al tema, así como la documentación de archivos y fuentes gubernamentales. El universo de estudio, fueron todas las informaciones legales obtenidas según los objetivos específicos del estudio. En conclusión, se evidenció que los delitos informativos en Latinoamérica y Perú tomaron auge a partir de la pandemia y continúan hoy por hoy ampliando su forma de trabajo, entre la suplantación de identidad, falsificación informática, fraude electrónico, ataques a la intimidad, estafas virtuales, entre otros, que afectan al ciudadano y las instituciones gubernamentales. Es por ello, que se hace necesario una revisión más profunda a las leyes, así como la implementación de medidas más radicales que no dejen impune este tipo de delitos, haciendo uso de acciones de investigación, seguimiento y captura más eficaces.

Palabras clave: delitos cibernéticos actuales, identidad, libertad sexual, plataformas informáticas, secretos comunicacionales.

Abstract
General Objective of the Article: Assessing the Adequacy of Law 30096 in Classifying Contemporary Cybercrimes.From a methodological perspective, the study employed basic research framed within a qualitative model, utilizing the inductive method for data analysis. Data collection techniques involved compiling relevant sources and documenting archives and governmental materials. The study's population encompassed all legal information gathered in accordance with the specific research objectives. In conclusion, it was evident that information-related offenses in Latin America and Peru surged during the pandemic and persistently evolve in modus operandi, encompassing identity theft, computer forgery, electronic fraud, privacy infringements, virtual scams, among others, affecting both citizens and governmental institutions. Therefore, there arises a necessity for a more thorough legislative review and the implementation of more stringent measures to combat such crimes effectively, incorporating enhanced investigative, monitoring, and apprehension actions.

Keywords: current cyber-crimes, identity, sexual freedom, computer platforms, communication secrets.

I. Introducción

Los nuevos paradigmas del crimen surgen como resultado de metamorfosis acontecidas en tiempos recientes, las cuales han instigado transformaciones equiparables a las generadas en la época del siglo XIX de la Revolución Industrial. La transformación tecnológica en los últimos años durante el siglo XX ha engendrado condiciones propicias para el florecimiento de los sistemas informáticos, los cuales no solo son empleados en el ámbito doméstico o laboral, sino que abarcan la totalidad de las actividades y disciplinas humanas (Martínez, et al., 2020) Aunado a ello, el surgimiento de internet propició la accesibilidad a los distintos sistemas informáticos denominados por Bill Gates como autopista de la información (El Comercio, 2023).

El uso de computadora o sistema de información tiene una básica incidencia en los avances sociales de cada nación y una directa asociación con el progreso económico y cultural, pero como contrapartida negativa, han surgido infracciones y violaciones de derechos a la propiedad o al uso de medios informáticos que han creado nuevos bienes jurídicos a proteger y generado la criminalidad por computadoras o delito informático, el cual es necesario definir y tipificar adecuada y sistemáticamente, en los principios penales rectores, como el principio de legalidad, entre otros. (Universidad Nacional de la Rioja, 2022).

En todo el mundo, los avances tecnológicos generaron el surgimiento del aprendizaje automático la robótica y la inteligencia artificial a un ritmo vertiginoso, dejando en duda muchas probabilidades ante el modelo habitual, ya que, todos estos lineamientos avanzados facilitaron la cotidianidad de las

personas y mejoraron sus vínculos profesionales y personales (Martínez et al, 2020), aunque se puede observar que estos avances han ocasionado un conjunto de dificultades que puede principalmente afectar a la sociedad en cuanto a su privacidad, causando diversos crímenes informáticos que han afectado la seguridad de las personas (Acosta et al., 2020), más aún, cuando este tipo de delito no ha sido clasificado ni actualizado en la norma (Nazario y Villanueva, 2022)

En el contexto mundial, esta forma de delitos informáticos se regula a través del derecho penal de los países que forman parte de la Unión Europea. En España, Díaz y Rangel (2020) refiere que la cooperación internacional es ahora más fuerte para poder combatir la ciberdelincuencia de manera efectiva. Con el cumplimiento del Convenio de Budapest, España tiene similares objetivos que otros países en la lucha contra el crimen cibernético comprometiéndose en la cooperación con otras naciones para la prevención y persecución de criminales informáticos. Particularmente aplicando lineamientos de seguridad en donde la población española navegue por la red de manera segura, según lo establecido el lineamiento de protección de la privacidad de las personas evitando así la accesibilidad no autorizada a modelos informáticos.

En América Latina, los países que han regulado este delito dentro de sus marcos legales son Colombia, Chile y Brasil. En Perú, también se presentan estos problemas sociales y económicos Le afectan a las personas que tienen que utilizar herramientas tecnológicas como las comerciales en la intervención de transacciones comerciales y aunque una Ley Nº 30096 denominada: Ley de Delitos Informáticos del 5 de diciembre de 2013 y modificada por la Ley N° 30171 del 10 de marzo de 2014, existen una serie de vacíos legales en la falta de una clasificación clara de los tipos de delitos informáticos, lo que incide en el nivel de vulnerabilidad de seguridad que puede traer su alcance sobretodo todo, cuando cada día aumentan los ciberdelitos (Nazario y Villanueva, 2022)

Los beneficios que aporta la tecnología facilitan las actividades delictivas, provocando daños a la propiedad jurídica de particulares o privados, sin embargo, ante las primeras manifestaciones de estos nuevos delitos informáticos, es muy poco probable que los tipos clásicos de delitos incluyan este tipo de acto tecnológico, razón por la cual el derecho penal moderno debe actualizarse para incluir con precisión estos llamados ciberdelitos.

Los avances tecnológicos asociados a los sistemas informáticos han permitido el ingreso han propiciado el paso del entorno material y tangible al de tipo informático, virtual e inmaterial (Indacochea, 2022). Se refiere el autor a que el mundo virtual ha venido cambiando de una manera veloz

todos los aspectos de nuestra vida y del mismo modo, lo ha hecho a través del derecho en sus distintas modalidades, no únicamente implementando programas informáticos, legales y sistemas computarizados, sino que se ha extendido a sectores bancarios, comerciales, financieros e industriales, lugares en donde los delitos han ido surgiendo por lo que requieren de una legislación adecuada que proteja al sujeto pasivo.

Por esta razón, en la actualidad se requiere de un contexto legal que protejan únicamente las vidas, sino que la calidad de la profesión existe una extendida violencia digital en el contexto laboral, no obstante, los elementos adoptados por las organizaciones no han tenido modificación alguna (Laboy et al., 2021). Sobre esta problemática Chipana y Rivera (2023) mencionan que las brechas de seguridad en las redes, son mayor hoy en día, lo que hace reflexionar si realmente existen leyes sobre el tema y si existen autoridades preparadas para enfrentarlos, ya que son derechos humanos básicos y, por tanto, esenciales para un adecuado desarrollo y bienestar. Es por ello, que se requiere la delimitación de las actividades de acción entre ambos tipos de derecho, por los importantes avances científicos, comunicativos y tecnológicos en donde se da una divulgación fácil de los hechos vinculados a la privacidad de los individuos, de manera que determinar un control sobre este permiso no es una acción sencilla en la jurisprudencia y doctrina, de manera que se pretende la combinación de derechos y deberes de difusión informática sin que las personas sean ofendidas.

Tomando en cuenta el contexto actual a nivel social y los avances tecnológicos en el país, se requiere un enfoque mucho más realista sobre los avances logrados. Es necesario superar la errada idea de que las tecnologías resuelven las diferentes dificultades. Debemos afrontar que, aunque las TIC son trascendentales para el progreso de un país, también han promovido y ampliado problemáticas tanto nuevas como antiguas, como el aumento de los crímenes informáticos. Estos representan uno de los grandes desafíos de la actualidad, ya que vulneran la seguridad de entidades públicas y privadas, así como de los usuarios, desafiando el rol de los sistemas judiciales nacionales (Guerrero, 2020).

La falta de llegar a un consenso común de lo que significa hablar de un ciberdelito, es la de no haber llegado a entender que no hay delito ni grande ni pequeño para diferenciar un delito de esta índole y se deben englobar todos los delitos cometidos con el uso de tecnologías de información y especialmente, aquellos donde se involucren sistemas informáticos. Este problema queda ejemplarizado con lo sucedido por el llamado ciberterrorismo, el cual no está limitado únicamente a las guerras o a colocar bombas explosivas, sino que además emplea la herramienta informática de Stuxnet y Flame que ocasionan la catástrofe que dejó inoperativa a la planta nuclear energética en Irán (Espinoza, 2022).

Desde un punto de vista doctrinal, podemos ver que el fenómeno de la delincuencia que utiliza nuevas tecnologías o sistemas informáticos aún no se ha comprendido plenamente, esto debido a que así como en la sociedad actual existe un nuevo modelo de vínculos comerciales donde todo se lleva de manera informática, también existe una nueva manera de delincuencia en la que el Perú no se encuentra adecuado para dar respuesta pronta y eficiente, pues no es se da la técnica de capacitación de los fiscales del Ministerio Público, o porque aún se cuenta con una base jurídica ambigua que deja a la sociedad en una posición desprotegida e indefensa (Huayca, 2022).

Como en el caso de la inmensa cantidad de denuncias sobre estafas y mensajerías fraudulentas, robos de datos personales, por parte de empresas creadas en internet y que, al ser denunciadas, no pueden ser procesadas porque los dueños del lugar no se encuentran en el país, o como el caso del phishing, en la cual ocurre el envío de mensajes a través del correo electrónico los cuales son redactados ingeniosamente para solicitar datos delicados e importantes que luego es usada para vulnerar la protección de datos personales y cometer alguna estafa (Aredo, 2021). Igualmente, los delitos producidos en la banca peruana y en donde muchas veces, el dueño de una cuenta no puede demostrar no haber sido quien retiro el dinero o como en el caso mencionado de los bonos sustraídos del banco durante la pandemia De acuerdo a esto, en el 2023, INDECOPI recibió 4.406 reclamos y 2.054 denuncias contra las empresas del sistema financiero como BCP, Interbank, BBVA, Falabella y Scotiabank por operaciones no reconocidas y en donde casi la mitad de las denuncias fueron a favor del usuario, pero la otra mitad, no pudo demostrar haber realizado esa operación y fue víctima de la delincuencia cibernética (Alarcón, 2023).

Por todo lo expuesto anteriormente, en la legislación peruana se debe hacer una revisión de los delitos que no están tipificados en la Ley 30096 y que debido a sus características transnacionales se deben aplicar bajo las normas internacionales con asistencia mutua entre los Estados involucrados.

II. Delitos informáticos

Existe una variedad de formas para referirse a esta conducta como: ciberdelitos, delitos cibernéticos, delitos electrónicos, delitos telemáticos, delitos computacionales, entre otros, pero en todos los casos, es definido como cualquier tipo de conducta criminógena en donde un ordenador se involucra como símbolo, material u objeto (Flores, 2020)

La Organización para la Cooperación del Desarrollo Económico (OCDE) esta referido a que los crímenes vinculados a sistema computacionales se consideran como aquellos procesos no éticos, ilícitos y sin autorización en donde abarca la automatización, procesamiento y transmisión de información (Carriedo, 2022).

2.1. Normativa aplicable a los delitos informáticos

De acuerdo a Tavora (2022), el Convenio de Budapest es el primer tratado internacional que abordó los delitos informáticos debido a que los Estados reconocían la insuficiente colaboración internacional y las diferencias entre los ordenamientos jurídicos que dificultaban la investigación y enjuiciamiento de los delitos informáticos (Flores, 2023)

El Estado peruano se adhiere al convenio de Budapest en el 2014 y se elabora la Ley Nº 30096 Ley de delitos informáticos del 21 de octubre del 2013 y modificada por la Ley Nº 30171 del 17 de febrero de 2014, por lo que esta ley se constituye en la principal norma contra la cibercriminalidad (Ocupa, 2023).

Cabe mencionar que esta norma ha sufrido muchas críticas por parte de los que argumentan que esta ley no cumple con sancionar adecuadamente los delitos informáticos y que fue hecha para salir del paso y cumplir con las obligaciones impuestas para ser parte del Convenio de Budapest, razón por la cual la legislación ha presentado el Proyecto de Ley Nº 5630/2020-CR "Ley de Seguridad Informática y Represión de los Delitos Informáticos", para crear un nuevo marco normativo especializado que incluye los delitos no considerados como informáticos como el acceso ilícito o intrusismo informático, la perturbación informática, la interceptación de datos informáticos, suplantación de identidad informática,, la pornografía infantil, el abuso de mecanismos y dispositivos informáticos, la protección al consumidor en el ámbito de comercio electrónico, entre otros. y la cual a la fecha sigue en revisión (Elías, 2022).

2.2. Delitos cometidos en plataformas virtuales que no son delitos informáticos bajo la Ley Nº 30096

Dentro del Derecho Público, se ubican en la rama del derecho Penal, otros delitos que, aunque son cometidos en plataformas virtuales no se consideran delitos informáticos. El propósito es la de protección de aquellos bienes titulados jurídicamente de importancia coartando de manera eventual la libertad del que atente en su contra estipulado en diferente lineamiento jurídicos.

Flores (2023) menciona los supuestos delitos cometidos en plataformas virtuales que no son considerados delitos informáticos por la Ley Nº 30096 y sus modificaciones

- El asedio de una persona por medio de una plataforma virtual y que afecta su entorno familiar, laboral y sentimental, pudiendo sentirse amenazada o acosada para realizar actos de connotación sexual, no es considerado dentro del alcance de la Ley Nº 30096 sino que esta conducta se subordina a los artículos 151-A y 176-C del Código Penal.

- El delito por estafas en compra-ventas realizadas en plataformas en línea para engañar y apoderarse del dinero de una persona, no se considera delito informático porque no implica la vulneración de sistemas informáticos y se subordina al artículo 196 del Código Penal.

- Delito de difamación por medios digitales no se considera delito informático porque no implica la vulneración de sistemas informáticos y se subordina al artículo 132 del Código penal.

- Las amenazas de muerte o algún otro tipo de daño, por mensajes enviados en plataforma virtual para lograr que una persona haga algo, se estaría cometiendo un delito de coacción, pero la conducta no se relaciona directamente con el uso de la tecnología.

Flores (2023) hace la aclaración de que, aunque las conductas citadas anteriormente no se encuentren tipificadas como delitos informáticos, no quiere decir que no son sancionadas por la ley, pero hace hincapié en que las personas deben tomar conciencia que sus conductas en línea si tienen consecuencias legales y que el respeto a las personas es igual de importante en el mundo virtual.

Al respecto, Velarde (2023) refiere que existen otras normas que regulan los casos de mal uso de la tecnología y sus dispositivos como herramientas para realizar tareas y determinar responsabilidades. Por ejemplo, la Ley 29904, del año 2012, Ley de promoción de la banda ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, indica dentro del Art. 6 que aquellos encargados de proveer el servicio de internet no tienen la autorización arbitraria de discriminar, bloquear, restringir o interferir en el derecho de los usuarios a la utilización de protocolos o aplicaciones indistintamente de su propiedad, origen, naturaleza y destino. Igualmente, OSIPTEL aprobó el Reglamento de Neutralidad de Red Nº 165-2016-CD/ OSIPTEL, modificado el 2023 por la Resolución de Consejo Directivo N.° 003-2023-CD/ OSIPTEL, en donde se determina que las organizaciones proveedoras del servicio de internet pueden implementar la protección frente a actividades malintensionadas interrumpiendo el servicio cuando sea necesario, además de brindar datos IP bloqueando y filtrando aplicaciones o servicios si se contraviene alguna ley específica.

2.3. Ley Nº 30096: Ley de delitos informáticos

Ahora bien, la Ley Nº 30096 establece como propósito la prevención y sanción de comportamientos ilícitos que afecten o menos caben información y sistemas informáticos, aparte de otros medios jurídicos de importancia penal que se cometen al usar las tecnologías comunicativas e informática, con el propósito de dar garantía y enfrentamiento en contra

de la ciberdelincuencia y para lograrlo cuenta con cinco títulos divididos (Velarde, 2023):

a. Crímenes en contra de sistemas informativos y de datos.

b. Crímenes informáticos en contra de la libertad e indemnidad sexual.

c. Crímenes que se cometen a nivel informático en contra del secreto y la intimidad comunicacional

d. Crímenes que se cometen a nivel informático que menoscaba en el patrimonio.

e. Crímenes que se cometen a nivel informático que menoscaba la fe pública y

f. Comunes disposiciones para los delitos que abarquen abusar de dispositivos y mecanismos informáticos como el desarrollar virus o malware entre otros.

En consecuencia, la Ley Nº 30096 describe los crímenes siguientes:

- Accesibilidad ilegal a sistemas informáticos (Artículo 2)
- Violación de la integridad de datos informáticos (Artículo 3)
- Violación de la rectitud de procedimientos informáticos (Artículo 4)
- Propuestas sexuales a menores a través de medios tecnológicos (Artículo 5)
- Comercio ilegal de datos (Artículo 6)
- Interceptación de información digital (Artículo 7)
- Estafa informática (Artículo 8)
- Usurpación de identidad (Artículo 9)
- Abuso de mecanismos y sistemas informáticos (Artículo 10)

2.4. Clasificación de los delitos informáticos

Por otro lado, de acuerdo a su clasificación, Villanueva (2023) indica que las formas de crímenes informáticos tipificados son:

1. Estafas realizadas a través de la manipulación de computadoras:

    a. Manipulación de los datos de entrada: Se refiere al acto de alterar o modificar la información que se ingresa inicialmente en un sistema informático. Este tipo de manipulación busca

cambiar los resultados o procesos posteriores de manera fraudulenta o no autorizada, comprometiendo la integridad y precisión de los datos procesados.

b. Manipulación de programas: se refiere a la alteración o modificación deliberada del código o funcionalidad de un software o aplicación informática. Este tipo de manipulación puede tener como objetivo cambiar el comportamiento del programa para obtener acceso no autorizado, robar información, causar daños, o lograr resultados fraudulentos. Al manipular programas, los atacantes pueden insertar código malicioso, eliminar o desactivar funciones de seguridad, y modificar algoritmos para beneficiar sus propios intereses a expensas de la integridad y seguridad del sistema afectado.

c. Manipulación de los datos de salida: Se refiere a la alteración intencional de la información generada por un sistema informático después de que se hayan procesado los datos de entrada. Este tipo de manipulación busca cambiar los resultados finales presentados a los usuarios, lo que puede llevar a decisiones erróneas o fraudulentas. La manipulación de los datos de salida puede implicar modificar reportes, alterar cifras en documentos financieros, o falsificar resultados de análisis, afectando la confiabilidad y precisión de la información proporcionada por el sistema.

d. Manipulación informática: Se refiere a cualquier acción deliberada que altere, modifique o interfiera con el funcionamiento normal de sistemas informáticos, software, datos o redes. Este tipo de manipulación puede incluir actividades como la modificación no autorizada de programas y datos, la introducción de código malicioso, la alteración de procesos informáticos, o la interrupción del servicio.

2. Falsificaciones informáticas:

a. Como objeto: esta referida a la creación o alteración de datos, documentos digitales, o identidades electrónicas de manera fraudulenta. Esto puede incluir la falsificación de firmas digitales, certificados, registros financieros, o cualquier otro tipo de información almacenada electrónicamente.

b. Como instrumento: se utilizan como herramientas para llevar a cabo otros delitos. Aquí, el énfasis está en cómo se emplean las técnicas de falsificación para facilitar actividades ilegales. Por ejemplo, un ciberdelincuente puede usar software

malicioso para alterar registros en una base de datos con el fin de desviar fondos o modificar datos de usuarios para acceder a cuentas bancarias. En estos casos, la falsificación informática es el medio a través del cual se comete el delito, sirviendo como un instrumento para lograr un objetivo ilegal, como el robo de dinero o información sensible.

3. Alteraciones o daños a programas o datos digitales:

   a. Sabotaje informático: se refiere al acto deliberado de manipular, interrumpir o dañar sistemas informáticos, redes, programas o datos con el propósito de causar perjuicio. Este tipo de acciones pueden incluir la introducción de virus, malware o código malicioso en sistemas operativos o aplicaciones para desestabilizar su funcionamiento normal.

   b. Acceso no autorizado a servicios y sistemas informáticos implica la intrusión ilegal en sistemas protegidos sin permiso explícito de los propietarios o administradores. Este tipo de actividad se realiza generalmente con el propósito de obtener información confidencial, manipular datos o realizar acciones fraudulentas.

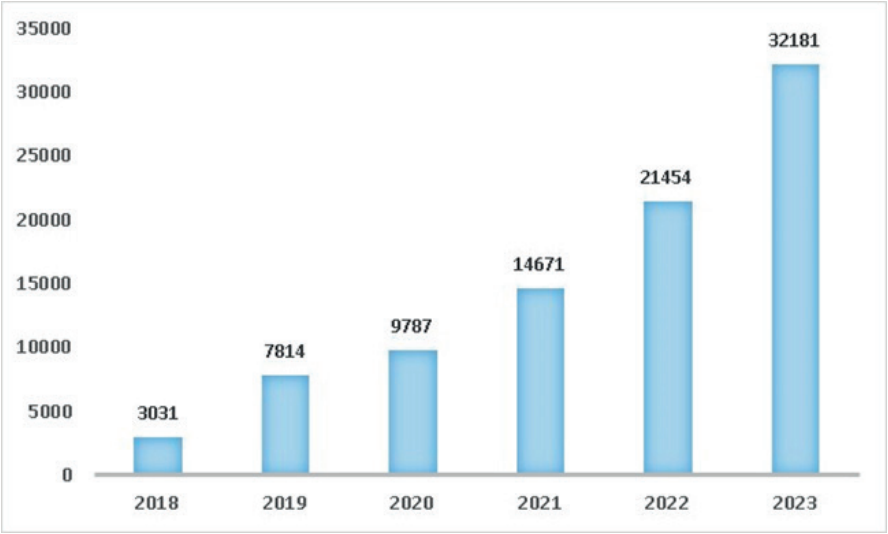
   c. Reproducción no autorizada de programas: se refiere a la copia ilegal o duplicación de software protegido por derechos de autor sin la debida licencia o permiso del titular de los derechos. Esta práctica es común en la piratería informática, donde se distribuyen copias ilegales de programas comerciales o de código abierto.

2.5. Ciberdelincuencia en el Perú del 2018 al 2024

De acuerdo con la Defensoría del Pueblo (2023)**,** la delincuencia informática constituye un problema de ámbito mundial que no solo afecta los datos personales, la propiedad y otros bienes jurídicos, sino que también puede poner en grave riesgo la integridad e incluso la vida de sus víctimas, como niños, niñas y adolescentes. No cabe duda que el avance de la tecnología en el quehacer cotidiano de las personas ha impulsado el incremento de los delitos cibernéticos durante los últimos años, y con mayor auge, durante la época más crítica de pandemia del Covid-19, debido a las restricciones planteadas por los diferentes gobiernos a nivel mundial con el fin de evitar su propagación.

En este sentido, La Policía nacional posee un registro de los últimos 5 años que evidencian un aumento proporcional de las denuncias asociadas a crímenes informáticos que se tipifican en esta ley.

Figura 1
Denuncias tipificadas en la Ley de Delitos Informáticos



Nota: Gráfico realizado con datos tomados de La Cámara (2024) ajustando el año 2023 a los datos proporcionados por Infobae (2023)

Las denuncias relacionadas con los delitos informáticos de los últimos años son: abuso de dispositivo y mecanismos informáticos, suplantación de la identidad, fraudes informáticos, atentado en contra la integridad de información digital, atentado en contra la integridad de modelos informáticos, acceso ilícito e interceptación de información informática (Defensoría del Pueblo, 2023).

III. Naturaleza jurídica del delito contra datos y sistemas informáticos

A continuación, se detallan diversos puntos que explican los delitos cibernéticos en contra los de los sistemas informáticos y datos de los individuos. En el marco legal peruano, dentro de la Ley Nº 30096 de Delitos informáticos se encuentra especificado en los crímenes contra la información y los sistemas digitales.

Se deben sacar los datos informáticos de acuerdo a los aspectos de impulsión electromagnética no cuentan con una naturaleza corporal y necesitan de procesamiento por algún tipo de sistema, por lo cual se debe conceptualizar el dato informático como toda información digital registrada y almacenadas en sistemas informáticos y dispositivos electrónicos y pueden ser: textos, imágenes, audios. videos, números o cualquiera otra información guardada y procesada en un sistema informático (Contreras, 2024).

Tabla 1
Legislación peruana del delito contra la información y sistemas informáticos

BIEN JURÍDICO	CIBERDELITO	ARTÍCULO
Contra los datos y los sistemas informáticos	Acceso ilícito	Ley de Delitos Informáticos, artículo 2
	Atentado a la integridad de los datos informáticos	Ley de Delitos Informáticos, artículo 3
	Atentado a la integridad de los sistemas informáticos	Ley de Delitos Informáticos, artículo 4
	Abuso de mecanismos y dispositivos informáticos	Ley de Delitos Informáticos, artículo 10

Fuente: Elaboración propia mediante ley Nº 30096 y Código Penal del Perú

Como se observa en la tabla 1, en la Ley Nº 30096 de Crímenes informáticos, en el segundo capítulo se encuentran los crímenes en contra de los sistemas e información digital tipificados en tres modalidades de delitos informáticos y descritos como:

> El Art. 2 se detallan los aspectos de un ilícito acceso, en donde si un individuo de forma ilegítima y con conocimiento de causa ingresa a un sistema informático o parte de él, vulnerando la seguridad que se establece para impedirlo, será motivo de delito representado por la privación de la libertad entre uno a cuatro años y entre 30 a 90 días de multa. Se establecerá igual pena si hay un acceso a un sistema informático en el que se exceda de lo que se le autorizó.
>
> En el Art. 3 en el que se tipifica la vulneración de la integridad de la información informática, se establece que aquel individuo que tenga un ilegal o deliberado daño, introducción, deterioro, alteración y supresión de información informática, haciéndola inaccesible, será amonestado con la privación de la libertad en un periodo de entre tres a seis años y entre 80 a 120 días de multas.
>
> En el Art. 4 se tipifica la vulneración de la integridad de los sistemas informáticos indicando que aquel individuo que de forma ilegítima y premeditada lo inutilice parcial o totalmente, impidiendo su acceso y la funcionalidad en el servicio que presta, será acusado con privativa de libertad en un periodo de entre tres a seis años y una multa de entre 80 a 120 días.
>
> En el Art. 10 en el que se describe el uso abusivo de dispositivos y mecanismos informáticos en donde ilegítima y premeditadamente se diseñe, fabrique, desarrolle, distribuya, venda, obtenga o importe uno o varios dispositivos, mecanismos, contraseñas,

programas informáticos, códigos de acceso o cualquier otro tipo de información informática, especialmente creados para cometer crímenes tipificados en la ley o el que brinde su servicio para contribuir a tal propósito será acusado con la privación de la libertad en un periodo de entre uno a cuatro años y de 30 a 90 días de multa.

Estos artículos de la Ley Nº 30096 fueron modificados por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014*:*

3.1. Tipicidad objetiva de los delitos contra datos y sistemas informáticos

Según a Chávez (2018) en la tipicidad objetiva de los crímenes que atenten en los sistemas y datos informáticos se describe:

- El sujeto activo en los crímenes contra sistemas e información informática es la persona o grupo de personas que realizan acciones ilícitas dirigidas a comprometer la seguridad, integridad, confidencialidad o disponibilidad de sistemas informáticos y datos.
- El sujeto pasivo en los crímenes contra sistemas e información informática es la entidad que sufre las consecuencias del acto delictivo, siendo afectada la integridad, confidencialidad o disponibilidad de su información y sistemas informáticos.
- El bien jurídico protegido dentro del contexto de los crímenes informáticos se refiere a los datos que se almacenan, tratan y transmiten de manera eficiente, generando un beneficio para la sociedad. Según Reyna (2001), el bien jurídico penal tutelado se basa en los datos como valía económica de la organización, los cuales no solo constituyen un interés vital social, sino que también se ajustan a parámetros que merecen tutela y protección.
- Conducta delictiva. De acuerdo a lo plasmado en la Ley 30096 este tipo de conductas se basa en un inicial hecho único y solo cuando se da el ingreso al sistema.

Conducta típica

En lo referente a los crímenes contra sistemas y datos informáticos, las acciones típicas se basan en aquellas que, de forma premeditada e ilícita, acceden a los sistemas. Estas acciones incluyen dañar, importar, borrar, deteriorar, modificar y hacer que los datos digitales sean inaccesibles, así como impedir la accesibilidad e inutilizar los sistemas informáticos, afectando así su correcto funcionamiento. (Villanueva, 2023). Entre los elementos de la tipicidad objetiva se encuentran:

- Acceso al sistema informático total o parcialmente.
- Vulnerabilidad de los lineamientos de seguridad.
- Límite de autorización sobre pasados

3.2. Tipicidad subjetiva de los delitos contra datos y sistemas informáticos

Se trata de un delito doloso, motivo por el cual no se permiten las sanciones de las conductas culposas o un accionar imprudente (Rodríguez, 2023). Es un acto que se realiza deliberadamente de manera voluntaria e intencionada. Un ejemplo de este delito es el proceso realizado en Katherine Flores Morales la Cruz, por acceso ilícito (además de fraude informático) a quien el Juzgado penal impuso prisión preventiva de 9 meses debido a que siendo supervisora de procesos operativos en la agencia 2 del centro Comercial Mega Plaza del Banco de Crédito del Perú, accedió de manera intencional y vulnerando los sistemas de seguridad logro un provecho patrimonial de más de 1 millón de dólares.

3.3. El delito de Hacking

Este delito se define como de intromisión o intrusismo informático, es decir, la accesibilidad sin autorización a sistemas informáticos quebrantando la seguridad del mismo tipificado en el Art. 2 de la Ley Nº 30096 cuya pena establecida es de entre uno a cuatro años de provación de libertad (Elías, 2023). El hacking es el paso principal que emplean aquellos que realizan delitos informáticos atentando en contra de la integración de sistemas y datos informático o suplantando identidades, así como otros.

3.4. El delito de cracking

Conocido como sabotaje informático, se describe en el Art. 3 de la Ley Nº 30096, los crímenes que atentan contra la integridad y naturaleza de los sistemas informáticos se configuran cuando el delincuente, de forma ilegítima y premeditada, inutiliza parcial o totalmente el sistema informático. Esto imposibilita la accesibilidad y funcionalidad del servicio que presta dicho sistema. (Elías, 2023).

3.5. Consecuencia jurídica

Los atentados contra datos informáticos pueden incluir delitos como el hacking, el phising, la distribución de malware, robo de contraseñas, y la vulnerabilidad de seguridad en los sistemas informáticos, los cuales pueden ser cometidos para la obtención de beneficios económicos, políticos o personales por lo cual son sancionados con una pena no menor de un año ni mayor de seis, y en el artículo 11 se establece los supuestos de agravación de acuerdo al caso y en donde la pena tiene tendencia ascendente (Vargas, 2023).

IV. Naturaleza jurídica del delito contra la indemnidad y libertad sexual

De acuerdo a la Defensoría del Pueblo (2023), los padres y madres de familia sostienen que la mayor conexión al ciberespacio ha ido acompañada de mayores riesgos hacia la indemnidad y la libertad sexuales de los menores de edad. Las Tecnologías de la Información y las Comunicaciones (TIC) a pesar que han representado siempre desarrollo y ventajas para la sociedad, también han generado un desafío constante frente a los riesgos y peligros que pueden surgir de su mal uso.

En el Convenio sobre La Ciberdelincuencia Budapest (2001), tenemos lo siguiente:

> *Artículo 9.- Delitos relacionados con la pornografía infantil.*
>
> 1. *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático; c) la difusión o la transmisión de pornografía infantil a través de un sistema informático; d) la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e) la posesión de pornografía infantil en un sistema informático o en dispositivo de almacenamiento de datos informáticos .*

Tabla 2
Ciberdelitos contra la indemnidad y la libertad sexuales en la legislación penal peruana.

BIEN JURÍDICO	CIBERDELITO	ARTÍCULO
Contra los datos y los sistemas informáticos	Proposiciones a niñas, niños y adolescentes con fines sexuales por medios tecnológicos	Ley de Delitos Informáticos, artículo 5
	Acoso sexual	Código Penal, artículo 176-B
	Chantaje sexual	Código Penal, artículo 176-C
	Formas agravadas de violación de la libertad sexual	Código Penal, artículo 177
	Pornografía infantil	Código Penal, artículo 183-A

Fuente: Elaboración propia mediante ley Nº 30096 y Código Penal del Perú

En relación al ciberdelito contra la indemnización y la libertad sexual, los verbos autoritativos son aquellos que establecen contacto o comunicación

con menores a través de internet. La acción típica que se toma es interceptar intencional e ilegalmente datos informáticos (Villanueva, 2023)

De acuerdo a lo mencionado en el párrafo 1 del Convenio sobre La Ciberdelincuencia Budapest (2001), se entiende por pornografía infantil todo material pornográfico que tenga la imagen de: un menor, una persona que parezca menor o cualquier imagen realista que represente a un menor, adoptando un comportamiento sexualmente explícito.

De acuerdo a Valdera (2018) se define como ciberacoso o Grooming a la intención sexual realizada por un adulto a través del internet o de medios tecnológicos, con la finalidad de ganarse la confianza de los niños o adolescentes, y que estos envíen imágenes de índole, sexual, para que este adulto se satisfaga sexualmente, pudiendo concertar un encuentro físico y posteriormente abusar de estos menores de edad.

4.1. Bien jurídico protegido

La protección regulada en el artículo 5, de la Ley N° 30096, se orienta a tutelar la indemnidad y libertad sexual de niños, niñas y adolescentes, por lo que, estando al objeto de la ley, debe entenderse que estos entran a llenar el contenido de lo expresado en "otros bienes jurídicos de relevancia penal". Por este motivo, la necesidad y merecimiento de pena se habilitará cuando se menoscabe la indemnidad y libertad sexual de niños, niñas y adolescentes a través de las formas previstas en el artículo 5 de la referida Ley, lo cual se refiere a que el autor del delito utilice el internet u otros medios análogos para contactar con los menores con el propósito de pedir u obtener material pornográfico o para concertar una cita con la finalidad de sostener relaciones sexuales. (Valdera, 2018). En resumen, el bien jurídico se trata de la libertad sexual, la que es la base sobre la cual se estructura todo el derecho penal sexual.

4.2. Tipicidad objetiva del delito contra la indemnidad y libertad sexual

Sujeto activo: Este puede ser cualquier persona, es decir es quien contacta con un menor de 14 años a efectos de solicitarle u obtener material pornográfico o para llevar a cabo actividades sexuales o con un menor entre 14 a 18 años.

Sujeto pasivo: El sujeto pasivo son los menores de edad, esto están comprendidos como los menores de 14 años a quienes producto del delito se les vulnera la indemnidad sexual y también están comprendidos los como sujeto pasivo los menores de edad entre 14 y menor de 18 años.

Conducta típica**:** En este tipo de delito, se requiere la comisión por parte del sujeto activo una serie de comportamientos que ejecutan el accionar delictivo, las cuales son:

a. El que (sujeto activo) a través de internet u otro medio análogo contacta con un menor de 14 años (sujeto pasivo) para solicitar u obtener de él material pornográfico.

b. El que (sujeto activo) a través de internet u otro medio análogo contacta con un menor de 14 años (sujeto pasivo) para llevar a cabo actividades sexuales.

c. El que (sujeto activo) a través de internet u otro medio análogo contacta con una persona entre 14 y menor a 18 años (sujeto pasivo) y medie engaño, para solicitar u obtener de él material pornográfico o para llevar actividades sexuales con él.

Cabe mencionar que, en los 3 comportamientos anteriores, se indica el contactar a través de internet por medio de cualquier tipo de tecnología de la información y la comunicación (TIC)

4.3. Tipicidad subjetiva de los delitos contra la indemnidad y libertad sexual

En este delito es netamente doloso, es decir para la violación de la indemnidad y libertad sexual por medios tecnológicos, el autor tiene plena conciencia de que va a realizar una acción que va a provocar un perjuicio a otra persona. Cuando el autor del hecho punible actúa con dolo, quiere cometer ese delito a sabiendas del daño que va a causar. Por lo que el agente o sujeto activo tiene que tener la intención dolosa y estar dispuesto a realizar las acciones típicas del delito.

4.4. Otros delitos facilitados por la tecnología en el Código Penal Defensoría del Pueblo (2023)

Además de los ciberdelitos tipificados en la Ley de Delitos Informáticos, el Código Penal prevé y sanciona delitos facilitados por el uso de las tecnologías de la información y las comunicaciones, que constituyen el modus operandi de los delincuentes. Entre estos, se pueden identificar los siguientes:

a. Ciberdelitos contra la indemnidad y la libertad sexuales, que comprenden el acoso sexual, el chantaje sexual y las formas agravadas de los delitos de violación de la libertad sexual.

    - El acoso sexual, incorporado en el artículo 176-B del Código Penal por el Decreto Legislativo Nº 1410, publicado el 2 de setiembre del 2018. Una de sus modalidades se comete valiéndose de las tecnologías de la información y las comunicaciones para vigilar, perseguir, hostigar, asediar o buscar establecer contacto o cercanía con una persona, sin el consentimiento de esta, para llevar a cabo actos de connotación sexual. Se agrava cuando la

víctima es adulta mayor, se encuentra en estado de gestación o tiene discapacidad; la víctima y el autor tienen o han tenido relación de pareja, son o han sido cónyuges o convivientes, o tienen vínculo parental hasta el cuarto grado de consanguinidad o segundo de afinidad; la víctima habita en el mismo domicilio que el agente o comparten espacios comunes en la misma propiedad; la víctima se encuentra en estado de dependencia o subordinación respecto del autor; la conducta se realiza en una relación laboral, educativa o formativa de la víctima; o cuando la víctima es adolescente entre 14 y 17 años de edad.

- El chantaje sexual, conocido como sextorsión, también fue incorporado en el artículo 176-C del Código Penal por el Decreto Legislativo Nº 1410. Este delito consiste en amenazar o intimidar a una persona por cualquier medio, incluyendo las tecnologías de la información y las comunicaciones, para obtener de ella una conducta o acto de connotación sexual. Se agrava si para su ejecución el autor amenaza a la víctima con la difusión de imágenes, materiales audiovisuales o audios con contenido sexual en los que esta aparece o participa.

- La Ley Nº 30838, publicada el 4 de agosto del 2018, modificó el artículo 177º del Código Penal para considerar como formas agravadas de los delitos sexuales –violación sexual, violación de persona en estado de inconsciencia o en la imposibilidad de resistir, violación de persona en incapacidad de resistencia, violación de persona bajo autoridad o vigilancia, violación sexual mediante engaño, actos contra el pudor y tocamientos, actos de connotación sexual o actos libidinosos sin consentimiento– cuando el autor registre estas conductas con cualquier medio visual, auditivo o audiovisual, o las transmita mediante tecnologías de la información y las comunicaciones.

b. Ciberdelitos contra la intimidad y el secreto de las comunicaciones, que comprenden los delitos de violación de la intimidad; la difusión de imágenes, materiales audiovisuales o audios con contenido sexual; la organización y el uso indebido de archivos computarizados; la posesión o comercialización de equipos destinados a la interceptación telefónica o similares; y la interferencia de comunicaciones electrónicas, de mensajería instantánea y similares.

    - La violación de la intimidad de la vida personal o familiar (artículo 154º), que se comete observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de

instrumentos, procesos técnicos u otros medios, o revelando la intimidad conocida de la manera antes prevista. Este delito se agrava por el uso de algún medio de comunicación social o si el autor actúa como funcionario o servidor público en el ejercicio del cargo y, más aún, si accede a la información a partir de la aplicación de la localización o geolocalización.

- El sexting no consentido, incorporado en el artículo 154-B del Código Penal por el mencionado Decreto Legislativo Nº 1410 de setiembre del 2018. Una de las formas agravadas de este delito consiste en la difusión, revelación, publicación, cesión o comercialización sin autorización de imágenes, materiales audiovisuales o audios con contenido sexual de cualquier persona, que se obtuvieron con su anuencia, utilizando redes sociales o cualquier otro medio de difusión masiva.

- La organización y el uso indebido de archivos computarizados (artículo 157º), que se realiza cuando alguien indebidamente organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas, y otros aspectos de la vida íntima de una o más personas. Este delito se agrava cuando el autor es funcionario o servidor público, y comete el delito en el ejercicio del cargo.

V. Naturaleza jurídica del delito informático contra el patrimonio

Se consideran delitos informáticos contra el patrimonio, aquellos comportamientos delictivos conducentes a burlar los procedimientos de seguridad, por medio del anagrama de ingreso, daño o destrucción a la base información o datos y aplicativos, etc., siendo materia de estudio hacia la propiedad, en los modos de sabotaje, estafa, fraude y hurto.

El fraude informático integra el grupo de delitos que afectan intereses patrimoniales ajenos, cuestión que lo acerca claramente a los delitos contra la propiedad, regulados en el Capítulo 5, artículo 8 de la Ley Nº 30096. Como se dijo, tal afectación, unida a la frecuencia de su comisión, explica que el fraude informático se haya convertido en la figura central de la criminalidad informática, actualmente muy relacionada con el comercio electrónico y las transferencias de fondos en línea a tal grado que, durante la pandemia del Coronavirus, se consideró a los ciberdelitos la otra pandemia que avanzó en silencio, debido a las cifras de fraudes que tuvieron un incremento del 59% durante los 6 primeros meses de la pandemia en 2020 (Flores, 2020)

Delgado (2022) describe esta modalidad de infracción informática como el ingreso ilícito a los datos o algún bien inmaterial o material, violando

las políticas de garantía de los sistemas informáticos, redes y dispositivos electrónicos con la finalidad de beneficio ilegal utilizando actos engañosos.

Tabla 3
Ciberdelitos contra el patrimonio en la legislación penal peruana.

BIEN JURÍDICO	CIBERDELITO	ARTÍCULO
Contra el patrimonio	Fraude informático	Ley de Delitos Informáticos, artículo 8
	Formas agravadas de estafa	Código Penal, artículo 196-A, numeral 5

Fuente: Elaboración propia mediante ley Nº 30096 y Código Penal del Perú

El artículo 8 de la "ley de delitos informáticos" tipifica una sola modalidad de delitos informáticos contra el patrimonio, al cual se rotula con el *nomen iuris* de "fraude informático":

> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa (Art 8 modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014)

Espinoza (2023) considera que se debería agregar a ese artículo un agravante como el incluido para cuando se afecte el patrimonio del Estado destinado a fines asistenciales o programas de apoyo social. Refiere que también debería incluirse una pena mayor si los agraviados son mayores de 60 años de edad, personas discapacitadas, de escasos recursos económicos, contra fondos de pensiones de jubilación o cuentas alimenticias de menores.

5.1. Bien jurídico protegido

Como en todos los delitos informáticos, existen varios bienes jurídicos afectados pero el principal en este tipo de ciberdelito es el patrimonio, el cual se trata de dinero electrónico que es desplazado desde la cuenta o tarjeta del agraviado y es transferido a cuentas de terceros desde donde será retirado o trasferido a la cuenta de los ciberdelincuentes.

5.2. Tipicidad objetiva del delito informático contra el patrimonio

La ley tipifica el denominado "fraude informático", que en su materialidad reclama que el agente, a través de las tecnologías de la información o de la comunicación, procure para sí o para otro un provecho ilícito en perjuicio de tercero, mediante el diseño, introducción, alteración, borrado, supresión,

clonación de datos informáticos o manipulación en el funcionamiento de un sistema informático.

Sujeto activo: El sujeto activo es genérico, el tipo no exige condición y/o cualidad específica. La persona que entra a una cuenta bancaria mediante la manipulación de los mecanismos de seguridad como clave, o token, o del sistema informático y realiza operaciones de trasferencias, pagos y demás, o la persona que con los datos de la tarjeta bancaria realiza compras no autorizadas por el titular. Se debe entender que estas personas, por lo que el sujeto activo también se considera al que presta su cuenta bancaria para que le trasfieran el dinero sustraído, el que recoge el dinero sustraído y todas las personas que participan. En este tipo de delito el sujeto activo puede ser un hacker, el trabajador de una entidad bancaria que facilita datos de sus clientes, el trabajador de una empresa de telefonía que repone chips sin autorización, un gamer o hacker amateur que realiza pedidos de comida o ropa con tarjetas bancarias de otros.

Sujeto pasivo: Este sujeto también es genérico. Los agraviados de este delito son varios desde personas de la tercera edad, personas que no tienen mucho conocimiento de operaciones bancarias, y hasta abogados, ingenieros, o profesionales de informáticos, es decir cualquier persona tenga conocimientos o no de informática puede ser víctima de del delito de fraude. En cualquier momento, los delincuentes informáticos pueden hacer una trasferencia no autorizada o alguna compra sin que tengamos conocimiento de ello. Hay que tener en cuenta que el sujeto pasivo también puede tratarse de una empresa o persona jurídica

Objeto del delito: Lo constituyen los sistemas informáticos de los bancos, las cuentas bancarias, las tarjetas de débito o crédito y las claves o token bancarias, las cuales son el blanco de los delincuentes con la finalidad de obtener un provecho ilícito.

Conducta típica: Las conductas exigidas por el código penal para este delito son:

- Procura para sí o para otro un provecho ilícito;
- Su conducta es en perjuicio de terceros;
- Lo hace mediante la planificación y elaboración de un plan;
- Introducción de claves;
- Alteración de datos y claves
- Borrado de datos;
- Supresión de datos;

- Clonación de datos informáticos como duplicados de tarjetas
- Manipulación de cuentas o tarjetas

5.3. Tipicidad subjetiva del delito informático contra el patrimonio

El tipo se representa como eminentemente doloso, porque el delincuente informático actúa con intención, a propósito, y de manera planeada. La norma presupone como condición objetiva de punibilidad que el comportamiento intrusista esté orientado a procurar, para sí o para otro, un provecho ilícito en perjuicio de tercero, exigiéndose de esta manera que el comportamiento esté motivado por un especial animus lucrandi, que debe comandar el inicio y desarrollo de la acción (Vizcardo, 2014)

5.4. Nuevos tipos de fraude

Debido a que las conductas en el ciberdelito son fronterizas en la actualidad no existen instrumentos eficaces para que los Estados acoten prácticas delictivas vinculadas a la nueva realidad tecnológica, por este motivo, cada vez más los ciberdelincuentes se ingenian para crear maneras de realizar sus actuaciones fraudulentas (Camargo et al., 2023). Entre las modalidades de fraude informático, se tienen las siguientes:

Prishing

Termino en ingles que alude a pescar. Este ciberdelito está "diseñado para usurpar la identidad de una persona pasiva y que consiste en la obtención de información como: números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales mediante engaño. Por ejemplo: cuando se recibe un correo electrónico o una ventana emergente y la víctima ingresa su nombre o información personal, y así, a los delincuentes les resulta más fácil obtener nuestros datos (Nazario y Villanueva, 2022)

Vishing

Esta es una modalidad de phishing en donde la víctima es contactada por medio de una llamada telefónica en donde el delincuente se hace pasar por agente del banco o vendedor de pólizas de seguros. Lo que busca el delincuente es acceder o conocer datos relevantes de la víctima (Carriedo, 2022)

Smishing

El smishing es una variante de phishing, pero mediante mensajes de texto (SMS). El delincuente envía enlaces adulterados a sus víctimas con la finalidad de asumir la figura de una entidad pública o privada para que sea la misma victima quien brinde sus datos personales bajo engaño (Flores, 2020)

Pharming

Este delito se configura cuando el delincuente crea y opera una página web falsa, con todas las características de la original, a modo de realizar operaciones normalmente, proporcionando información personal que pueda validar sus operaciones en los canales virtuales dispuestos por el banco, de esta manera el pharming no se lleva a cabo enviando mails en modo masivo, si no que se vulnera la dirección de la web lícita para redirigir a las personas que ingresen hacia otro alojamiento falso pero que aparentemente es el verdadero (Tuesta, 2022).

Clonación de tarjetas

El delito se comete utilizando un lector electrónico de banda magnética (*Skimmer*) *por medio del cual algunos empleados deshonestos* de restaurantes, gasolineras y otr*os establecimientos extraen* datos de tarjetas de crédito. Luego se copia*n en* una computadora portátil o PC y finalmente se copia a otra tarjeta clonada que contiene los mismos datos personales que la tarjeta original. Por ejemplo: cuando *se* realiza una compra mediante entrega *delivery* y utiliza un punto de venta *(POS)* modificado para extraer los datos de la tarjeta de crédito, los delincuentes clonarán dicha tarjeta y realizarán compras en línea o m*ediante otros canales digitales (Flores, 2020)*

5.5. Propuesta de regulación del fraude informático en actual trámite parlamentario

La firma de abogados CPB refiere que, el Grupo Parlamentario Perú Libre presentó el Proyecto de Ley N°3251/2022-CR, con la finalidad de regular la responsabilidad que tienen las empresas del Sistema Financiero en los fraudes informáticos cometidos a sus clientes mediante operaciones activas y pasivas fraudulentas, y de esta manera establecer las acciones a cumplir para resolver los problemas y el tiempo para hacerlo. De esta manera, mediante este proyecto de ley, se busca proteger y garantizar las operaciones activas y pasivas de los clientes y usuarios del sistema financiero, para reducir el perjuicio económico que estos actos producen en el ciudadano y salvaguardar la reputación crediticia de la empresa.

Las medidas adoptadas son: la obligación de devolver los importes y/o anular las operaciones no autorizadas reportadas por los usuarios de las entidades financieras, en cualquier caso y a más tardar al día hábil siguiente de reportado el incidente. Solamente, si la empresa tiene pruebas para dudar de la veracidad del reporte, deberá informarlo por escrito a la brevedad tanto al usuario como a la Superintendencia de Banca, Seguros y AFP, adjuntando las pruebas que sostienen su decisión, así como la prueba de que en esa operación se activaron todos los mecanismos de verificación que

demuestren que dicha operación fue correctamente realizada (Congreso de la República, 2022).

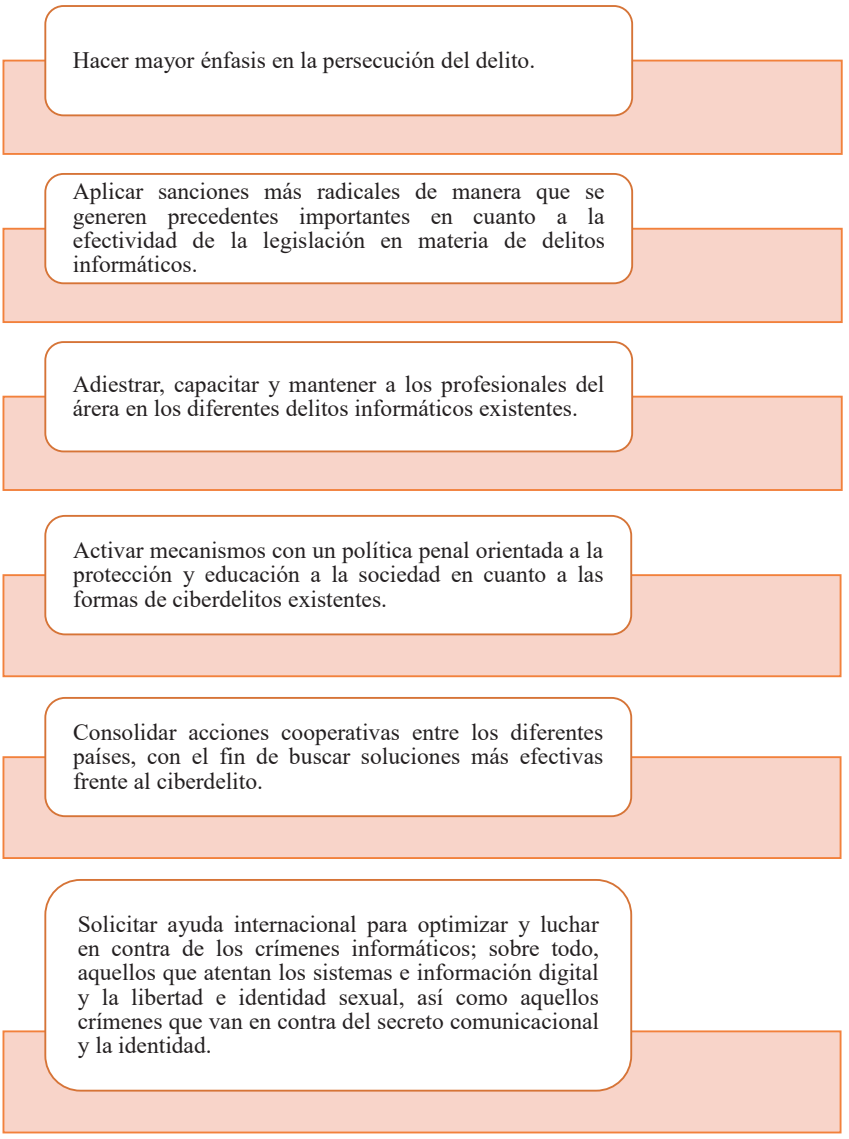
VI. Propuesta

Partiendo del hecho de que la Constitución Política de Perú establece los derechos a la dignidad humana, y considerando que la tecnología informática está presente en todos los ámbitos de la sociedad, desde el entorno laboral, social, familiar, educativo, salud, bancario entre otros, es necesario que se realice una revisión a las leyes que regulan el uso de dicha tecnología y los mecanismos que permitan imputar los delitos cibernéticos; pues, así como la tecnología ha influido en el crecimiento y rendimiento de los recursos económicos y académicos, también se ha convertido en una fuente útil para aquellos que se dedican a desarrollar plataformas delictivas especializados en la estafa y suplantación de identidad.

A dichas acciones se les ha tipificado con la denominación de delitos informáticos, para lo cual, los países a nivel mundial decidieron establecer las leyes de delitos en esta área en sus respectivos países. En el caso de Perú, la Ley de Delitos Informáticos, la cual en palabras de Morales (2016), requiere ser estudiada a profundidad por poseer varias críticas que van desde la ausencia de medidas de prevención en cuanto a los delitos cometidos contra datos y sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexual hasta los delitos informáticos contra la intimidad y el secreto de las comunicaciones, los cuales considera de muchas formas llenas de vacíos.

En este sentido en la Figura 2 se ofrecen algunas propuestas.

Figura 2
Propuesta como respuesta ante las víctimas de delitos informáticos



6.1. Consecuencias de la implementación de la propuesta

La implementación de una propuesta enfocada en combatir o dar respuesta a las víctimas de delitos informáticos, genera con consecuencia la inversión que el Estado de hacer en la preparación y capacitación de personas encargado de investigar los delitos y demostrar el hecho. Todo ello como consecuencia de que el ciberdelito es un agravante que se manera a través de los medios tecnológicos y que requiere una normativa más eficiente que la regule. En opinión de Chipana (2023), la influencia conducida por el tratamiento de los delitos informáticos en el país es relativa aun cuando hoy día se cuenta con el apoyo de la comunidad internacional a través del Convenio de Budapest, la cual permite establecer lazos de ayuda mutua entre países de Latinoamérica y del mundo que se encuentran dentro de dicho convenio.

Otra de las consecuencia obedece a la implementación de políticas de seguridad más estrictas, las cuales, son un poco complicadas de desarrollar considerando que existe un alto nivel de uso de las fuentes informáticas, donde las personas no toman en cuenta las consecuencias de brindar información confidencial a desconocidos en las redes, adicionalmente, el desinterés de muchos en entender que no todo lo que circula por las redes es confiable, lo cual se convierte en una oportunidad para los ciberdelincuentes.

6.2. Beneficios que aporta la propuesta

Dentro de los beneficios que aporta lo que se propone en este estudio, se pueden mencionar los siguientes:

Incremento de la bioseguridad en todos los niveles sociales, laborales y empresariales, incluyendo a los organismos nacionales.

Se requiere capacitar a los individuos para que estos conozcan que hacer y a dónde acudir si son víctimas de crímenes cibernéticos, así como evitar serlos.

Incorporar nuevos modus operandi en la Ley de Delitos Informáticos a fin de actuar de forma más eficiente y efectiva contra tales situaciones.

VII. Conclusiones

La tecnología informática surge con las primeras computadoras a nivel mundial, con el paso de los años la tecnología comenzó a sufrir grandes innovaciones que involucraron la evolución de los celulares y computadoras, posteriormente nace el internet convirtiéndose en una red informática mundial, el cual tuvo un impacto positivo por cuanto permitió que todos los países del mundo se conectaran. Seguidamente nacen las redes sociales mediante las cuales las personas, organizaciones, ministerios y países mantienen conexiones importantes; unos con fines recreativos, de comunicación y otros con fines comerciales.

Pero con el nacimiento de estos medios, nacen también aquellos que, especializándose en la materia tecnológica deciden dedicarse al delito. Estos delitos iniciaron con los robos de datos de tarjetas de crédito y débito, que en algunos países denominaron clonación de tarjetas, delito penalizado en el artículo 8 de la Ley de Delitos Informáticos de Perú.

Sin embargo, para efectos de este estudio, se indagó de tres delitos fundamentales que se deben conocer: crímenes que atentan en contra el sistema y la información digital, crímenes informáticos que atentan contra la libertad identidad sexual y aquellos en contra del secreto comunicacional y la intimidad. Cada uno de ellos posee su pena en la Ley correspondiente, y a través de las indagaciones se observa que cada país contempla en sus respectivas leyes las penas a cumplir por delito cometido, sin embargo, existen vacíos jurídicos, así como desconocimiento de la población sobre cómo actuar cuando sufre algún tipo de daño cibernético.

Es una realidad, que esta problemática va en alarmante crecimiento, pues el acceso a los medios informáticos es cada vez más extenso y los mismos son cada año más novedoso que el año anterior; es decir, cada año la tecnología evoluciona y con ello la destreza de los ciberdelincuentes. Nada más en el Perú durante el año 2017 muchas instituciones se vieron afectadas por los famosos programas ransomware, los cuales son códigos que al ser descargados en los equipos inician un ataque que involucra el secuestro de información y bloqueo del equipo, evitando que el usuario pueda manipularlo.

En consecuencia, es importante que, a medida que evoluciona el delito cibernético también evolucionen las leyes, o en su defecto, se le adiciones artículos que traten de forma específica los delitos inmersos dentro de los tipos ya presentes en las mismas.

Referencias

Acosta, M., Benavides, M., García, N. (2020). Cybercrime: Impunity organizational and its complexity in the business of the world. *Revista Venezolana de Gerencia 25* (89). ISSN: 1315-9984. https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Alarcón, L. (2023). Robos digitales: las millonarias multas a los bancos por consumos no reconocidos. *Ojo Público.* https://ojo-publico.com/4559/las-millonarias-multas-los-bancos-por-consumos-no-reconocidos

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos*. Tesis de Grado. Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/80920/Aredo_LLA-SD.pdf?sequence=1&isAllowed=y

Camargo, Z. R. L., Gálvez, E. I. T., Rodríguez, E. L. O., & Camargo, J. L. (2023). Evasión tributaria y su incidencia en la recaudación del impuesto a la renta en Perú. *Revista de ciencias sociales*, *29*(7), 420-432. https://dialnet.unirioja.es/servlet/articulo?codigo=9034448

Chávez, E. (2018). *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017.* Tesis de Doctorado. Universidad Nacional Federico Villarreal. https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Chipana, E. y Rivera B. (2023). *Análisis jurídico de la regulación del ciberacoso en la Ley de delitos informáticos, Perú-2022.* Tesis de Grado. Universidad Cesar Vallejo. https://hdl.handle.net/20.500.12692/127894

Carriedo, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México.* Tesis de Maestría. Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Contreras, S. (2024). Los delitos informáticos en el Código Penal. Dexia Abogados. https://www.dexiaabogados.com/blog/delitos-informaticos/

Convenio sobre La Ciberdelincuencia Budapest. (2001). https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

Defensoría del Pueblo. (2023). La ciberdelincuencia en el Perú: Estrategias y retos del Estado. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Delgado Benites, F. J. (2022). El tratamiento penal de los delitos informáticos contra el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa-Chimbote. [Tesis de Licenciatura: Universidad Señor del Sipán]. Repositorio de Universidad Señor del Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/10400

Díaz, M. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista criminalidad*, *62*(2), 199-217. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/download/168/258

El Comercio (2023). ¿Cómo será la ciudad inteligente que quiere construir Bill Gates?. [25 de noviembre de 2023]. https://elcomercio.pe/tecnologia/actualidad/como-sera-la-ciudad-inteligente-que-quiere-construir-bill-gates-noticia/

Elías, R. (2022). **La evolución del cibercrimen en el Perú. De hurtos telemáticos a ataques contra sistemas informáticos**. En *Cibercriminalidad y delitos informáticos. Aspectos sustantivos, probatorios y jurisprudenciales. Protección penal de la información y sistemas informáticos.* (pp. 40 - 85). LIMA. Instituto Pacífico. Recuperado de: https://revistas.pucp.edu.pe/index.php/themis/issue/view/1312

Elías, R. (2023). El delito de hacking o acceso ilícito a sistemas informáticos. THEMIS Revista De Derecho, (83), 413-433. https://doi.org/10.18800/themis.202301.023

Espinoza, M. (2022). *Mitigación de vulnerabilidades informáticas utilizando un firewall de software libre con Pfsense en las empresas de revisiones técnicas de la ciudad de Tacna en el año 2021.* Tesis de grado. Universidad Privada de Tacna. https://repositorio.upt.edu.pe/bitstream/handle/20.500.12969/2575/Espinoza-Peche-Maximo.pdf?sequence=1&isAllowed=y

Flores, J. (2020). Los ciberdelitos: la otra pandemia que avanzó en silencio en el Perú, [18 de abril del 2020]. https://pagina3.pe/tecnologia/los-ciberdelitos-la-otra-pandemia-que-avanzo-en-silencio-en-el-peru/

Flores, J. (2023) Delitos a través de plataformas virtuales. ¿Vinculación necesaria a los tipos penales previstos en la Ley de Delitos Informáticos? En *Cibercriminalidad y delitos informáticos. Aspectos sustantivos, probatorios y jurisprudenciales. Protección penal de la información y sistemas informáticos.*. (pp. 40 - 85). LIMA. Instituto Pacífico. Recuperado de: https://revistas.pucp.edu.pe/index.php/themis/issue/view/1312

Guerrero, E. (2020). Efectos de la pandemia de COVID-19 sobre la adopción de las TIC en el Perú. *Ius Inkarri*, *9*(9), 491-523. http://revistas.urp.edu.pe/index.php/Inkarri/article/view/3697

Huayca, H. (2022). *Propuesta modificatoria de artículos 8 y 9 de Ley 30096 ante incremento de Delitos Informáticos*. Tesis de Grado, Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/116339/Huayca_JHG-SD.pdf?sequence=1&isAllowed=y

Indacochea, J. F. (2022). *La eficiencia administrativa y su incidencia en la liquidez de la microempresa jipi chifle en la ciudad de Jipijapa*. [Tesis de licenciatura: Universidad Estatal del Sur de Manabí]. Repositorio de la Universidad Estatal del Sur de Manabí. https://repositorio.unesum.edu.ec/bitstream/53000/3409/1/TESIS-%20JULEISY%20FERNANDA%20INDACOCHEA%20FIGUEROA.pdf

Laboy, L., Steiner, A. I. R., & Suárez, W. F. (2021). La violencia digital como amenaza a un ambiente laboral seguro. In *Forum Empresarial* (Vol. 26, No. 1, pp. 99-107). Centro de Investigaciones Comerciales e Iniciativas Académicas. https://www.redalyc.org/journal/631/63169773004/63169773004.pdf

Ley N° 29904, Ley de promoción de la banda ancha y construcción de la Red Dorsal Nacional de Fibra Óptica. (15 de abril de 2015). https://www.osiptel.gob.pe/media/py5js1qy/ds014-2013-mtc.pdf

Ley Nº 30096, Ley de Delitos Informáticos (5 de diciembre de 2013). https://www.policia.gob.pe/pnp/archivos/portal/doc/9885doc_24.pdf

Ley Nº 30838, Ley que modifica el código penal y el código de ejecución penal para fortalecer la prevención y sanción de los delitos contra la libertad e indemnidad sexuales. (4 de agosto de 2018). https://busquedas.elperuano.pe/dispositivo/NL/1677448-1

La cámara (2024). Inseguridad ciudadana en el Perú: cifras impactantes y soluciones urgentes. [18 de febrero del 2024] https://lacamara.pe/inseguridad-ciudadana-en-el-peru-cifras-impactantes-y-soluciones-urgentes/

Martínez, R., Palma, A. y Velásquez A. (2020). Revolución tecnológica e inclusión social. Reflexiones sobre desafíos y oportunidades para la política social en América Latina. CEPAL. https://www.cepal.org/sites/default/files/publication/files/45901/S2000401_es.pdf

Morales, D. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10002/Nazario%20Delgado%20Nora%20%26%20Villanueva%20Sanchez%20Lucia.pdf?sequence=6&isAllowed=y

Nazario, N. y Villanueva L. (2022). *Fraude informático en la modalidad de Phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal.* Tesis de Grado. Universidad Señor del Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10002/Nazario%20Delgado%20Nora%20%26%20Villanueva%20Sanchez%20Lucia.pdf?sequence=6&isAllowed=y

Ocupa, B. (2023). *Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022. [*Tesis de Maestría] Universidad cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/119930/Ocupa_SBS-SD.pdf?sequence=5&isAllowed=y

Presidencia de la República del Perú- (1984). Decreto legislativo 295 de 1984. Código Civil. Diario oficial el Peruano del 25 de julio de 1984. https://spijlibre.minjus.gob.pe/content/publicaciones_oficiales/img/Codigo-Civil.pdf

Presidencia de la República del Perú. (2018). Decreto legislativo 1410 de 2018. Decreto legislativo que incorpora el delito de acoso, acoso sexual, chantaje sexual y difusión de imágenes, materiales audiovisuales o audios con contenido sexual al código penal, y modifica el procedimiento de sanción del hostigamiento sexual. https://busquedas.elperuano.pe/dispositivo/NL/1690482-3

Proyecto de Ley Nº 5630/2020-CR. Ley de Seguridad Informática y Represión de los Delitos Informáticos. https://www.osiptel.gob.pe/media/bdidmioz/pl-5630-2020-cr.pdf

Reglamento de Neutralidad de Red Nº 165-2016-CD/OSIPTEL, modificado por la Resolución de Consejo Directivo N.° 003-2023-CD/ OSIPTEL. (9 de enero de 2023). https://busquedas.elperuano.pe/dispositivo/NL/2142044-1

Reyna Alfaro, L. M. (2001). Reflexiones sobre el contenido del bien jurídico-penal y la protección de los bienes jurídicos colectivos. *Revista jurídica del Perú*, *51*(18), 187-200.

Rodríguez, F. R. (2023). *Delitos informáticos-1ra edición*. Ecoe Ediciones.

Tavora, M. (2022). Vigilancia e investigación policial en el ciberespacio aspectos procesales del ciberpatrullaje. [Tesis de Doctorado]. Universidad de Sevilla. https://dialnet.unirioja.es/servlet/dctes?codigo=309409

Tuesta Estela, R. C. (2022). Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima–2022. [Tesis de Pregrado: Universidad Norbert Wiener]. Repositorio Universidad Norbert Wiener. https://repositorio.uwiener.edu.pe/handle/20.500.13053/8054

Universidad Nacional de la Rioja (2022). Tipos de delitos informáticos y legislación aplicable. *La universidad en internet* (28 de noviembre de 2022. https://www.unir.net/derecho/revista/tipos-delitos-informaticos

Valdera, J. (2018). El protocolo de investigación, denuncia y juzgamiento del grooming. [Tesis de Maestría: Universidad Nacional Pedro Ruiz Gallo]. Repositorio de la Universidad Nacional Pedro Ruiz Gallo. http://repositorio.unprg.edu.pe/handle/20.500.12893/7903

Vargas, M. (2023). Atentado a la Integridad de datos informáticos. (Artículo 3 de la Ley de Delitos Informáticos). En *Cibercriminalidad y delitos informáticos. Aspectos sustantivos, probatorios y jurisprudenciales. Protección penal de la información y sistemas informáticos.*. (pp. 40 - 85). LIMA. Instituto Pacífico. Recuperado de: https://revistas.pucp.edu.pe/index.php/themis/issue/view/1312

Velarde, C. (2023). Prevención de los ciberdelitos. Algunas reflexiones desde casos ocurridos en el Perú. *Revista Iberoamericana de Derecho Informático* (13) 133-148. https://dialnet.unirioja.es/servlet/articulo?codigo=9265282

Villanueva, J. (2023). Ley de delitos Informáticos N° 30096 y su influencia en La Población de Chiclayo en tiempos de Covid-19. Tesis de Grado. Universidad Señor del Sipán https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10627/Villanueva%20Calderon%20Juan%20Amilcar.pdf?sequence=1&isAllowed=y#:~:text=Tipicidad%20Objetiva%20de%20los%20Delitos,producto%20de%20una%20causalidad%20simple

Vizcardo, S. J. H. (2014). Tipificación de los Delitos Informáticos Patrimoniales en la nueva ley de Delitos Informáticos N 30096. *Alma máter segunda época*, (1), 69-80. https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/view/11870