Código:	2	0	2	2		0	7	7	8	

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESTUDIOS GENERALES LETRAS

TRABAJO INDIVIDUAL

Título: **"Tras las Huellas Digitales del Fraude": Las Regulaciones Legales aplicadas en el Estado Peruano en contra de los Fraudes Informáticos, Desafíos y Comparación con Perspectivas Internacionales.**

Alumno(a): **MIKE NOÉ HUAMÁN SÁNCHEZ.**

Tipo de evaluación: **Entrega Final Monografía**

Curso: **Investigación Académica (INT-124)**

Horario: **0303**

Comisión: **B**

Profesor(a): **Richard O'Diana Rocca**

Jefe de Práctica: **Pedro Calvay Torres**

SEMESTRE 2023-2

Código:	2	0	2	2	0	7	7	8	

Título de la monografía

“Tras las Huellas Digitales del Fraude”: Las Regulaciones Legales aplicadas en el Estado Peruano en contra de los Fraudes Informáticos, Desafíos y Comparación con Perspectivas Internacionales.

Presentada como parte del curso Investigación Académica, EEGGLL, PUCP

Nombre: Mike Noé Huamán Sánchez

20220778

0303 - 0303B

Correo electrónico: a20220778@pucp.edu.pe

Diciembre - 2023

Código:	2	0	2	2	0	7	7	8	

Resumen

En este presente trabajo de investigación se pretende evaluar la calidad de la regulación aplicada por el Estado Peruano ante los delitos informáticos. Por ello, se consideran aspectos como los antecedentes de la legislación actual de los ciberdelitos en Perú para proporcionar una visión óptima de la manera que tiene el país de comprender estos conceptos. Por lo que, en perspectiva de un análisis adecuado de esta problemática, la regulación nacional se busca comparar con los países de España, México, Reino Unido y Estados Unidos. La pregunta de investigación tiene como objetivo determinar las carencias o desafíos que enfrenta el Perú en cuanto a la regulación de los fraudes informáticos, en comparación con la experiencia legislativa de otros países a nivel global. La hipótesis plantea que la regulación de fraudes informáticos en el Estado Peruano es deficiente y presenta problemas en su implementación, debido a que este carece de un marco legal adecuado para enfrentar amenazas de delitos digitales.

De esta manera, al término de la investigación, se propone demostrar que el Estado Peruano, posee regulaciones y tipificaciones que resultan insuficientes para el control de nuevas formas delictivas, en especial en el ámbito de los fraudes informáticos. Además, en el tema del fraude informático, existe un debate en su definición por la ambigüedad de esta; debido a que, en algunos países, este delito se comprende como el uso no autorizado de sistemas informáticos y en otros, como en Perú, se refiere al acto de sustraer bienes o patrimonio mediante herramientas digitales.

Palabras clave: *ciberdelitos, fraude informático, derecho comparado, legislación peruana de delitos informáticos.*

Código:	2	0	2	2	0	7	7	8	

Tabla de Contenidos

Introducción

Ante la preocupante situación del aumento de casos delictivos en el Perú, la inseguridad ciudadana se ha convertido en un factor representativo de las principales problemáticas en la población. Debido a esto, cotidianamente se puede apreciar una cantidad considerable de delitos cometidos en diversos rubros que afectan a la integridad de los ciudadanos y a la estabilidad del país. Sumado a esto, el desarrollo constante de la tecnología y la integración de esta en la sociedad han permitido la aparición de infracciones con implicancias en un espacio digital. Es así que, en el ámbito de la seguridad ciudadana, surge un nuevo sector a analizar: la protección legal contra los delitos informáticos.

Los delitos informáticos, por el aumento de casos, se han convertido en una preocupación a nivel mundial y nacional; puesto que, el avance tecnológico de este tipo de ilegalidades permite una mayor facilidad de ejecución en estos y registra numerosas víctimas a causa de la desinformación que actualmente se tiene sobre esta problemática. Por ello, dicho factor es uno de los principales motivadores del desarrollo de esta investigación. La presencia de ciberdelitos en el Perú es una realidad social que un amplio sector de la población, de manera directa o indirecta, percibe y reconoce; incluso, es posible postular que algunos de los lectores de este presente proyecto hayan recibido mensajes o correos electrónicos de contactos que simulan ser una entidad bancaria o alguna institución de prestigio para solicitarles información personal o financiera.

De esta manera, el siguiente trabajo se enfocará en analizar las regulaciones legales aplicadas en el Estado Peruano, y la efectividad de estas, en contra de los delitos informáticos, en especial en el sector de los fraudes informáticos. Para empezar, en el primer capítulo se abordarán los conceptos básicos y jurídicos para comprender de manera más eficaz el tema de los ciberdelitos. Se detallará la definición estándar de delitos informáticos y el origen de este término, así como la de fraude informático y sus principales modalidades en el Perú. Además, debido a que la efectividad del marco legal peruano de los delitos informáticos se determinará también mediante la comparación con perspectivas internacionales, se mencionará el concepto del derecho comparado y la importancia que tiene en este estudio legislativo. En ese sentido, este capítulo de la investigación aportará conceptos de utilidad para el entendimiento del desarrollo del trabajo.

En vista de que la pregunta central del proyecto se basa en determinar cuáles son las carencias y desafíos que enfrenta el Perú en cuanto a la regulación de los fraudes

informáticos, en comparación con la experiencia y legislación de otros países a nivel global. El segundo capítulo se centrará en el desarrollo de la hipótesis planteada mediante el uso de dos variables de investigación.

En primer lugar, que la regulación aplicada en el Estado Peruano con respecto a los fraudes informáticos es ineficaz y no se encuentra correctamente tipificada. El estudio de dicha variable se acompañará de un análisis de los antecedentes previos al surgimiento de las normativas contra delitos informáticos en el Perú para postular el tipo de comprensión que tiene la legislación peruana en este rubro. Finalmente, como segundo punto, la regulación de fraudes informáticos en el Perú es incompleta a comparación de países de nivel internacional, como España, México, Reino Unido y Estados Unidos. De esta manera, se determinarán similitudes y diferencias que posee la nación en aspectos como la tipificación de delitos informáticos o la presencia de instituciones reguladoras de ciberdelitos.

Por este motivo, el trabajo de investigación se llevará a cabo mediante el análisis de la legislación peruana vigente en relación con los fraudes informáticos, así como también a través de la revisión comparativa de las regulaciones de otros países. Para esto, se utilizarán fuentes legales y académicas que proporcionen información relevante sobre las regulaciones y prácticas en materia de ciberseguridad y delitos informáticos en Perú y otros países. Asimismo, se tomarán en cuenta las experiencias y estudios previos del tema, así como informes y estadísticas de instituciones de seguridad ciudadana. El objetivo principal de la investigación es brindar un aporte de conocimiento y análisis acerca de las regulaciones legales aplicadas en el Estado Peruano en contra de los fraudes informáticos, identificando los desafíos y comparándolos con perspectivas internacionales.

Al culminar la investigación se buscará verificar la validez de la hipótesis, que indica que la regulación actual de los fraudes informáticos en el Estado Peruano es deficiente y exhibe una serie de problemas en su implementación; a diferencia de otros países de nivel internacional, los cuales cuentan con un marco legal relativamente idóneo para enfrentar las amenazas provenientes de los delitos digitales. Asimismo, se espera identificar las carencias específicas que enfrenta el Perú en términos de regulación de fraudes informáticos y proponer recomendaciones para mejorar esta situación, con base en las experiencias y mejores prácticas de otros países.

Capítulo I

Conceptos básicos y jurídicos

En este primer capítulo, se abordará los conceptos básicos y jurídicos necesarios para comprender adecuadamente el tema de los fraudes informáticos y las regulaciones legales aplicadas en el Estado Peruano frente a estos. Además, se profundizará en el campo de los delitos informáticos para entender su conexión con la problemática recurrente del aumento de casos cibernéticos-delictivos en el Perú.

1.1. Delitos informáticos

Con el constante avance tecnológico en el que estamos inmersos cada uno de los ciudadanos, es frecuente reconocer que acciones que realizamos de manera cotidiana, hace unos años, eran dificultosamente posibles de plantear. En la actualidad, gracias a la tecnología, encontramos soluciones a problemas que anteriormente requerían más tiempo y esfuerzo. Es así que, como lo plantean Nazario y Villanueva (2022), el desarrollo del mundo digital ha representado un aporte notable en la mejoría de las sociedades. Sin embargo, estos mismos avances han comprometido a las personas a depender cada vez más de sus dispositivos y las herramientas que estos les proveen; ocasionando así, que cada uno de nosotros esté más ligado a algún artefacto digital como los smartphones o las computadoras.

En ese contexto, la sociedad civil contemporánea, al trasladar obligatoriamente cada uno de sus datos personales a un espacio cibernético[1], se encuentra frente a problemáticas con actividades delictivas cometidas a través de medios electrónicos o digitales. Debido a que, según Pozo (2021), así como “el uso masivo del internet y los teléfonos celulares como Smartphone, tabletas, laptops, etc., nos han traído muchos beneficios, en el entorno académico, económico, cultural y social”, en las últimas décadas han originado nuevas formas de criminalidad. Y estas simbolizan un riesgo para la integridad de los ciudadanos en términos de información personal, patrimonio, entre otros elementos fundamentales.

Los delitos informáticos, denominados también cibercrímenes o ciberdelitos, se entienden como cualquier acción de carácter antijurídico que implique o se realice en un espacio digital. De igual manera, Ponce postula que los delitos informáticos “son aquellas

[1] El espacio cibernético es el ámbito virtual en el que se realizan actividades de un grupo de usuarios mediante dispositivos electrónicos para interactuar y compartir información (redes sociales, los sitios web, las bancas móviles, los correos electrónicos, entre otros).

conductas delictivas que tiene como objetivo las tecnologías de la información y comunicación (TIC) para efectuar hechos delictuosos y consumar [un] delito" (2022). Así pues, los delitos informáticos, al igual que los delitos comunes, son la representación de alguna actividad ilegal que vaya en contra a lo estipulado por la legislación de un determinado estado social y su regulación puede variar dependiendo de su gravedad o su naturaleza.

Como detalla Salinas (2013) la diferencia que denota este tipo de infracciones es la implicancia que poseen en relación con los diversos elementos informáticos presentes en la sociedad actual (citado en Nazario y Villanueva, 2022). Por ello, los métodos de ejecución de estas violaciones legales requieren del uso de dispositivos electrónicos como servidores, computadoras, celulares, entre otros.

1.1.1. Datos personales e informáticos

Asimismo, con el notable avance de la tecnología y que actualmente dicho progreso ha ocasionado una ruptura de las fronteras de la comunicación, nos encontramos frente a esta latente exposición de nuestra información (D'Avila y Leonhardt, 2016). Por ello, es importante precisar que entendemos por datos personales[2] e informáticos que exponemos en un entorno digital.

Complementando lo postulado, es posible aludir que los datos informáticos se refieren a la información almacenada y procesada en dispositivos electrónicos. Por ello, Cornejo alega que los datos informáticos son cualquier "representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático" (2021, p. 95). Estos datos pueden incluir archivos, imágenes, videos, mensajes u otra información que esté disponible de forma digital. De esta manera, debido a que el carácter de los datos personales y los datos informáticos provienen de la misma naturaleza, estos conceptos se encuentran estrechamente relacionados y se complementan para comprender las implicaciones legales de los delitos informáticos.

1.1.2. Características de los delitos informáticos

Algunas de las características principales de los delitos informáticos son las siguientes. En primer lugar, la ejecución de este tipo de actividades ilegales requiere de la

[2] Los datos personales son toda información que identifica o hace identificable a una persona existente. Es decir, son aquellos datos que están vinculados, de manera directa (nombres) o indirecta (número de DNI), a nuestra identidad.

utilización de un sistema digital, o red de computadoras, que produce servicios maliciosos con la finalidad de sustraer información. Asimismo, Ponce (2021) propone que cada uno de los infractores, en la mayoría de casos, son especialistas en temas de informática y tecnología. Además, suelen ser realizados por ciberdelincuentes desde el anonimato que emplean herramientas tecnológicas para ocultar su identidad y dificultar su rastreo (Riega, Huamani y Machuca, 2021).

Con relación a aquello, es posible denotar que los ciberdelitos varían ampliamente en su naturaleza; y estos, a su vez, suponen una evolución constante al ritmo de la tecnología para adaptarse a los nuevos medios y sistemas de comunicación. Esto principalmente debido a que, como menciona Agustina, “el uso de la tecnología como medio comisivo [...] es lo que caracteriza a los ciberdelitos” (2021) y aquello implica una serie de cambios continuos en los delitos.

1.1.3. Tipos de delitos informáticos

Precisamente por los continuos cambios en la tecnología anteriormente mencionados, es relevante analizar, a continuación, los tipos de delitos más frecuentes en la sociedad actual. Como menciona Cornejo (2021), los delitos informáticos comunes se vinculan con los objetivos de las conductas transgresoras, las cuales buscan efectuar un engaño hacia una víctima para obtener datos mediante diversas modalidades ilícitas. Para empezar, algunas de las infracciones cibernéticas más habituales son aquellas que implican la suplantación de identidad.

Este tipo de delito ocurre cuando una persona emplea la información de carácter personal de otra sin su consentimiento para realizar acciones fraudulentas, como abrir cuentas en redes sociales, efectuar compras en línea, entre otras. En ese sentido, la suplantación de identidad se entiende como la actividad de falsificar datos y representar una persona o imagen que no es de mi propiedad. Por ello, es posible aludir que dicho delito no solo hace referencia a la usurpación de identidad de un civil, sino también a la de entidades, instituciones o empresas. Además, con los avances digitales, el aumento en la frecuencia de esta práctica se ha reforzado con el fácil acceso a información personal que podemos encontrar en internet.

Otro de los ciberdelitos fuertemente presentes en nuestro contexto informático es el acoso cibernético. Este delito hace referencia a la persecución persistente y hostigamiento

de una persona o un conjunto de individuos, hacia otra, a través de medios electrónicos como redes sociales. En la actualidad, en específico en webs de uso social, es posible apreciar numerosos casos de víctimas de acoso cibernético, las cuales son expuestas a insultos, amenazas, difamación y otros. Sin embargo, la realización de este tipo de comportamientos no solo se limita a las redes sociales, sino que también se extiende a otros medios, como los mensajes de texto, llamadas telefónicas o correos electrónicos (Ruíz, Bono-Cabré y Magallón, 2019). Estas ilegalidades producen consecuencias emocionales y psicológicas en los afectados, promoviendo el deterioro de la salud mental de estos.

En el sector de la propiedad intelectual, las infracciones vinculadas con la violación de derechos de autor son igual de frecuentes. Como consecuencia de la globalización de las herramientas digitales, estas infracciones han aumentado y se destacan por incluir actos como la distribución o venta, sin previa autorización, de creaciones amparadas por leyes de derechos de autor. Es decir, dicha ilegalidad, poco regulada, es producto de la intensificación de la piratería con la tecnología, lo que convierte a este delito en una actividad accesible para cualquier ciudadano que posea algún dispositivo electrónico.

De igual manera, otras violaciones legales comunes dentro del espacio digital son aquellas en contra de la seguridad informática, en específico, la sustracción no autorizada de datos personales. Este delito, como postulan Riega, Huamani y Machuca, consiste en acceder a información confidencial sin el consentimiento del titular, representando un robo de documentación privada (2021). Además, dicha acción delictiva está vigorosamente relacionada con la práctica del fraude informático, ya que los datos sustraídos pueden utilizarse para efectuar estafas, engaños en línea, entre otros crímenes. Por ello, luego de analizar algunos de los tipos de delitos informáticos más frecuentes, podemos postular que cada uno de estos actos ilegales se complementan entre sí y producen un ambiente virtual inseguro y propenso al aumento de la criminalidad cibernética.

1.2. Fraude informático y sus modalidades

El fraude informático, como su mismo nombre postula, consiste en el empleo indebido de tecnología informática con la finalidad de obtener beneficios económicos a través de prácticas ilícitas hacia víctimas de diversas categorías. Por ello, Ponce (2022) menciona que, los fraudes informáticos implican “un montaje o una artimaña ideal [que] libera una acción de astucia, de engaño” mediante la tecnología. Bajo esta perspectiva, el fraude informático puede ser definido como cualquier acto que involucre el uso de herramientas digitales para

engañar o estafar a cierto público, y que generalmente esté guiado por el deseo de sustraer bienes o información de carácter confidencial.

De esta forma, un ciberfraude puede implicar elementos como la creación de páginas web falsas, duplicación de páginas de prestigio, mensajes o correos de texto con contenido fraudulento, robo de datos personales, suplantación de identidad, control de información financiera, entre otros. Es decir, que los infractores suplantan el sitio web de instituciones con el propósito de apropiarse de datos de acceso a las cuentas bancarias (Riega, Huamani y Machuca, 2021).

Cabe resaltar que, ante dicho escenario, este tipo de delito puede repercutir en pérdidas económicas significativas tanto para las personas afectadas como para empresas o instituciones afectadas. Además, es importante destacar que el fraude informático puede presentarse en diversas modalidades; de las cuales, se detallaran a continuación, aquellas que poseen un mayor número de denuncias en el Perú.

En primer lugar, una de las modalidades más frecuentes en territorio peruano, según los reportes de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía, se encuentra el *phishing*[3]. El *phishing* es una técnica de fraude informático que consiste en engañar a las víctimas a través de mensajes de texto o correos digitales, aludiendo ser entidades de reconocimientos, como instituciones financieras, con el fin de obtener información confidencial, como datos financieros o contraseñas (Vinelli, 2021). Además, esta modalidad también se puede apreciar en la clonación de páginas web para atraer a la víctima y hacerle creer que se encuentra navegando en un sitio seguro; para que, así, ingrese su información confidencial sin precaución alguna.

Asimismo, dicho delito se complementa con la variante de fraude informático conocida como "*vishing*"[4], que consiste en la suplantación de alguna entidad mediante llamadas telefónicas con la misma finalidad del phishing. En otros términos, la víctima recibe llamadas en las cuales se le solicita su información confidencial con la justificación de que se necesita ese tipo de datos para alguna urgencia bancaria (Nazario y Villanueva, 2022). Aquel método con carácter ilícito es frecuente y registra cifras notables de víctimas por la falta de información sobre su naturaleza. Por ello, cuando un usuario, que no posee conocimientos tecnológicos

[3] Término en inglés "*phishing*", que significa pescar, y se relaciona con que, mediante este tipo de fraudes, los infractores "pescan" datos de usuarios a través de "anzuelos".
[4] Término que deriva de la unión de *voice* y *phishing* (Nazario y Villanueva, 2022)

en su totalidad, recibe constantemente llamadas fraudulentas, se encuentra más propenso a ser afectado por alguna de estas variantes delictivas.

De igual manera, el fraude informático está fuertemente presente en el ámbito de las transacciones comerciales en línea. Algunos de los casos más relevantes, involucran la creación de páginas falsas que simulan ser negocios de renombre, como podría ser Falabella, Amazon, Mercado Libre, entre otros. Estas páginas falsas son diseñadas con el objetivo de recrear con exactitud cada detalle de la web; y así, estafar a los usuarios y obtener sus datos financieros.

Dicha variante de fraude informático mencionada, se difunde a través de las redes sociales, donde se publican anuncios que exponen ofertas falsas que captan la atención del público por su disminuido costo de los productos, ocasionando que accedan a estos sitios fraudulentos (Pozo, 2021). Por esta razón, las estafas realizadas mediante el supuesto de una venta efectuada con una notable oferta en su valor monetario, en un espacio digital, comprenden de igual modo una modalidad de ciberfraude.

En ese sentido, la sustracción ilegal de datos desemboca, en algunos casos, en la modalidad de "*carding*", que consiste en la utilización de dicha información financiera para realizar compras ilegales de pequeños montos; de manera que, se consiga sustraer la mayor cantidad de dinero sin generar sospechas de alguna ilegalidad a los sistemas internacionales de compras por internet (Ponce, 2022). El "*carding*" es uno de los métodos más frecuentes en lo que respecta al ámbito de los fraudes informáticos.

Es así que, el modo de operar mencionado ha tomado popularidad y representa una ilegalidad con un cierto nivel de dificultad en su persecución; esto debido a que, su práctica involucra el uso de sistemas de lavado de dinero a través de diversos medios de fácil acceso en el espacio digital. Entre los que destacan: monederos digitales, bancos de criptomonedas, tiendas de videojuegos en línea, servicios de *streaming*[5], tiendas de intercambio de artículos o cosméticos digitales de juegos, entre otros.

Por último, el delito de fraude informático, en casos peruanos reportados por la DIVINDAT, se ha visto relacionado con el robo de dispositivos móviles, en especial smartphones. Debido a la gran cantidad de información que poseen los teléfonos adquiridos a través de hurto o robo, estos permiten el desarrollo de diversas modalidades de fraude.

[5] Servicios de *streaming* de entretenimiento digital como Netflix, HBO Max, Disney Plus, entre otros.

Entre las más frecuentes podemos encontrar las variantes de "*SIM swapping*", que consiste en duplicar la tarjeta SIM de un dispositivo robado, para evitar perder los datos por un posible bloqueo y acceder a bancas digitales y sustraer dinero; u otros hurtos como el "*Thief Transfer*", en el que infractores utilizan la tarjeta SIM robada en un smartphone nuevo para obtener información personal y cometer fraudes, según un artículo publicado por El Peruano (2023).

De esta manera, es posible plantear que, en el Perú, existe una correlación entre la delincuencia física y la cibernética; puesto que, la sustracción de bienes materiales de manera ilícita, como celulares o computadoras, permite la realización de ciertos delitos que involucran un ámbito digital. Por esta razón, es pertinente llevar una regulación y persecución adecuada tanto en el rubro de las infracciones físicas como cibernéticas.

1.3. Derecho comparado

Continuando con nuestra conceptualización, es importante comprender el concepto de derecho comparado. Según Ferrante, el derecho comparado es el análisis científico de sistemas legales con el fin de examinar sus semejanzas y disparidades, teniendo en cuenta las diversas repercusiones en la sociedad (2016). Es por ello que, podemos decir que el derecho comparado es entendible como una disciplina que se encarga de analizar y comparar las diferentes formas en las que los diversos sistemas jurídicos alrededor del mundo abordan determinadas cuestiones legislativas.

El Derecho comparado permite determinar contrastes entre diferentes sistemas legales para identificar soluciones similares a problemas jurídicos comunes (Morán, 2002). Esto implica que, en situaciones donde existen conflictos normativos, el derecho comparado puede proporcionar elementos de otros sistemas jurídicos que pueden ser utilizados como aporte para solventar y fortificar las carencias presentes en el país con la problemática.

Sin embargo, es relevante tener en cuenta que el rol del derecho comparado en el ámbito penal posee ciertas limitaciones a diferencia de otras ramas de esta disciplina. El derecho comparado, desde las implicancias del derecho penal, se rige de lineamientos que establecen una interpretación inflexible de las leyes, donde la aplicación directa de dicha regulación es fundamental; es decir, se apoya sustancialmente del principio de ley estricta. El principio de ley estricta, o principio de legalidad, es un concepto considerable en el derecho penal, este establece que no se puede imponer una pena sin que dicha infracción cometida esté concretamente legislada dentro de una ley penal (Orbegoso, 2020).

Es decir, un individuo solo puede ser condenado si sus actos están definidos como delitos dentro de una ley existente del Código Penal. Por lo que, si algo no se encuentra registrado en el Código Penal, no es posible integrar interpretaciones nuevas para completar este vacío o laguna legal, únicamente se puede plantear argumentos sin que estos se desvíen del marco legal. Por ello, el desarrollo de este trabajo de investigación nos permitirá comparar y aportar interpretaciones adecuadas a las leyes establecidas para los delitos informáticos; y, en caso encontrar casos fuera de los límites de la regulación del Código Penal Peruano, plantear si es viable realizar modificaciones.

Capítulo II

2.1. La ineficacia de la regulación de los fraudes informáticos en el Estado Peruano

En la cotidianeidad, se puede apreciar que el Perú se encuentra inmerso en una numerosa cantidad de delitos cometidos a raíz de los elevados índices de inseguridad ciudadana y del constante crecimiento de la delincuencia (Vinelli, 2021). Dicha problemática, al igual que otras que acontecen en la nación, es parte de la realidad social peruana contemporánea; y, como se planteó en el capítulo anterior, este fenómeno también se ha extendido al ámbito digital, dando lugar a los delitos informáticos.

Según los datos proporcionados por la Policía Nacional del Perú y compartidos en una publicación de Infobae (2023), durante el presente año 2023, se han aumentado en un 150% las denuncias por ciberdelitos. Además, la DIVINDAT de la PNP indicó que actualmente se ha registrado la cifra de 2445 casos de ciberdelitos. En ese sentido, se afirma que en el Perú se realizan alrededor de 400 denuncias de estos actos ilícitos de manera mensual. Por esta razón, es de vital importancia analizar el nivel de configuración de las infracciones informáticas en el Estado Peruano y evaluar su ineficacia, haciendo un énfasis en los fraudes informáticos y sus modalidades.

Una de las medidas considerables tomadas por el Estado para combatir el crecimiento de las infracciones informáticas fue la promulgación de la Ley N.º 30096, también conocida como Ley de Delitos Informáticos. Dentro de esta ley, se establecen disposiciones específicas para regularizar las conductas delictivas vinculadas con el uso de dispositivos digitales para cometer transgresiones. Sin embargo, es importante efectuar un análisis de sus antecedentes para comprender las circunstancias bajo las cuales se promulgó esta ley.

En primer lugar, en el año 1991, se incorporó al Código Penal, en el artículo 186, el primer delito informático denominado “hurto telemático”[6], en el cual se sancionaba aquellos actos involucrados con crímenes que afectan el patrimonio mediante la aplicación de “sistemas informáticos o telemáticos” (Vega y Arévalo, 2022). De esta manera, en dicho año se instauró el concepto de este tipo de modalidades delictivas, asociadas principalmente como una variante del hurto agravado.

[6] El término hurto “telemático” y este surge de la combinación de las palabras “telecomunicación” e “informática”. Por ello, alude al empleo de técnicas en informática y telecomunicaciones para obtener información digital para diversos fines.

Posteriormente a ello, con el avance de la tecnología y el tiempo, la idea de la regularización de los delitos informáticos fue desarrollándose y obteniendo fuerza mediante iniciativas legales. Con relación a aquello, Vega y Arévalo mencionan que, entre el periodo de 2011 al 2013, “se presentaron ocho proyectos de ley que trajeron consigo la promulgación de la Ley [N.º 30096]” (2022). De forma cronológica, fueron presentadas diversas propuestas legislativas, consiguiendo una construcción de la tipicidad de estos delitos.

En primera instancia, se postuló el Proyecto de Ley N.º 034-2011, titulado Ley de los Delitos Informáticos; seguido a este, se propuso el Proyecto de Ley N.º 307-2011, nombrado “Ley especial sobre Delitos cometidos con el uso de las tecnologías de la información y las comunicaciones”. Asimismo, se presentó un proyecto de ley (Proyecto de Ley N.º 1136-2011) que modificaba el artículo 207-C del Código Penal, incorporando el delito de robo de identidad virtual y el delito informático agravado (207-D). Además, se publicaron el Proyecto de Ley N.º 1257-2011 y el Proyecto de Ley N.º 2112-2012, que exponían nociones de los delitos de violación del secreto de las comunicaciones y el empleo ilegal del servicio de telecomunicaciones, respectivamente.

Por último, el Proyecto de Ley N.º 2398-2012 que modificaba el artículo 176 del Código Penal con respecto a la transferencia de datos por medios digitales “para ejercer influencia contra un menor para actividades sexuales explícitas o actos de connotación sexual” (Ravines, 2023); y, el Proyecto de Ley N.º 2482-2012, denominada como “Ley que incorpora el artículo 175-A en el Código Penal tipificando el delito de acoso sexual infantil mediante nuevas tecnologías de información y telecomunicaciones”.

En ese sentido, como se expone anteriormente, la implementación de la Ley 30096, sobre Delitos Informáticos, no ha tenido un desarrollo espontáneo, sino que su realización ha sido posible debido a una serie de mociones reguladoras con relación a esta problemática. De ese modo, la incorporación de esta ley fue un proceso continuo que conllevó debates acerca de los conceptos que comprenden los delitos informáticos. Además, la presentación de los proyectos de ley mencionados refleja una situación de preocupación por parte del Estado, en la cual, a raíz del aumento de casos infractores, se buscó regularizar dichos actos en sus distintas categorías (violación a la intimidad virtual, robo de datos informáticos, acoso cibernético, entre otros).

Es así que, según Cornejo, el 22 de octubre del año 2013, se efectuó la promulgación de la Ley N.º 30096 a través de una publicación del Diario Oficial El Peruano, conocida

también como la Ley de Delitos Informáticos, que tenía como objetivo la prevención y sanción de ilegalidades efectuadas mediante sistemas informáticos; y fue planteada para conseguir un control eficaz de los ciberdelitos (2021). Dicha ley, en términos jurídicos, se rige bajo los lineamientos de una ley penal especial; es decir, "se suma a un conjunto de normas penales especiales que tiene [el territorio peruano]" (Vega y Arévalo, 2022). De esta manera, esta normativa posee un cierto nivel de singularidad e individualidad; puesto que, no se encuentra articulada directamente en el Código Penal, sino que funciona como un complemento a este y cumple con el propósito de criminalizar y regular las infracciones ubicadas fuera de la cobertura legal del Código Penal.

Sin embargo, meses posteriores a su promulgación, el cuestionamiento de su nivel legislativo ocasionó algunas reformas dentro de esta ley. Además, desde dicha postulación hasta la actualidad, el Estado Peruano ha realizado un conjunto de cambios y acciones para consolidar la protección ante los crímenes digitales. Como es el caso de la adhesión del Perú en el Convenio sobre Ciberseguridad, mayormente referido como el Convenio de Budapest[7], que sirvió como base para que las leyes penales planteadas en el país conservaran una congruencia internacional y facilitó la cooperación con otras naciones a nivel global (Huamán, 2020).

Por ello, dentro de la Ley N.º 30096 existen normativas que buscan controlar efectivamente las diversas modalidades de los ciberdelitos (Mejía, Hurtado y Grisales, 2023). Así pues, esta ley se estructura de artículos organizados en las siguientes temáticas: delitos contra datos y sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexuales (obtener material pornográfico de un menor a través del internet), delitos informáticos contra la intimidad y el secreto de las comunicaciones, delitos informáticos contra la fe pública (suplantación de identidad) y delitos informáticos contra el patrimonio.

Con respecto a este último punto mencionado, es relevante analizar los parámetros que engloban los crímenes cibernéticos que atentan contra el patrimonio de un ciudadano; con el fin de comprender adecuadamente las capacidades y limitaciones que este artículo

[7] El Convenio de Budapest, es un acuerdo internacional formulado por el Consejo de Europa en 2001, y busca promover la colaboración a nivel internacional en la lucha contra los delitos informáticos. Actualmente dicho convenio cuenta con más de ochenta Estados afiliados; el Perú se incorporó el 13 de febrero de 2019 a través de la Resolución Legislativa N.º 30913 del Congreso de la República (Reyna y Caro, 2022).

posee ante los casos de fraudes informáticos en la realidad social peruana. De igual manera, es preciso detallar su tipificación y evaluar si posee una definición adecuada.

El sector de los crímenes informáticos sobre el patrimonio se sitúa en el quinto capítulo de la Ley de Delitos Informáticos, dentro de este se tipifica únicamente un delito, denominado Fraude Informático (establecido en el artículo 8). Es así que, el artículo 8 de dicha ley condena cualquier aprovechamiento ilegal que se realice a través "[del] diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático" (Artículo 8, Ley N.º 30096).

Por ello, Vega y Arévalo (2022) postulan que, esta normativa se comprende desde una perspectiva de protección ante la sustracción ilícita del patrimonio de un individuo como parte de sus bienes jurídicos mediante el empleo de herramientas tecnológicas. No obstante, la tipicidad de este delito se desvincula, en cierto nivel, con lo instituido por el Convenio de Budapest; puesto que, en este, la definición de fraude informático se formula excluyendo el valor patrimonial que contiene la comisión de estas infracciones.

Esto se debe principalmente a que, como se mencionó con anterioridad, en el año de 1991, en el Perú se instauró el concepto de robo de bienes monetarios por medio de sistemas tecnológicos; es decir, se estableció una regulación legal alrededor de la definición de "hurto telemático". Por lo que, la legislación de fraudes informáticos no proviene directamente de la Ley de Ciberdelitos, sino que es resultado de la presencia de una variante ya existente de dicha infracción en la nación, que fue regulada a través de la infracción de "hurto telemático", denominado como el primer delito informático tipificado en el Código Penal (Puelles, 2014).

Por esta razón, la delimitación que posee esta normativa sobre el fraude informático se desvincula con lo planteado con el Convenio de Budapest y brinda una descripción más asociada a la realización de un acto agravado[8]. Es así que, esta definición entra en debate acerca de su tipificación; debido a que algunos profesionales del tema, como Llaneza o Rovira, mencionan que debería modificarse la denominación de "fraude" y reemplazarlo por "manipulación informática defraudatoria" (citado en Vega y Arévalo, 2022). Sin embargo, otros especialistas señalan que realizar eso es caer en una incongruencia, puesto que el fraude informático no necesita de un engaño para ser efectuado, sino de la participación en el manejo ilícito de datos informáticos.

[8] En el sentido de un delito hacia el patrimonio de cada individuo, efectuado de manera dolosa.

En virtud de ello, es pertinente evaluar el nivel de eficacia que contiene el sector de la ley promulgada correspondiente a los fraudes informáticos; y para esto, se analizará su calidad de tipicidad, los sujetos a los que va destinada y la condena hacia las transgresiones digitales. Para empezar, con respecto a la tipicidad, la conceptualización de dicho fraude requiere, de manera obligatoria, una manipulación de datos informáticos mediante un sistema digital para obtener información o beneficios económicos[9]. Por este motivo, es posible aludir que el artículo 8 de la Ley N.º 30096 alude a un delito de conducta dolosa, debido a que es necesaria la presencia de una intención perjudicial de lucro en cada fase de la infracción (Espinoza, 2022).

Además, este delito presenta una serie de modalidades notablemente extensa; por lo que, su delimitación se centra en aquellas violaciones donde se perjudica a un tercero (creación, alteración, clonación o supresión de datos informáticos). Según lo presentado por Espinoza, el sujeto activo de esta acción ilegal “podría ser cualquier persona con conocimientos básicos de informática” (2022); y, por otro lado, el sujeto pasivo, los ciudadanos sin un entendimiento adecuado de los medios digitales contemporáneos, como personas de la tercera edad o con acceso limitado a dispositivos tecnológicos.

No obstante, a pesar de que esta problemática ha sido trabajada por el Estado desde hace dos décadas, actualmente se sigue cuestionando si la configuración de fraude informático en el Perú es la adecuada; puesto que, el avance de las tecnologías ha permitido el desarrollo de nuevas modalidades de ciberfraude y estas no se encuentran cubiertas en su totalidad por la regulación (Reyna y Caro, 2022).

De esta manera, dicho suceso atenta contra el principio de ley estricta de la legislación; debido a que, al tratarse de una ley penal, esta no puede contener ambigüedad y es necesario que comprenda un marco legal más amplio sobre esta problemática. Por consiguiente, a consecuencia de la delimitación insuficiente de los fraudes informáticos, esta permite el aumento de casos despenalizados en la sociedad a través del existente vacío legal de este tipo de delitos.

[9] Aquella definición la diferencia de un delito de hurto estándar, puesto que no se violenta físicamente al individuo agraviado.

2.2. Las normativas legales contra fraudes informáticos y sus deficiencias en comparación con países de nivel internacional

Continuando el análisis sobre la eficiencia del sistema legislativo con respecto a los delitos informáticos, en particular con los fraudes informáticos, es fundamental evaluar otras regulaciones de países de nivel internacional; para así, realizar una comparativa y determinar si el Perú conserva o no congruencia con las medidas globales adoptadas por otras naciones. En primer lugar, Reyna y Caro postulan que se debe considerar, en este rubro de delitos, que el nivel de desarrollo tecnológico de una nación influye en la capacidad que esta posea para la configuración adecuada de leyes contra el cibercrimen (2022).

Por ello, aquellos países que presentan un nivel mayor de avance tecnológico, evidencian, en la mayoría de casos, una regulación más completa y actualizada en materia informática. De esta manera, habiendo postulado las normativas aplicadas en el Perú para estos actos ilícitos; se efectuará una comparación con las legislaciones de España, México, Reino Unido y Estados Unidos, en vista a fortalecer las estimaciones acerca de los conceptos digitales y formular las posibles discordancias en el marco legal de los crímenes digitales del Perú con dos naciones que se comunican en español y otras dos que emplean un idioma extranjero.

Empezando la comparativa con el país de España, es preciso mencionar que en este la legislación española no contempla un sector en específico dedicado a los delitos informáticos, como en el caso del Estado Peruano. No obstante, dentro del Código Penal Español se detallan algunas normas que tipifican conductas asociadas a ciberdelitos; por lo que, a pesar de no poseer una ley individual como Perú, sí postulan una regulación actualizada para la penalización de los actos delictivos referidos. De esta manera, según Reyna y Caro (2022), la nación española contiene algunos delitos informáticos tipificados en el interior de su Código Penal, entre los que podemos destacar a continuación.

En primer lugar, ubicado en el octavo título del Código Penal, denominado “Delitos contra la libertad sexual”, y en el segundo capítulo[10] de este, se encuentra el artículo 183, que habla acerca de la difusión de pornografía infantil. Seguido a esto, en el primer capítulo del décimo título, llamado “Delitos contra la intimidad, el derecho a la propia imagen y la

[10] Capítulo II, titulado “De las agresiones sexuales a menores de dieciséis años”.

inviolabilidad del domicilio", se ubica el artículo 197, que hace alusión al robo de datos personales.

Es decir, cuando obtienen los datos personales de otro ciudadano sin su consentimiento, con el fin de utilizarlos para suplantar su identidad, cometer fraude o causarle algún otro daño. Es así que, a pesar de no especificarse directamente la participación de cierto medio digital, esta ley contiene un nivel de utilidad para la regulación de delitos informáticos y protección de información. Además, dicho concepto contribuye en la persecución eficaz del robo de información personal en las redes sociales.

Sin embargo, se presenta una peculiaridad en el ámbito de los fraudes informáticos; esto debido a que, en España, se plantean dos conceptos para abordar esta problemática: el fraude informático y la estafa informática[11]. Por un lado, el denominado "fraude informático", se instaura en el artículo 264 del Código Penal y postula que este delito se produce cuando, de manera ilícita, se accede a algún sistema informático y se manipulan los datos dentro de este, principalmente con el objetivo de obtener ganancias económicas.

De esa forma, se define al fraude informático como aquel acto infractor que implica la alteración de información en un sistema digital con fines lucrativos; lo cual denota una diferencia con la normativa peruana, en donde el ciberfraude implica una condición agravante hacia un tercero con conocimientos limitados de informática, aproximándose más a la terminología del Artículo 2 de la Ley Peruana N.º 30096, denominado como "Acceso ilícito". El cual menciona que "será condenado aquel que acceda ilícitamente a un sistema informático vulnerando la seguridad de este" (Artículo 2, Ley N.º 30096).

Por otro lado, el artículo 248 menciona el término de "estafa informática", en el que se describe que dicha infracción sucede cuando, mediante un engaño efectuado con medios digitales, una persona induce a un tercero a efectuar actos en perjuicio suyo. Este concepto supone la regulación de casos donde un individuo se ve afectado patrimonialmente por una estafa realizada a través de la falsificación de datos expuestos para inducir a la equivocación; hecho frecuente en el contexto peruano. En ese sentido, este último artículo se acerca a la definición que el Perú contempla sobre fraude informático; puesto que, como lo mencionaron Vega y Arévalo (2022), este se encuentra mayormente vinculado a la noción de "hurto

[11] Ambos ubicados en el título de "Delitos contra el patrimonio y contra el orden socioeconómico".

telemático" con la excepción de que en el Estado Peruano esta norma no se tipifica la necesidad de un engaño.

En contraste, analizando las normativas en México, es posible aludir que la tipificación de los delitos informáticos se encuentra en una situación relativamente precaria. Aquello en consecuencia de que el concepto de "ciberdelito" no está configurado dentro de la legislación mexicana; puesto que, a pesar de que ciertas infracciones digitales están tipificadas en el Código Penal Federal, no se presentan detalladas en su totalidad (Alcalá y Meléndez, 2023). Es decir, que existen delitos que actualmente no están delimitados en el Código Penal de México y suponen un vacío en el marco legal del país.

Algunos de los delitos tipificados que es posible ubicar como parte de las normas del derecho penal mexicano son los siguientes. En el noveno título del Código Penal Federal, en los capítulos I y II, se tipifican los delitos acerca de la "Revelación de Secretos"[12] y el "Acceso Ilícito a Sistemas y Equipos de Informática"[13]. Como se puede evaluar, esta última ley se asemeja a la definición que España plantea sobre fraude informático. Por ello, comparándolo con la situación legislativa de Perú, la nación andina demuestra, en cierto nivel, un trabajo más eficaz en lo que respecta a tipicidad de delitos informáticos. Debido a que, a excepción de algunas leyes especiales que abarcan ciertos casos, en México no se ha formulado de manera clara la terminología de esta temática.

Además, Alcalá y Meléndez (2023) sugieren que, esto se refleja en el hecho de que país de México no posee ninguna institución dedicada a la prevención de cibercrímenes y reporta una tasa elevada de casos infractores; lo que representa una incongruencia en su sistema regulatorio, y esta idea se refuerza teniendo en cuenta que México es una de las naciones adscritas en el Convenio de Budapest. Por esta razón, en vista comparativa con el Perú, el delito informático y su terminología se encuentran tipificados con mayor eficacia en el territorio andino.

Seguidamente, según lo postulado por Pupillo (2018), en Reino Unido la tipificación de los delitos informáticos se rige por la *Cybersecurity Act*[14] planteada en 2016, basada en la *Computer Misuse Act* (Ley de Abusos Informáticos) de 1990. Es así que, se alude que en dicha nación los conceptos de crímenes asociados a los sistemas digitales poseen una

[12] Artículo 210 - 211 *bis*.
[13] Artículo 211 *bis* 1 - Artículo 211 *bis* 7.
[14] Ley de Seguridad Cibernética, en español

notable diferencia a los países hispanohablantes por la longevidad de sus normativas. Dentro de esta ley, se detalla las reformas aplicadas por la implicación del Reino Unido en la Agencia de la Unión Europea por la Ciberseguridad (ENISA en sus siglas en inglés), aquello representa que su normativa se ha encontrado en un constante cambio para adaptarse al surgimiento de nuevas modalidades delictivas.

Con respecto al tema de fraude informático, Reino Unido tipifica este delito como el acceso desautorizado (*Unauthorised Access*) a un sistema informático (Pupillo, 2018); es decir, que dicha delimitación guarda semejanza con el concepto de ciberfraude en España, y se distancia de la configuración de fraude informático en Perú, acercándose al Artículo 2 de la Ley Peruana de Delitos Informáticos. Por ello, la definición que se emplea en Reino Unido y en España plantea una suerte de acceso ilícito efectuado a través de medios digitales sin consentimiento.

Por último, en Estados Unidos, a diferencia de Reino Unido, la configuración de delitos informáticos se remonta al año 1986 con la *Computer Fraud and Abuse Act*[15] (Ley de Fraude y Abuso Informático), lo que simboliza que el país estadounidense posee una mayor preocupación por la regulación eficaz de ciberdelitos. En esta ley se regulan todos aquellos delitos que impliquen algún daño efectuado mediante herramientas digitales (Albert y Grimmelmann, 2023). De esta manera, la CFAA comprende infracciones como: acceso no autorizado a un sistema informático[16] (concepto similar al fraude informático español), modificación de datos informáticos, difusión de información confidencial, fraude informático, entre otros.

En relación con la temática de fraude informático, Albert y Grimmelmann aluden que, Estados Unidos comprende este delito como cualquier acto que se realice mediado por un sistema cibernético y se efectúe con el propósito de obtener un lucro económico (2023). En ese sentido, desde una vista comparativa, la definición que establece Estados Unidos de fraude informático es similar a la determinada en el Estado Peruano. Es decir, que las naciones mencionadas tipifican el fraude informático con cierto nivel de semejanza, debido a que, en ambos países se delimita este delito como una infracción contra el patrimonio.

Sin embargo, por factores como un mejor desarrollo de los procesos judiciales, se refleja que Estados Unidos aplica y penaliza con mayor eficacia esta normativa que Perú; lo

[15] CFAA por sus siglas en inglés.
[16] Semejante a la definición del Artículo 2 de la Ley N.° 300096 en Perú.

cual puede simbolizar que la nación americana posee una tipicidad coherente de manera superior en este rubro, a diferencia del Artículo 8 de la Ley N.º 30096 de Perú. Además, Estados Unidos dispone de instituciones más capacitadas para fomentar la ciberseguridad, como la Oficina Federal de Investigaciones (FBI) o el Departamento de Justicia de los Estados Unidos (DOJ).

De esta manera, después de realizar un análisis acerca de las diferentes legislaciones internacionales con relación a la regulación de los fraudes informáticos, es posible postular lo siguiente. El Estado Peruano, a pesar de poseer una delimitación aparentemente óptima para el control de los delitos informáticos, a diferencia del país de México; cuando su legislación es comparada con naciones como España o Estados Unidos, se denota que aún se encuentran presentes una serie de carencias en lo que respecta a la tipificación y aplicación de estas normativas.

En el rubro de los fraudes informáticos, esta deficiencia se percibe debido al constante debate que existe entre los diversos países acerca del concepto y límites que este delito tiene. Por ello, es plausible mencionar que el Perú debe adoptar medidas como las efectuadas en España, Estados Unidos y Reino Unido, donde se ha conseguido hacer una distinción eficaz entre “fraude informático” y “estafa informática”; lo cual ha representado un aporte para la penalización y persecución adecuada de estas infracciones. Además, dicha tipificación acertada debe ser reforzada por la compañía de instituciones dedicadas a los delitos informáticos que permitan la correcta investigación y la colaboración transnacional.

Conclusiones

1. Los delitos informáticos se comprenden como cualquier actividad ilícita que implique el uso de un sistema digital para la ejecución de este. En ese sentido, la dependencia de los dispositivos electrónicos fomenta el aumento de criminalidad informática. Asimismo, la aparición de nuevas modalidades de delitos informáticos se vincula con el avance tecnológico; puesto que, si estas ilegalidades se llevan a cabo en un ciberespacio que constantemente está evolucionando, los delitos se modificarán también para adaptarse a estos cambios continuos.

2. Los datos personales y los datos informáticos están fuertemente relacionados en el ámbito de los delitos informáticos, debido a que ambos representan información confidencial de un ciudadano y su extracción indebida posee una implicación legal. Por lo que, una infracción digital que conlleva la sustracción de datos informáticos sin autorización puede simbolizar el mismo grado de consecuencia que un robo de datos personales.

3. El fraude informático se entiende como la utilización indebida de herramientas tecnológicas para obtener bienes económicos mediante un engaño. En ese sentido, el fraude informático requiere de un montaje o entornos falsos que susciten a la víctima al error. De modo que, este tipo de fraude necesita sustancialmente de un engaño para efectuarse.

4. El derecho comparado en el ámbito penal se rige por el principio de ley estricta o principio de legalidad, este establece que no se puede dictaminar una pena si el delito cometido no se encuentra tipificado en alguna ley penal. Además, dicho principio postula que una normativa penal contiene una interpretación inflexible, no debe poseer ambigüedad. Por lo tanto, una ley de este sector tiene la obligación de disponer de una tipificación adecuada que abarque las principales conductas delictivas de la infracción referida.

5. En cuanto al nivel de regulación del fraude informático en el Perú, es posible definir que la tipificación y delimitación es insuficiente; puesto que, a pesar de tener como antecedente el “hurto telemático” en la legislación peruana, esta establece el fraude informático como una extracción ilícita del patrimonio excluyendo la necesidad de un engaño. Aquello simboliza una problemática, debido a que, si dicha ley se rige por el principio de legalidad, plantea una incongruencia al omitir el engaño como requisito

para la regulación de esta infracción, ya que la mayoría de fraudes de esta modalidad se efectúan a través de manipulación de datos informáticos que suscitan a sus víctimas al error. De esta manera, la legislativa peruana evidencia un vacío legal que produce situaciones donde casos delictivos quedan en impunidad debido a las carencias que la ley actual contiene.

6. En el ámbito del fraude informático, existe un debate entre diversos países y legislaciones; esto debido a que, en algunas naciones, como Reino Unido y Estados Unidos, el fraude informático se considera aquella acción que implica el uso de sistemas informáticos para la sustracción no autorizada de información. Sin embargo, en otros países, este concepto se vincula con la extracción ilícita de patrimonio mediante herramientas digitales, la cual requiere, de manera sustancial, un engaño para inducir al agraviado a la equivocación; así como se plantea la denominación de ciberestafa aplicada en el Código Penal Español.

   Es así que, en la mayoría de naciones analizadas, estos hacen una distinción entre “fraude informático” y “estafa informática”, postulando el acceso no autorizado a sistemas digitales y la sustracción de patrimonio a través de engaños, respectivamente. Por ello, en Perú, a pesar de presentar esta misma distinción en el Artículo 2 (Acceso ilícito) y el Artículo 8 (Fraude informático) de la Ley de Delitos Informáticos, ambos conceptos requieren de una mejor tipificación.

7. Después de haber concluido con la investigación, es posible postular que la hipótesis planteada inicialmente es verdadera, el Perú posee una legislación deficiente en materia de delitos informáticos. Aquello debido a que, con el constante aumento de casos de esta índole, a causa de la aparición de nuevas tecnologías para efectuar crímenes digitales, la normativa peruana de ciberdelitos (Ley N.º 30096) establece parámetros que no son eficaces regular las nuevas modalidades emergentes, tanto a nivel de prevención en los ciudadanos, como en la persecución y sanción de los delitos.

   Por ello, en vista a comparativas aplicadas con otras legislaciones nacionales a nivel mundial, el Estado Peruano debe realizar ciertas reformas en dicha ley, en especial en el sector de fraude informático analizado en el presente trabajo. Además, debe efectuar una mayor inversión en este rubro para implementar mejoras en las instituciones encargadas de la persecución de estos actos ilícitos y facilitar la jurisprudencia transnacional para así obtener un control delictivo más eficaz.

Bibliografía

AGUSTINA, José

2021 "Nuevos retos dogmáticos ante la cibercriminalidad". *Estudios Penales y Criminológicos*. Barcelona, volumen 41, pp. 705-777. Consulta: 28 de agosto de 2023.

https://revistas.usc.gal/index.php/epc/article/view/7433

ALBERT, Kendra y James GRIMMELMANN

2023 "Do the Right Thing: Exploring the intersection of legal compliance and ethical judgment". *Communications of the ACM*. New York, volumen 5, pp. 18-20. Consulta: 25 de octubre de 2023.

https://openurlebscocom.ezproxybib.pucp.edu.pe/c/d6owsy/openurl?sid=ebsco:plink&id=ebsco:iih:163324662

ALCALÁ, Miryam y Miguel MELÉNDEZ

2023 "Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas". *PAAKAT: Revista de Tecnología y Sociedad*. Guadalaja, volumen 13, número 24. Consulta: 30 de octubre de 2023.

https://www.scielo.org.mx/scielo.php?pid=S2007-36072023000100005&script=sci_arttext

CABEZA, Yuriko

2023 Denuncias por ciberdelincuencia se incrementan en un 150% en el 2023: mayoría son por fraude. *Diario Digital Infobae*. Consulta: 1 de noviembre de 2023.

https://www.infobae.com/peru/2023/09/09/denuncias-por-ciberdelincuencia-se-incrementan-en-un-150-en-el-2023-mayoria-son-por-fraude/

CONGRESO DE LA REPÚBLICA

2013 *Ley N.° 30096*. Ley de Delitos Informáticos. Lima, 22 de octubre. Consulta: 25 de octubre de 2023.

https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

CORNEJO, Jesús

2021 "Criminalidad Informática y la Discusión Sobre el Bien Jurídico Protegido en los Delitos Informáticos". En MEINI, Iván y Yvan MONTOYA (coordinadores). *Libro Homenaje en memoria del profesor doctor Felipe Villavicencio Terreros.* Lima: Centro de Investigación, Capacitación y Asesoría Jurídica del Departamento Académico de Derecho de la Pontificia Universidad Católica del Perú, pp. 93-102. Consulta: 28 de agosto de 2023.

https://repositorio.pucp.edu.pe/index/handle/123456789/182684

D'AVILA, Fabio y Daniel LEONHARDT

2016 "Derecho Penal y ciberdelitos. Breves aproximaciones dogmáticas". *Revista de Pensamiento Penal.* Porto Alegre. Consulta: 15 de octubre de 2023.

https://repositorio.pucrs.br/dspace/handle/10923/11271

DIARIO OFICIAL DEL ESTADO PERUANO

2023 "¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú". *Diario El Peruano.* Consulta: 10 de octubre de 2023.

https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

ESPINOZA, Victor

2022 *Delitos informáticos y nuevas modalidades delictivas.* Primera edición. Lima: Pacífico Editores SAC.

FERRANTE, Alfredo

2016 "Entre derecho comparado y derecho extranjero. Una aproximación a la comparación jurídica". *Revista Chilena de Derecho.* Santiago de Chile, volumen 43, número 2. Consulta: 15 de octubre de 2023.

https://dx.doi.org/10.4067/S0718-34372016000200010

HUAMÁN, Marleny

2020 Los delitos informáticos en Perú y la suscripción del convenio de Budapest. Tesis para optar al título profesional de abogada. Cusco: Universidad Andina del Cusco, Facultad de Derecho y Ciencias Políticas. Consulta: 2 de septiembre de 2023.

https://repositorio.uandina.edu.pe/handle/20.500.12557/4116

MEJÍA, Mauricio, Sandra HURTADO y Andrés GRISALES

2023 "Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones". *Revista de Ciencias Sociales*. Maracaibo, volumen 29, número 2, pp. 356-372. Consulta: 29 de agosto de 2023.

https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

MINISTERIO DE JUSTICIA DEL GOBIERNO DE ESPAÑA

1995 *Código Penal de España.* Boletín Oficial del Estado, número 281. Consulta: 25 de octubre de 2023.

https://www.boe.es/biblioteca_juridica/codigos/abrir_pdf.php?fich=038_Codigo_Penal_y_legislacion_complementaria.pdf

MORÁN, Gloria

2002 "El derecho comparado como disciplina jurídica: la importancia de la investigación y la docencia del Derecho Comparado y la utilidad del método comparado en el ámbito jurídico". *Anuario da Facultade de Dereito da Universidade da Coruña*. La Coruña, número 6, pp. 501-529. Consulta: 10 de octubre de 2023.

https://ruc.udc.es/dspace/handle/2183/2179

NAZARIO, Nora y Lucía VILLANUEVA

2022 *Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal*. Tesis para optar el título profesional de abogado. Pimentel: Universidad Señor de Sipán. Escuela Profesional de Derecho. Consulta: 2 de septiembre de 2023.

https://repositorio.uss.edu.pe/handle/20.500.12802/10002

ORBEGOSO, Miluska

2020 "El Principio de Legalidad: Una aproximación desde el Estado Social de Derecho". *IUS ET VERITAS*. Lima, número 60, pp. 198-209. Consulta: 10 de octubre de 2023.

https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/22722

PONCE, Juan

2022 *La clonación de tarjetas de créditos y débitos, su implicancia como delito informático en el Perú*. Tesina para optar el título profesional de abogado. Lima: Universidad Peruana de las Américas, Escuela Profesional de Derecho. Consulta: 2 de septiembre de 2023.

http://repositorio.ulasamericas.edu.pe/handle/upa/2715

POZO, Francisco

2021 *Nuevos Delitos Informáticos por impulso de la Transformación Digital por causa del Covid-19 en el Perú.* Tesina para optar el título profesional de abogado. Lima: Universidad Peruana de las Américas, Escuela Profesional de Derecho. Consulta: 15 de octubre de 2023.

http://190.119.244.198/handle/upa/2716

PUELLES, Ricardo

2014 ”Luces y sombras en la lucha contra la delincuencia informática en el Perú”. Revista Hiperderecho. Lima. Consulta: 2 de noviembre de 2023.

https://hiperderecho.org/wp-content/uploads/2014/07/01_delitos_informaticos_elias.pdf

PUPILLO, Lorenzo

2018 “EU Cybersecurity and the Paradox of Progress”. *CEPS Policy Insight*. Roma, número 6. Consulta: 1 de noviembre de 2023.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131559

RAVINES, Yosselym

2023 *Fundamentos jurídicos para incorporar el phishing como agravante en el artículo 11° de la Ley N° 30096-Ley de delitos informáticos en el Perú*. Tesis para optar al título profesional de abogada. Cajamarca: Universidad Privada del Norte, Facultad de Derecho y Ciencias Políticas. Consulta: 2 de noviembre de 2023.

https://repositorio.upn.edu.pe/handle/11537/34436

REYNA, Luis y Dino CARO

2022 *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*. Primera edición. Estado de México: Derecho Global Editores.

RIEGA, Yasmina, Hubert HUAMANI y Jorge MACHUCA

2021 “Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú”. *Lex: Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas*. Lima, volumen 19, número 28, pp. 197-236. Consulta: 28 de agosto de 2023.

https://dialnet.unirioja.es/servlet/articulo?codigo=8255000

RUÍZ, Andrea, Roser BONO-CABRÉ y Ernesto MAGALLÓN

2019 "Ciberacoso y ansiedad social en adolescentes una revisión sistemática". *Revista de Psicología Clínica con Niños y Adolescentes.* Barcelona, volumen 6, número 1, pp. 9-15. Consulta: 15 de octubre de 2023.

https://dialnet.unirioja.es/servlet/articulo?codigo=6749051

SECRETARÍA DE GOBERNACIÓN

1931 *Código Penal Federal de México*. Diario Oficial de la Federación. Consulta: 25 de octubre de 2023.

https://mexico.justia.com/federales/codigos/codigo-penal-federal/

VEGA, Jorge y Maguín ARÉVALO

2022 *Ciberdelitos: Análisis en el Sistema Penal*. Primera edición. Lima: Editorial Iustitia.

VINELLI, Renzo

2021 "Los delitos informáticos y su relación con la criminalidad económica". *Ius Et Praxis*. Lima, número 53, pp. 95-110. Consulta: 29 de agosto de 2023.

https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995