UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TESIS

FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL

PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

Autores:

Bach. Nazario Delgado Nora Ysabel
https://orcid.org/**0000-0001-5549-5731**

Bach. Villanueva Sanchez Lucia Victoria
https://orcid.org/**0000-0003-4247-3298**

Asesor:

Dr. Idrogo Pérez Jorge Luis

https://orcid.org/0000-0002-3662-3328

Línea de Investigación:

Ciencias Jurídicas

Pimentel – Perú

2022

Aprobación de jurado:

Mg. Cueva Ruesta Wilmer César Enrique
Presidente del jurado de tesis

Mg. Ruesta Bregante Irma Marcela
Secretaria del jurado de tesis

Mg. Delgado Fernández Rosa Elizabeth
Vocal del jurado de tesis

Dedicatoria

La presente tesis está dedicada a ti padre Jehová porque está es tu voluntad. A mis padres Nora Delgado y José Nazario porque gracias a ustedes pude lograrlo y sé que se sienten orgullosos de mí así como yo lo estoy de ustedes. A mis hijas A&K y a ti mi Myra por haberme inspirado a ser una mejor persona y profesional.

A mis dos hermanos quiero decirles que lo estamos logrando.

La presente tesis va dedicada con los mejores sentimientos de mí ser a mis padres Manuel y Santos Villanueva Sánchez, pues han sido el soporte ideal para lograr el objetivo Profesional.

A mi hijo Santiago Manuel H. Villanueva, pues desde que llegó a mi vida se ha convertido en el pilar fundamental para lograr todo lo propuesto en mi plan de vida, con el fin de ser el mejor ejemplo para él.

Agradecimiento

Agradecemos infinitamente a Dios por tanto amor y bendición, esta meta es su voluntad.

Agradecemos a nuestros padres, hijos, familia y amigos por haber sido parte de este proceso muy importante para nosotras, a nuestros excelentes docentes de nuestra honrosa Universidad Señor de Sípan en especial la Facultad de Derecho.

Mil gracias.

Resumen

La presente investigación establece como problema principal fraude informático en la modalidad de phishing y la necesaria actualización de la legislación peruana, es por ello que establece como objetivo general si que al aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad de phishing, teniendo en cuenta que se desarrolló con una metodología de tipo mixta desde un enfoque cuantitativo y cualitativa, estableciendo una población conformada por los operadores del Derecho, llámense Abogados especialistas en el derecho penal, jueces y fiscales de la Ciudad de Chiclayo, permitiendo concluir que de acuerdo a la actualización realizada a la legislación que regula los delitos informáticos se logró obtener una eficiente persecución y sanción penal frente al delito de fraude informático en modalidad de phishing, ya que es evidente que los actos realizados por el fraude informático quedaban impune, por el tan solo hecho de no encontrar a las personas que realizan estos actos que perjudican directamente a la sociedad, dejando así una brecha para que otra personas que tengan conocimiento electrónicos puedan cometer estos actos ilícitos sin que puedan ser sancionados adecuadamente.

Palabras Clave: Delito de Phishing, Fraude informático, Sanción penal

Abstract

The present investigation establishes as the main problem computer fraud in the form of phishing and the necessary update of Peruvian legislation, that is why it establishes as a general objective if that when applying an update of the legislation for an efficient prosecution and criminal sanction of the crime of computer fraud in the form of phishing, taking into account that it was developed with a mixed type methodology from a quantitative and qualitative approach, establishing a population made up of law operators, call themselves lawyers specialized in criminal law, judges and prosecutors of the City of Chiclayo, allowing to conclude that according to the update made to the legislation that regulates computer crimes, it was possible to obtain an efficient prosecution and criminal sanction against the crime of computer fraud in the form of phishing, since it is evident that the acts carried out by computer fraud went unpunished, for the so so the fact of not finding the people who carry out these acts that directly harm society, thus leaving a gap for other people who have electronic knowledge to commit these illegal acts without being able to be adequately sanctioned

Keywoord: Phishing crime, Computer fraud, Criminal sanction

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

I. INTRODUCCION

En el mundo el avance de la tecnología ha generado de que los robots, la inteligencia artificial y el aprendizaje de las maquinas evolucionen a un paso veloz, dejando mucho de las posibilidades en tela de juicio ante un modelo tradicional, pues todas estas medidas avanzadas facilitan la vida de la persona y mejorar sus relaciones personales y laborales, sin embargo se puede percatar que este avance ha traído consigo varios problemas que afectan a la sociedad principalmente ante su privacidad, debido a que se han generado diversos robos informáticos que han perjudicado la integridad personal, más aún cuanto este tipo de delitos no se encuentra tipificado o actualizado en la norma.

En este contexto, se centra aquí en los aspectos específicos del fraude informático, pues estos incluyen ataques a la integridad y confidencialidad de los datos personales, así como a los activos bancarios y la confianza del titular y la seguridad del sistema financiero para realizar todo tipo de transacciones civiles y comerciales.

La norma anterior fue modificada de acuerdo con la Ley 30171, publicada en 2014, que prohíbe el acceso no autorizado (artículo 2), los ataques a la integridad de los datos y sistemas informáticos (artículos 3 y 4) y la incautación de datos informáticos (artículo 7), incluido el fraude (artículo 8) y el abuso de los mecanismos y dispositivos informáticos (artículo 10) afirman las palabras “a sabiendas e ilícitamente” que los delitos se han cometido indebidamente y se ha derogado el artículo 6, que se refiere al movimiento ilegal de información.

Frente a esta normativa el artículo en análisis es el 8 considerado como fraude información, pues a través de esta modalidad, se han presentado diversos medios de robo de información, uno de ellos es el phishing, considerado como un modelo de engaño que se genera con la finalidad de poder robar información bancaria para poder atentar contra el patrimonio de la persona, para ello se presentan diversas paginas falsas, las cuales se presentan en los bancos o en las entidades financieras.

Es así que, ante las restricciones, en la actualidad, la Ley de №. 30096, “Ley de Delitos Informáticos” es de particular importancia, un estándar específico de traición penal que se aplica a los sistemas informáticos y de información, la indemnización y la libertad sexual, la confidencialidad y el secreto de la comunicación, el patrimonio y las creencias públicas en las que se utilizó la Tecnología Criminal, ante la comisión de los diversos delitos penales.

E aquí el problema de información en donde se evidencia que dentro del fraude informático no existe una distinción penal entre la modalidad de fraude y la modalidad de phishing, pues este estos casos la modalidad debería ser distinta por el hecho de que debería haber mejor persecución penal y la sanción debería ser mayor que el de la pena interpuesta.

Ante esta situación, el Ministerio de Asuntos Públicos se ha propuesto desarrollar un estudio descriptivo reconociendo las fortalezas y debilidades del Estado en el abordaje de estos desafíos de política pública, con datos policiales y tributarios, tanto cualitativos como cuantitativos. Como aporte teórico y normativo, los lineamientos y recomendaciones de la Convención de Budapest, suscrita por el gobierno peruano en 2019, y las definiciones y disposiciones de la Ley de Delitos Informáticos (Ley N ° 30096), que se encuentran vigentes desde 2013, fueron tenido en cuenta.

Finalmente se comprende que la mayor en la que se presenta el delito es a través de mensajes de textos los cuales son publicados por medio de las redes sociales, pues se comprende que este tipo de delitos roba la información necesaria y bancaria de la víctima, es así que se comprende que de todas las denuncias presentadas por los delitos informáticos de la Divindat la mayor parte se genera por el fraude informático.

1.1. Realidad problemática

1.1.1. Internacional

En el mundo el avance de la tecnología a generado de que los robots, la inteligencia artificial y el aprendizaje de las maquinas evolucionen a un paso veloz, dejando mucho de las posibilidades en tela de juicio ante un modelo tradicional, pues todas estas medidas avanzadas facilitan la vida de la persona y mejorar sus relaciones personales y laborales, sin embargo se puede percatar que este avance ha traído consigo varios problemas que afectan a la sociedad principalmente ante su privacidad, debido a que se han generado diversos robos informáticos que han perjudicado la integridad personal, más aun cuanto este tipo de delitos no se encuentra tipificado o actualizado en la norma (Darrell, 2016).

Pues en la sociedad la información actual, el llamado "delito cibernético" se produce en la vida cotidiana humana en muchas formas, lo que representa una amplia heterogeneidad de nuevos fenómenos delictivos y formas renovadas de delitos tradicionales, especialmente a través de sistemas informáticos o redes de transmisión e intercambio de datos a través de Internet, que su complejidad práctica dificulta la persecución y, por lo tanto, aumenta el nivel de gravedad.

En este contexto, se centra aquí en los aspectos específicos del fraude informático, pues estos incluyen ataques a la integridad y confidencialidad de los datos personales, así como a los activos bancarios y la confianza del titular y la seguridad del sistema financiero para realizar todo tipo de transacciones civiles y comerciales.

Es así que el crimen informático llega a través de complicidad interna de manera personal, perjudicando la vulnerabilidad de la información de la organización, así mismo se estable que en la mayoría de casos los delitos cibernéticos son mayormente presentados a través del robo informático, pues esta modalidad adquiere de que, de la víctima se tome en cuenta datos personales, cuentas bancarias y claves secretas.

Ahora respecto al robo informático, se considera que esta nueva modalidad es llamada como phishing, pues en países como México, conforme lo menciona Solís (2020), esta figura antijuridica se genera a través del robo de información bancaria, en donde se actúa con un modus operandi parecido al del robo digital, pues se observa que este problema en México ha generado que se reporten en el 2020 un promedio de 715%, ante ello la autora menciona que el país va por buen camino con respecto a la legalización del delito, sin embargo se puede percatar que en estos casos se evidencia que aún se siguen generando nuevos delitos, los cuales muchos de ellos no están regularizados.

Cosa similar sucede en España, en donde comprende que en los últimos meses a ocurrido una estafa informática, que en sus mayoría de casos a sido perjudicable para las empresas, pues se comprende que la cibercriminalidad aumento en un 40% durante los últimos años, esto se debe al avance de la tecnología, el comercio electrónico y los nuevos medio de comunicación y trabajo, ante ello el Estado requiere y propone que se ejecuten mejor seguridad jurídica cibernética ante la protección personal e integra de la persona (Efe, 2021).

Esto también ocurre en Chile, en donde la mayor parte del fraude informático ocurre a través de los bancos, pues en la actualidad se presenta un modelo de estafa que el código penal analiza como una figura especial perteneciente a los delitos información, sin embargo frente a las nuevas modalidades como es el caso del fishing esta no se presenta debido a que la ley en su totalidad no se actualiza frente a los nuevos delitos presentados, es por ello que se recomienda tomar en cuenta el principio de adecuación penal, para que los magistrados al aplicar la norma, está la adecuen de acuerdo al delito cometido (Oxman, 2013).

Así mismo se comprende que este delito en su mayor parte actuado como un robo de datos a través de páginas web que no son seguras, pues en Colombia esta modalidad informática delictiva según Admin (2021), a sido de gran importancia para el propio Estado ya que requieren prevenirlo a través de la ejecución de denuncias, sin embargo se comprende que entre el 2016 y el

2017 se han presentado un promedio de 31.428 denuncias, de las cuales, muchas de ellas han sido actuadas para el robo de información sistema, lo cual a ejecutado que se implementen nuevos medio regulatorios para la protección económica y jurídica de la persona.

Frente a los países analizados, se evidencia que a nivel internacional las modalidades delictivas con el paso del tiempo, más aun con el avance de la tecnología han ido evolucionando y generando muchas de ellas beneficios para la sociedad, pero otras perjuicio, como es el caso del robo informático, es así que se tiene que estas nuevas modalidades delictivas presentadas ante la mayoría de países considerada como phishing , dificulta la protección constitucional y legal que tiene que tener toda persona en base a su información y a su integridad.

Pues de acuerdo al análisis se evidencia que en la mayoría de países se logra visualizar el avance del delito de fraude informático, mayormente en modalidad de phishing y sin embargo hay aun países, que no tienen una legalización actualidad, ni mucho menos una pena prescrita ante estos tipos de casos, pues lo que se si analiza es que en la mayoría se requiere mejorar la protección jurídica y sancionar penalmente el delito.

Ante esta medida se comprende que no solo cada Estado requiere interponer mejor seguridad jurídica, sino también la Interpol quien ha evidenciado que en el 2020 a partir de la repercusión del covid-19 la ciberdelincuencia ha sido objeto sustancia pena de cada país, más aún para las pequeñas empresas, pues se evidencia que durante el trascurso del año se han detectado un promedio de 907000 correos, los cuales son ilegales y presentados de manera maliciosa (Interpol, 2020).

Es así que se requiere que todo tipo de Estado genere mejor precaución empresarial y ciudadana en donde se actúa bajo un modus operandi de resección económica y de panorama empresarial, accediendo a que dentro de las nuevas oportunidades se genere una mejor comisión del delito y se instruya a los magistrados a delimitar la red y los ciberataques.

1.1.2. Nacional

A nivel local dentro del territorio peruano se evidencia que con el trascurso del tiempo las modalidades delictivas de robo cibernético, han ido aumentando día a día, pues como bien se analiza no hay una norma especifique todos los tipos existentes de robo informática, es así que en el 2013 el Estado requiere que se interpongan nuevas medias frente a los alcances de delitos cibernéticos, pues se creó la Ley 30096, Ley de delitos informático, la cual tiene como fin llegar a prevenir y sancionar todo tipo de conductas que logren afectar los sistemas y datos informáticos a través de la relevancia penal, llegando a garantizar la lucha eficaz contra la ciberdelincuencia.

La norma anterior fue modificada de acuerdo con la Ley 30171, publicada en 2014, que prohíbe el acceso no autorizado (artículo 2), los ataques a la integridad de los datos y sistemas informáticos (artículos 3 y 4) y la incautación de datos informáticos (artículo 7), incluido el fraude (artículo 8) y el abuso de los mecanismos y dispositivos informáticos (artículo 10) afirman las palabras “a sabiendas e ilícitamente” que los delitos se han cometido indebidamente y se ha derogado el artículo 6, que se refiere al movimiento ilegal de información (Zevallos, 2020).

Frente a esta normativa el artículo en análisis es el 8 considerado como fraude información, pues a través de esta modalidad, se han presentado diversos medios de robo de información, uno de ellos es el phishing, considerado como un modelo de engaño que se genera con la finalidad de poder robar información bancaria para poder atentar contra el patrimonio de la persona, para ello se presentan diversas paginas falsas, las cuales se presentan en los bancos o en las entidades financieras.

Muchas de estas modalidad son ejecutas por medio de organizaciones criminales, las cuales se encargan de manera colectiva presentar un enlace fraudulencia en donde se le solicita a la persona la actualización de sus datos, con el fin de robo de información, es así que se llega a evidencia que este tipo de robo a aumentado más cuanto se ha presentado las restricciones de la pandemia Covid- 19, pues se comprende que en el año 2021 se presentaron

un promedio de 1188 casos de delitos informáticos, los cuales está relacionado principalmente en el fraude informático (Gestión, 2021).

Es así que, ante las restricciones, en la actualidad, la Ley de №. 30096, “Ley de Delitos Informáticos” es de particular importancia, un estándar específico de traición penal que se aplica a los sistemas informáticos y de información, la indemnización y la libertad sexual, la confidencialidad y el secreto de la comunicación, el patrimonio y las creencias públicas en las que se utilizó la Tecnología Criminal, ante la comisión de los diversos delitos penales.

Por tal motivo, en el Perú a partir del 2021 la División de Investigación de Delitos de Alta Tecnología (Divindat), analiza y ve los casos más frecuentes que se encuentran relacionados con el fraude informático y la suplantación de la identidad, pues conforme lo mencionado por el coronel PNP Erick Ángeles, jefe de la Divindat, se comprendió que cada mes se presentan 300 denuncias de ciberdelitos, muchas de ellas conllevando al fraude informático, clonación de tarjetas y trasferencias no autorizadas, es así que se logra establecer que la modalidad más frecuente presentada es la de phishing, sin embargo se comprende que ante este tipo de delito cibernético, aun la norma no se llega agenciar en su totalidad de persecución penal, pues se evidencia que dentro del territorio peruano la ley no contempla en su totalidad una persecución penal y una sanción que vaya de acuerdo al delito (El peruano, 2021).

E aquí el problema de información en donde se evidencia que dentro del fraude informático no existe una distinción penal entre la modalidad de fraude y la modalidad de phishing, pues este estos casos la modalidad debería ser distinta por el hecho de que debería haber mejor persecución penal y la sanción debería ser mayor que el de la pena interpuesta.

Así mismo se comprende que ante este problema la ley requiere de una nueva actualización en donde se evidencia las nuevas modalidades y los nuevos medios de pruebas que se actúan para poder encontrar el sujeto ilícito o la organización criminal que repercuta ante la sanción penal.

1.1.3. Local

En nuestro país, las cifras del Ministerio de Fomento muestran que el número de denuncias por delitos informáticos aumenta rápidamente de año en año. De octubre de 2013 a julio de 2020, en donde se registraron 21.687 denuncias en las fiscalías penal y mixta, de las cuales el 40% provino de 2019. Sin embargo, durante el mismo período, se presentaron el 58% de ellas y solo se presentaron 108 sentencias.

Ante esta situación, el Ministerio de Asuntos Públicos se ha propuesto desarrollar un estudio descriptivo reconociendo las fortalezas y debilidades del Estado en el abordaje de estos desafíos de política pública, con datos policiales y tributarios, tanto cualitativos como cuantitativos. Como aporte teórico y normativo, los lineamientos y recomendaciones de la Convención de Budapest, suscrita por el gobierno peruano en 2019, y las definiciones y disposiciones de la Ley de Delitos Informáticos (Ley N ° 30096), que se encuentran vigentes desde 2013, fueron tenido en cuenta (Ministerio Público, 2020).

Es así que a nivel local se comprende que dentro de la región Lambayeque a partir del año 2020 se han ejecutado un promedio de 1412 denuncias las cuales tiene como materia de investigación los delitos informáticos, pues muchas de ellas han sido tratadas a través de la División de Investigación de Delitos de Alta Tecnología (Divindat), precisando que de los casos 929 han sido presentados como fraude informático y 748 como un delito de operación trasferencias electrónicas no autorizadas.

Finalmente se comprende que la mayor en la que se presenta el delito es a través de mensajes de textos los cuales son publicados por medio de las redes sociales, pues se comprende que este tipo de delitos roba la información necesaria y bancaria de la víctima, es así que se comprende que de todas las denuncias presentadas por los delitos informáticos de la Divindat la mayor parte se genera por el fraude informático (Andina, 2020).

1.2. Antecedentes de estudio

1.2.1. Internacional

Valle (2017), en su investigación titulada, El delito informático de Phishing, la cual fue presentada para obtener el Grado de Maestro en Derecho Penal, en la Universidad Autónoma de los Andes, establece:

> Como objetivo principal de la investigación analizar el delito de Phishing para su adecuada regulación jurídica, aplicando una metodología de tipo descriptiva que permitió concluir que en el estado ecuatoriano se ha dado el primer paso hacia las leyes vigentes que toman en cuenta la información y los estándares informáticos, que se vislumbra como un avance significativo en el país debido a los avances tecnológicos de los últimos años, pero aún es claro, el camino es largo y las discusiones sobre tecnología no deben ser penalizadas. (p.125)

Herrera (2016), en su investigación titulada, El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal, la cual fue presentada para optar el título profesional de Abogado de la Universidad Central de Ecuador, señala:

> Para el desarrollo de la investigación se estableció como objetivo principal, el análisis al delito informático y la determinación de una correcta tipificación del delito, para ello se aplicó una metodología de tipo analítica y propositiva, permitiendo concluir que el Phishing es un delito informático muy peligroso y genera una advertencia en la comunidad, ya que la sociedad está protegida por los derechos de privacidad y propiedad, la Constitución, el Código Penal y los ciudadanos. Por lo tanto, debe redactarse de acuerdo con el Código Penal Orgánico Universal. (p.89)

Terán (2016), en su investigación titulada, La necesidad de incorporar en el código penal el tipo penal de falsificación informática (Phishing), la cual fue presentada para optar el título de profesional de Abogado de la Universidad Mayor de San Andrés, desarrolla:

> Como objetivo principal la incorporación del delito de Phishing en la normatividad del código penal en el estado boliviano, el cual desarrollo una metodología de tipo explicativa que permitió concluir que se deba

> fortalecer el sistema de justicia penal e involucrar a la ciudadanía en la prevención, protección y protección de esta forma de fraude informático, y la adopción de normativas específicas que definan claramente las acciones relacionadas con el fraude informático. (p.108)

Zapata (2019), en su investigación titulada: El delito de estafa en la modalidad “Phishing” a través de internet y sus medios probatorios en Venezuela, la cual fue presentada para obtener el grado de Doctor en la Universidad de Carabobo, desarrolla:

> Como objetivo principal, el análisis al delito de estafa en modalidad de Phishing y le ineficacia normativa del estado venezolano, el cual aplico un desarrollo de tipo descriptivo, permitiendo concluir que, en principio, el sistema basado en pruebas establecido por Venezuela para los procesos penales no está restringido ni relacionado con el uso de la tecnología de la información, más que relacionado con los medios de comunicación, y el canal debe ser aclarado de la mejor manera. (p.87)

Flores (2017), en su investigación titulada, El phishing como comportamiento penalmente relevante, la cual fue presentada para obtener el grado de Doctor en Derecho en la Universidad Católica de Valparaíso, señala:

> Como objetivo principal de la investigación es determinar el comportamiento penalmente relevante frente al delito de phishing, aplicando una metodología de tipo explicativa que permitió concluir que el delito de Phishing es uno de los factores más distintivos de esta figura es la construcción social y subsecciones técnicas que ayudan a ajustar la verdadera naturaleza de la comunicación recibida de la víctima en el ataque. Por lo tanto, es posible que estos últimos actúen con la creencia de que se comunicarán con una entidad "significativamente legítima". (p.43)

1.2.2. Nacional

Mengoa (2021), en su investigación titulada, Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú, la cual fue presentada para optar el título profesional de Abogado de la Universidad Cesar Vallejo, expresa:

> Como objetivo principal el análisis del delito de fraude informático en su modalidad de Phisher-mule para su adecuada sanción penal, la cual fue desarrollada con una metodología de tipo explicativa que permitió concluir que podemos ver que el comportamiento Phishing-mule puede ser modificado en cualquier parte, lo cual es impredecible, por lo que se requiere una investigación en profundidad para planificarlo cuidadosamente e incluirlo en el número de penalización, o reglas especiales, y por lo tanto se recomienda que el curso de este estudio será monitoreado de cerca, ya que en los últimos años, ha habido un aumento de los malos avances tecnológicos, como el fraude informático, la extorsión entre otros. (p.33)

Paredes (2017), en su investigación titulada, De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010, la cual se presentó para obtener el grado de Maestro en Derecho Penal en la Universidad Nacional Mayor de San Marco, establece:

> Que el objetivo principal de la investigación es demostrar la ineficiencia de la normatividad peruana frente a los delitos informáticos, aplicando una metodología de tipo explicativa que permitió concluir que es apropiado utilizar la palabra delito informático o técnico, ya que el consumidor utiliza sistemas informáticos para cometer diversos tipos de delitos, no solo los que se denominan delitos informáticos. (p.248)

Mori (2019), en su investigación titulada, Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012, la cual fue presentada para obtener el grado de Maestro en Derecho Penal en la Universidad Nacional Federico Villareal, establece:

> Que el objetivo principal de la investigación es dar a conocer la ineficiencia normativa frente a la protección penal de los delitos

> informáticos, con una metodología de tipo explicativa, concluyendo para comprender el nivel de trabajo de los administradores judiciales que investigan y procesan delitos informáticos y protegen la privacidad criminal en secreto, se encontró que los jueces admitieron falta de capacitación técnica en delitos informáticos, pero los fiscales y la policía dicen que se oponen los jueces también admiten que no conocen la tecnología. (p.72)

Hancco (2018), en su investigación titulada, La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017, fue presentada para optar el título profesional de Abogado de la Universidad Nacional de San Agustín, estableciendo que:

> El objetivo principal de la investigación es analizar la eficiencia o ineficiencia normativa de la Ley N° 30096 frente al bien jurídico protegido, para ello se utilizó una metodología de tipo explicativa que permitió concluir que se determina que en una variedad de delitos no existe conexión entre la gravedad de los hechos y el veredicto, se puede apreciar que el derecho penal no incluye distinciones entre barreras administrativas, infracciones penales y delitos, el término penal que se analiza, abarca todos los comportamientos que afectan al "sistema". (p.149)

Espinoza (2017), en su investigación titulada, Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control, la cual fue presentada para optar el título profesional de Abogado de la Universidad Nacional del Altiplano, estableciendo:

> Que el objetivo primordial de la investigación es analizar si el derecho penal que sanciona los delitos informáticos es eficaz frente a la deslegitimación del poder punitivo, el cual aplico una metodología de tipo explicativa, permitiendo concluir que el derecho penal informático (ciberdelito), el conocimiento del derecho penal, a través de la interpretación del derecho penal, requiere que los agentes del orden

tengan un sistema para reducir la gestión de la autoridad penal en la comunidad administrativa y promover muevas reglas para proteger las libertades y la privacidad de las personas.

1.2.3. Local

Fuentes (2021), en su investigación titulada, Modificación de la Ley 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019, la cual fue presentada para optar el título profesional de Abogado de la Universidad Señor de Sipán, expresa:

> Como objetivo de la investigación es analizar la Ley 30096 con el propósito de incorporar a los actos de Phishing, Pharming y Carding como delitos penalizables, aplicando una metodología de tipo explicativa que permite concluir que Ahora, el problema con el ciberdelito es que no solo roba información personal del sistema bancario, sino también el hecho de que estas entidades generalmente compran y venden software malicioso en redes oscuras y luego lo comercializan a medida que sucede. Estos delincuentes incluso tienen un servicio para resolver problemas con sus servidores ilegales. (p.50)

Alvarado (2018), en su investigación titulada, Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de independencia, mediante el uso de phishing 2017, la cual fue presentada para optar el título profesional de Abogada de la Universidad Señor de Sipán, desarrollando como:

> Objetivo principal el análisis del delito de Phishing y su vulneración ante la seguridad informática, la cual desarrolla una metodología de tipo explicativa, que permite concluir que una vez analizada la teoría y la práctica de esta tesis, es posible investigar y concluir que, si no existe una política de si en este organismo que pueda mitigar el embate de las construcciones sociales, la información puede fácilmente violarse como el activo más importante. (p.52)

Cruzalegui (2016), en su investigación titulada, Plan de preparación forense digital para maximizar la capacidad de recabar evidencia digital en procesos de medios de pago SA, 2016, la cual fue presentada para optar el título profesional de Abogado de la Universidad Nacional Pedro Ruiz Gallo, señala:

> Como objetivo principal la elaboración e incorporación de un plan forense digital para contrarrestar los delitos de ciberdelincuencia, aplicando una metodología de tipo descriptiva, permitiendo concluir que, para asegurar la integridad de la evidencia digital, desde el momento de su constitución hasta su inicio, la empresa debe armonizar sus controles administrativos, técnicos y físicos para brindar capacitación judicial digital. (p.39)

Díaz (2019), en su investigación titulada, La aplicación de la ley Nº. 30096 - Ley de delitos informáticos respecto a su regulación en el derecho penal peruano, la cual fue presentada para optar el título profesional de Abogado de la Universidad Cesar Vallejo, expresa:

> Que el principal problema del estado peruano es la falta de una correcta regulación, es por ello que se presenta como objetivo principal el análisis de la Ley N° 30096 con el propósito de una correcta modificatoria penal, aplicando una metodología de tipo explicativa que ayudo a concluir que los jueces y policía no es suficiente para castigar a los llamados ciberdelincuentes porque no están capacitados para conocer este tipo de delitos debido a su complejidad técnica. (p.67)

Pardo (2018), en su investigación titulada, Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018, la cual fue presentada para optar el título profesional de Abogado de la Universidad Cesar Vallejo, establece:

> Como objetivo principal el análisis de los delitos informáticos para un adecuado tratamiento jurídico y protección del patrimonio, desarrollando una metodología de tipo aplicada, el cual genero la siguiente conclusión el tratamiento del derecho penal para los delitos informáticos contra la propiedad no es el mismo, porque los tipos y métodos de delitos informáticos contra la propiedad no son conocidos por fraude

> informático, lo que genera incertidumbre en la interpretación de la ley de que los delitos informáticos no pueden ser castigados. (p.153)

1.3. Abordaje Teórico

1.3.1. Análisis Doctrinal

1.3.1.1. Los delitos informáticos

La trascendencia del fenómeno informático, según indica Pérez (2019), es de tal envergadura que se puede afirmar que es equivalente a la transición de la comunicación oral a la escrita o a la posterior invención de la imprenta, que significó la difusión masiva de ideas a través del papel, con la grave deforestación que ello trae consigo. Esta tradicional forma de comunicación, sin embargo, debido a los cambios climáticos generados por el calentamiento global, se ha visto gravemente amenazada por la comunicación virtual, que, dicho sea de paso, evita la deforestación. Además, esta última supera con creces las barreras naturales y de espacio que limitan la comunicación verbal y escrita: hoy en día tenemos la posibilidad de compartir en tiempo real una determinada información con personas que viven en el hemisferio opuesto. Pese a los grandes beneficios que trae consigo la comunicación instantánea respecto a la interacción social y las comunidades virtuales, también ha traído consigo la aparición de nuevas formas de criminalidad que no se pueden combatir eficazmente por la dificultad de identificar a los agentes que se escudan en el anonimato. Ante este escenario, las instituciones del derecho penal y los procedimientos para levantar el secreto bancario y/o el secreto de las comunicaciones deben remozarse para afrontar estos retos.

Casi a diario observamos que sujetos inescrupulosos aprovechan que el comercio por la red y las compras online se han incrementado por el aislamiento social obligatorio para hacer de las suyas y sorprender a diestra y siniestra a numerosas víctimas que caen en sus garras atraídos por sus cantos de sirena. Cabe señalar que la limitación del aforo de las empresas y centros comerciales los ha llevado a diversificar su oferta en el espacio virtual. Para ello han habilitado plataformas y recurrido a la entrega de sus productos

por delivery. De esto se aprovechan los ciberdelincuentes nacionales y extranjeros para ofertar por internet balones de oxígeno, vacunas, empleo, créditos a tasas competitivas, trámites de bonos y todo tipo de mercadería distribuible supuestamente bajo la modalidad de delivery. En ese contexto surgió el presente estudio, al constatar en la práctica cotidiana que esas conductas delictivas contra el patrimonio cometidas en el espacio virtual, relacionadas todas ellas con el engaño y que vemos a diario en los medios de comunicación, no están tipificadas en los delitos contra el patrimonio de la Ley N.º 30096, Ley de Delitos Informáticos (en adelante, LDI).

Para cometer en la red en su forma más burda esta clase de fechorías que afectan el patrimonio de personas incautas, por regla general, los agentes no interfieren ni manipulan el funcionamiento de un sistema informático, tampoco alteran, borran, suprimen o clonan datos informáticos de terceros (verbos rectores del art. 8 de la LDI); simplemente, valiéndose del más burdo engaño y aprovechando las tecnologías de la información y comunicación (TIC) y/o medios de pago electrónico (v. gr.: billetera móvil) ligados a un teléfono celular clonado o cuyo titular es un toxicómano, lanzan ofertas irreales de bienes y servicios que registran gran demanda por la pandemia. Incluso han sorprendido a gobiernos locales, lo cual es anecdótico.

Entonces, ¿qué hacer? La investigación de esta clase de conductas representa un gran problema para los operadores jurídicos (fiscales especializados y la División de Delitos de Alta Tecnología de la Policía Nacional del Perú), por la facilidad de desaparecer las evidencias de la red. Es necesario obtener en tiempo real los datos relativos al tráfico asociados a comunicaciones fraudulentas, así como levantar el secreto de las comunicaciones para identificar el IP o hosting que han utilizado los delincuentes. No olvidemos que el delito es transfronterizo y los agentes delictivos utilizan nombres falsos

Por otro lado, al no estar incluida la forma básica del timo en el fraude informático de la LDI, si se llega a identificar al autor o autores, un abogado escrupuloso exigirá que la conducta de su cliente se reconduzca al tipo básico de estafa previsto en el art. 196 del CP, pues no concurriría ningún verbo

rector del art. 8 de la referida ley. Esta falencia, desde el punto de vista operativo, dificulta el trabajo del persecutor penal, pues impide que se valga de la cooperación internacional en la investigación de los delitos informáticos. El Convenio sobre la Ciberdelincuencia o Convenio de Budapest garantiza que las partes se presten toda la ayuda mutua posible a fin de continuar con éxito las investigaciones y obtener las pruebas necesarias en el formato electrónico pertinente; sin embargo, si no hay delito informático, no se podrá invocar los principios generales de la asistencia mutua del convenio.

Para paliar estos males que se han incrementado de forma exponencial a causa de la pandemia de COVID-19, se ofrece una propuesta de lege ferenda para que se incluya la forma básica del delito de estafa en el capítulo de delitos informáticos contra el patrimonio de la LDI, con el objeto de evitar vacíos de punibilidad en la conducta de los agentes delictivos que utilizan el espacio virtual como factor preponderante para embaucar a sus víctimas y hacerse de sus bienes.

1.3.1.2. Aspectos históricos dogmáticos

La digitalización paulatina de todas las ramas del saber y de las actividades empresariales con sus beneficios y peligros provocó que nuestro país se sacuda del letargo, pues no podía permanecer indefinidamente a la zaga del fenómeno informático, habida cuenta la numerosa cantidad de delitos que inciden sobre los sistemas informáticos, sin dejar de lado las actividades ilícitas cometidas a través de computadoras y/o el internet. Por ello, antes de la promulgación de la LDI, que data del 22 de octubre del 2013, la conducta de los delincuentes informáticos que afectaba el patrimonio de sus víctimas se encontraba regulada como agravante en el inciso 3 del segundo párrafo del art. 186 del CP (hurto agravado). Dicho inciso sancionaba la “utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación de claves secretas”; sin embargo, esta regulación no era propia de un delito informático (este aún no tenía autonomía) y dejaba impunes, entre otras, muchas conductas en las que se utilizaba equipos de cómputo y el internet precisamente para obtener claves secretas.

Luego, a través de la Ley N.° 27309, publicada el 17 de julio del 2000, se incorporó el capítulo x a nuestro Código Punitivo. Este capítulo, referido a los delitos informáticos, adicionó los arts. 207-A, 207-B y 207-C al CP. Posteriormente, a través de la Ley N.° 30076, del 19 de agosto del 2013, se añadió el art. 207-D. Estos artículos regulaban: la interferencia y acceso ilícito a una base de datos; la alteración, daños o destrucción de una base de datos; sus circunstancias agravantes; y el tráfico ilegal de datos. Todas estas normas fueron derogadas al promulgarse la LDI, que luego fue modificada por la Ley N.° 30171, del 10 de marzo del 2014, para adecuar nuestra legislación a los parámetros del Convenio de Budapest, del 23 de noviembre del 2001, cuya adhesión fue aprobada por Resolución Legislativa N.° 30913, del 12 de febrero del 2019, y ratificada por D. S. N.° 010-2019-RE, del 9 de marzo del 2019.

Desde de la incorporación del capítulo x a nuestro CP, la investigación del delito informático era realizada por la División de Estafas de la Dirección de Investigación Criminal (Dirincri), los departamentos de investigación criminal (Depincri) e incluso las comisarias, es decir, no había especialización ni en la Policía Nacional del Perú (PNP) ni en la Fiscalía. Sin embargo, esta situación cambió radicalmente al expedirse la Resolución Directoral N.° 1695-2005-DIRGFN/EMG, del 8 de agosto del 2005, que creó la División de Investigación de Delitos de Alta Tecnología (Divindat). Adicionalmente, al percatarse del crecimiento exponencial del ciberdelito por la pandemia y para ponerse a tono con los tiempos y recoger el clamor de los órganos de persecución penal de América y del mundo, la Fiscalía de la Nación, a través de la Res. N.° 1503-2020-MP-FN, publicada el 1 de enero del 2021, creó la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público. Esta unidad tiene competencia nacional y una de sus funciones es brindar asesoría a los fiscales en las investigaciones de los delitos comprendidos en la LDI, en el art. 196-A.5 del CP (estafa agravada) y en aquellos casos en los que la obtención de prueba digital sea determinante para la investigación

1.3.1.3. Características conceptuales de los delitos informáticos

Definir el ciberdelito es una tarea titánica. Algunos autores consideran que es imposible encontrar un concepto unitario, toda vez que su definición ha ido cambiando desde hace cuarenta años, conforme han ido evolucionando las TIC y el objeto de protección de la norma. No es nuestro propósito agotar el tema, pues nuestro análisis solo se refiere a los delitos informáticos contra el patrimonio; sin embargo, esbozamos algunas definiciones. Según Hernández (2009) señala que al principio el ilícito informático se limitaba al ámbito patrimonial, esto es, a la protección de bienes intangibles ligados al mundo de los ordenadores. Así, se punían conductas como el acceso indebido, alteración, destrucción y tráfico de bases de datos y/o programas de computadoras (software). Luego está lista se amplió, pues con la digitalización de una ingente cantidad de datos y la expansión de las redes sociales se tuvo que proteger la intimidad personal, la suplantación de identidad, la indemnidad y libertad sexual y, nuevamente, el patrimonio, esta vez afectado por los fraudes informáticos, entendidos estos como manipulación o interferencia en el funcionamiento de sistemas informáticos que causen perjuicios patrimoniales.

Salinas (2013) define al delito informático como la:

> Conducta típica, antijurídica, culpable y punible en la que la computadora, sus técnicas y funciones desempeñan un papel trascendental, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente.

Por su parte, Villavicencio Terreros entiende que la criminalidad informática está conformada por:

> Aquellas conductas dirigidas a burlar los sistemas de seguridad, esto es, invasiones a computadoras, correos o sistemas de datos mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología.

Estas definiciones están ligadas a la concepción restringida del fenómeno informático, donde los principales afectados son los datos del sistema, el software y, en algunos casos, el hardware; sin embargo, conforme han surgido

nuevas conductas típicas efectuadas a través del internet, ha recobrado relevancia la visión amplia u omnicomprensiva del fenómeno informático, ligado a la expansión del derecho penal, el cual es utilizado actualmente como panacea para reprimir toda clase de conductas lesivas. En ese orden de ideas, según Hernández (2009), se puede definir como delito informático a toda acción antijurídica que se realice en el espacio virtual o entorno digital con el empleo de las TIC como medio o fin y que cause perjuicios relevantes. Esta concepción difiere de las concepciones intermedia y restringida del delito informático.

Morillas (2017) señala que la concepción intermedia, defendida en la doctrina hispana por González Rus, considera que:

> En los delitos informáticos el sistema informático y sus elementos, en algunos casos, son el objeto material del delito y, en otros casos, son instrumentos del delito. Asimismo, tal concepción estima que los delitos informáticos deben mantenerse apartados de los tradicionales, salvo que con las conductas "tradicionales" también se generen daños a los sistemas informáticos.

Por su parte, la concepción restringida destaca la autonomía del delito informático. Para esta concepción, el delito informático abarca solo las conductas que atenten contra el software o soporte lógico de un sistema de procesamiento de datos o de información y que no puedan ser subsumidas en los delitos tradicionales, aunque los agentes para lograr sus propósitos empleen las TIC.

Las características de los delitos informáticos, según apunta Morillas (2009), son los siguientes:

a) Los ilícitos se cometen a distancia, esto es, sin interacción física entre víctima y victimario, pues los contactos se dan generalmente por el chat o vía telefónica. Se trata de un delito transfronterizo por la propia naturaleza del ciberespacio que acorta la separación física entre las partes.

b) La falta de regulación en la red dificulta la verificación de la información que circula en el ciberespacio.
c) El anonimato prima en la mayoría de transacciones de bienes y servicios. Existe gran facilidad para borrar las huellas perceptibles del delito.
d) Los sujetos activos en los delitos informáticos que afectan un sistema o una base de datos (hackers, crackers) son personas que poseen conocimientos avanzados de programación.
e) Existe indeterminación en las victimas, pues los destinatarios de las ofertas fraudulentas son el colectivo social, cuyos miembros ni siquiera son conocidos por el agente.
f) Existe una elevada cifra negra de la criminalidad por la misma naturaleza del delito, que puede ser transfronterizo, y por las dificultades para identificar a los agentes, ya que estos se esconden tras nombres hipocorísticos. Por ello, para combatirlos se hace indispensable la especialización y la cooperación internacional conforme lo prevé el Convenio de Budapest

1.3.1.4. El bien jurídico protegido

No se ha concretado en la doctrina un criterio uniforme para establecer cuál sería el bien jurídico protegido en estas variadas formas de criminalidad. Este dependerá del concepto de cibercriminalidad que se adopte, el cual actuará como un criterio de legitimación para la intervención del derecho penal. Así, el término “criminalidad informática” en sentido estricto alude a comportamientos típicos que afectan a un sistema informático, es decir, al software y a todo soporte lógico que permite el procesamiento de datos, así como a la protección de la intangibilidad y confidencialidad de dicho sistema, v. gr.: contra el sabotaje o espionaje. En cambio, en sentido amplio la cibercriminalidad engloba también a ciertos delitos tradicionales cometidos a través de computadoras y/o el internet. Pese a esas dificultades, la mayoría de legislaciones sostienen que se trata de un delito pluriofensivo. En nuestro país, en la exposición de motivos de la ley de la materia, pese a los avances tecnológicos y los problemas generados por el uso generalizado de las TIC,

no se ha configurado un nuevo interés jurídico digno de protección además de los tradicionales.

La doctrina se divide entre los que sustentan la concepción de cibercrimen en sentido estricto y los que la sustentan en sentido amplio. En el primer caso, el bien jurídico protegido es la “funcionalidad informática”, entendida esta como presupuesto para la realización de actividades relevantes para las personas e instituciones de un Estado democrático de derecho. La “funcionalidad” se identifica con el “conjunto de condiciones” que posibilitan el funcionamiento de programas (software), es decir, la adecuada realización de “operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo” (Mayer, 2017)

Para el otro sector de la doctrina, el bien jurídico tutelado se concibe en dos planos concatenados entre sí. En el primero se encuentra la información en general, “almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos”. En el segundo plano, “los demás bienes jurídicos afectados” por la interacción de los medios o instrumentos propios de la actividad informática, tales como la intimidad, la indemnidad sexual, la fe pública, etc. La información debe ser entendida como “el contenido” de una base de datos o como “el producto de los procesos informáticos automatizados”. De esta forma, la información es un bien autónomo de valor económico que debe ser tutelado, sin perjuicio de brindar protección a los demás bienes jurídicos tradicionales que confluyen en la red de redes y se ven afectados por la cibercriminalidad, tales como el patrimonio, la indemnidad y libertad sexual, la fe pública, entre otros, aunque dichos bienes estén tutelados por otros tipos penales (Gutiérrez, 2017)

Por su parte, Palomino (2014) señala que el desarrollo de las TIC ha traído consigo un nuevo interés social merecedor de protección. Por ello, es necesario regular los procedimientos de almacenamiento, transmisión y empleo de mecanismos automatizados, en donde el bien jurídico protegido sería el orden informático y las bases de datos de soporte inmaterial.

1.3.1.5. El fraude informático en la modalidad de phishing

Hablar del phishing es hablar de delitos informáticos. Esta práctica delictiva apareció a mediados de la década pasada con el único objetivo de apoderarse de la información confidencial del usuario (número de cuenta, tarjeta, contraseñas/ PIN de acceso, número de documento, etc.) y con ello sustraer su patrimonio. En la actualidad, esta modalidad delictiva sigue en auge debido a los avances de la tecnología y la globalización.

En el ámbito internacional, este tipo de delito informático está regulado en el Código Penal de cada país de la Unión Europea. En Latinoamérica, Colombia, Chile y Brasil también regulan este tipo de delitos en su marco jurídico. El Perú no es ajeno a esta problemática socioeconómica que afecta a la ciudadanía y que utiliza los medios tecnológicos como herramientas de trabajo para intervenir, por ejemplo, en transacciones bancarias. Si bien es cierto en nuestro país tenemos la Ley N.º 30096, Ley de Delitos Informáticos (5 de diciembre del 2013), que fue posteriormente modificada por la Ley N.º 30171, el 10 de marzo del 2014, consideramos que existen varias lagunas jurídicas al no tipificar de manera explícita los tipos de delitos informáticos, lo que repercute en la reducida seguridad que puede brindar su radio de acción a pesar de que cada día aumentan estas formas delictivas.

El phishing pertenece a la categoría de delitos de fraude informático, por ende, es imprescindible definir qué es fraude informático y los tipos de fraudes que existen, para luego abordar el tema en cuestión.

El fraude informático es uno de los delitos que atenta contra el patrimonio de una persona natural o jurídica. Su componente principal es el ánimo de lucro. Este delito se fundamenta en tres supuestos: 1) engaño, 2) error y 3) disposición del dinero e individuo que realice este acto ilícito. Muchas veces, las legislaciones no están acorde con el contexto social, debido a que están desfasadas frente a estos tipos de delitos, en consecuencia, existen individuos inescrupulosos que se aprovechan de los vacíos legales para ejecutar ilícitos penales en diferentes modalidades. Una de estas modalidades es el phishing, que se apoya en los sistemas informáticos de alta gama.

1.3.1.6. El concepto y orígenes del Phishing

A nivel mundial, los casos de phishing han ido en aumento a raíz de los avances de la tecnología, pues los hackers perfeccionan, cada vez más, las modalidades de sustracción de data, clonación, suplantación, introducción de virus en los sistemas financieros o webs. Incluso países del primer mundo, como España, Francia e Italia, que cuentan con una ingeniería informática más eficiente que cualquier país de Latinoamérica, se ven afectados, pues, a pesar de sus modernos sistemas y modificaciones de normas, se les hace difícil combatir la ciberdelincuencia en todas sus modalidades.

El Perú no es la excepción, pues son evidentes las falencias que tiene el Estado respecto a brindar seguridad informática. Aunque tengamos una ley especial para este tipo de delitos, Ley N.° 30096, donde se encuentra regulado el delito de fraude informático (del que forma parte del phishing), esta es general y ambigua porque no especifica, por ejemplo, las modalidades de fraudes y sus respectivas penas. Por ello, consideramos que es necesario abordar la problemática del phishing, que, si bien es cierto, por su denominación, muchos no logran entender el significado, es uno de los delitos que va creciendo a gran escala.

Actualmente, el phishing es uno de los tipos de amenazas de fraudes informáticos más peligrosos para el desarrollo de la sociedad, ya que implica la sustracción de tus datos personales, contraseñas, tarjetas de créditos. Asimismo, no solo es un peligro para las personas naturales, también lo es para las personas jurídicas, que se han visto perjudicadas bajo esta nueva modalidad de fraude. Acerca del origen de la palabra phishing, Leguizamón refiere lo siguiente:

El origen de la palabra phishing proviene del término fishing, que significa pescar. Se identifica con esta palabra porque la intención de esta estafa es “pescar” a usuarios (las víctimas) de internet para que revelen información susceptible. Es decir, intentan que coja el “anzuelo” y ofrezcan sus datos confidenciales.

Pero también hay razones por las cuales se utiliza el vocablo “ph” para referirnos al término y no la “F”. Esto se debe a que los primeros hackers eran conocidos como phreaks. Proviene de la palabra phreaking, que es el estudio, aprendizaje y comprensión de las nuevas tecnologías. Tanto el término hacker como phreaker siempre han estado relacionados y están estrechamente vinculados y, por tanto, el uso del “ph” es para que sea más fácil identificar los ataques cibernéticos (Leguizamón, 2015, p.9)

El phishing, en términos sencillos, es el procedimiento por el cual el usuario (la víctima) es contactado, a través de correos electrónicos o mensajes de texto, por el ciberdelincuente que simula ser una persona o entidad bancaria confiable, para así apoderarse de datos confidenciales, claves, estados de cuenta, etc. Luego de obtener la información confidencial de manera fraudulenta, esta es utilizada indebidamente para acceder a las cuentas personales de la víctima y quitarles su patrimonio.

Del mismo modo, Leguizamón (2015), indica que:

La forma de phishing más utilizada es el envío masivo de correos electrónicos, a las cuentas de Gmail, Hotmail, etc. Con la finalidad de engañar a la víctima y que proporcione sus datos personales al phisher”.

Con el pasar de las décadas esta técnica ha ido mejorando, ya que muchas veces es difícil detectar un correo falso, lo que facilita el acto ilícito. A diario recibimos diferentes tipos de mensajes en nuestros celulares o correos electrónicos. Y si bien muchas veces estos nos causan fastidio por su evidente falsía, otras veces podemos estar distraídos y emocionamos al recibir alguna “oferta” interesante, por lo que fácilmente podemos caer en la “trampa” y convertirnos en una víctima más de los ciberdelincuentes.

De igual manera, existen otros tipos de delitos informáticos. El pharming (otra modalidad de ataque al servidor) consiste en redirigir el tráfico cibernético hacia una web falsificada para cometer el fraude. El vishing (término que deriva de la unión de voice y phishing) es el medio por el cual la víctima recibe un correo electrónico indicándole que debe marcar un número telefónico debido a alguna urgencia bancaria, pero, al hacerlo, el receptor le solicita a la

víctima sus datos personales —lo cual es absurdo—. Esto se da porque el ciberdelincuente ya ha conseguido información confidencial mediante un ataque de phishing, pero le falta la clave SMS o token digital para completar o validar una operación. Por último, tenemos el smishing, que es algo parecido al phishing, pero a través de mensajes de texto, SMS. Estas modalidades de fraude cibernético han funcionado eficientemente, pues han logrado dañar patrimonialmente a cientos de víctimas en el mundo, los cuales no han podido recuperar su dinero.

Oxman (2013) menciona que:

Tanto el phishing como el pharming tienen una estrecha relación. Ambos son dos tipos de delitos de fraudes informáticos que están en boga en la última década.

La finalidad de los dos es apropiarse de los datos personales del usuario (claves secretas, cuentas bancarias, correos electrónicos) para perjudicarlos patrimonialmente; sin embargo, la diferencia es el medio que se utiliza para lograr que se cometa el hecho punible: mientras que el phishing es utilizado a través de correos electrónicos para redirigir hacia una web falsa, el pharming lo que hace es introducir un virus al internet del usuario a través del DNS (Domain Name Server) para también llevarlo hacia una web falsa. Podemos decir que el término phishing es capturar información a través de internet.

A pesar de los cambios y mejoras que se han realizado en los diferentes niveles de software, ha sido difícil frenar esta ola de delitos informáticos. Más aún en tiempos de pandemia de COVID-19, donde se han expuesto mucho más las falencias que tiene nuestro sistema informático peruano.

1.3.1.7. Los tipos de Phishing

Sobre la base de diferentes investigaciones realizadas acerca del phishing, creemos que es importante mencionar qué tipos existen y sus modalidades.

Para López (2019) los tipos de phishing son los siguientes: deceptive phishing, malware-based phishing, content-injection phishing, spear phishing, pharming y smishing

1.3.1.7.1. Deceptive phishing

El deceptive phishing es el tipo de phishing más común. Esta modalidad consiste en enviar de manera masiva correos electrónicos de la entidad suplantada, y tienen el propósito de solicitar algún dato o clave. Los correos fraudulentos son muy frecuentes a nivel mundial, por lo que miles de usuarios son víctimas de links que los inducen al error para poder sustraerles su patrimonio.

1.3.1.7.2. Malware-based phishing

El malware-based phishing es un tipo de virus troyano. Primero, a través de un archivo adjunto malicioso, infecta la máquina de la víctima; luego, cuando la víctima utiliza su navegador web — Google u otro— y visita la página de una entidad bancaria, el virus se activa inmediatamente. Las credenciales que tiene cada entidad son robadas por este malware para sustraer la información de la víctima y así quitarle todo el dinero de su cuenta bancaria.

1.3.1.7.3. Content-injection phishing

Este tipo de modalidad es difícil de detectar porque si el sujeto activo que realizó la operación tiene conocimiento de informática, una vez que haya introducido el virus pueden pasar días o meses hasta el momento de activarse.

1.3.1.7.4. Spear phishing

El spear phishing es similar al deceptive phishing, pero con la diferencia de que los correos electrónicos que se envían van dirigidos a una determinada persona natural o jurídica. Esta modalidad es mucho más refinada porque conocen a su objetivo, sus gustos o preferencias. Los correos que se envían son tan sofisticados que dificultan su detención debido a su adaptación al receptor.

1.3.1.7.5. Pharming

En estos casos, la víctima es engañada y sufre un ataque a su servidor, que se utiliza para decidir qué navegador usar del internet. Esto puede ejecutarse

tanto al servidor público como a un servidor local. En otras palabras, cuando la persona desee entrar a su navegador, será redirigida a otro que el delincuente ha introducido para sustraer data o engañar al usuario.

1.3.1.7.6. Smishing

Suelen ser denominados así porque el fraude se realiza a través de mensajes de texto. Estos suelen ser concisos y tienen un contenido sugestivo, así logran capturar la atención de la víctima. Para perjudicar patrimonialmente a la víctima, esta tiene que hacer clic en el enlace adjunto al contenido del mensaje de texto.

1.3.1.8. El phishing en la era digital

Los fraudes informáticos se han incrementado a un nivel exponencial en estos tiempos de pandemia de COVID-19. Las noticias evidencian el aumento de casos de ciudadanos que denuncian haber sido víctimas de ciberdelincuentes. Sin embargo, ¿qué han hecho las entidades financieras y las instituciones del Estado para prevenir y sancionar estos delitos? Hasta el momento la ayuda es escasa y el marco jurídico que tenemos respecto a los delitos informáticos es muy general (Matos, 2021, p.153)

Entonces, ¿cómo nos protegemos para evitar ser víctima del phishing y de otros fraudes informáticos? La Guía de Seguridad de la Universidad de Jaén (España) (2018), nos brinda algunos consejos al respecto:

a) Informarnos sobre cómo detectar un mensaje de phishing.

b) No compartir información de nuestras cuentas bancarias, claves, códigos y otros.

c) Ser cautelosos al momento de llenar cuestionarios virtuales (para capacitaciones, diplomados, encuestas, trámites, etc.) con nuestra información personal.

d) Ignorar correos electrónicos o mensajes de texto de remitentes desconocidos, así sean de entidades financieras con las que tengamos un vínculo financiero, es preferible hacer caso omiso por precaución.

En todo caso, ante la duda, comunicarnos directamente al número de la institución bancaria. Por regla general, ningún banco solicita información confidencial vía telefónica u otros medios. Ante la insistencia para que compartamos información, podemos acudir a cualquier dependencia policial y manifestar tales hechos.

e) Si tenemos sospechas de un mensaje, nunca hacer clic en el link que nos envían. Dirijámonos directamente a la página web a través del buscador. No olvidemos verificar siempre el candado de seguridad.

f) Jamás contestemos correos electrónicos referidos a la cancelación de cuentas, créditos o mensajes similares. Primero llamemos a la entidad financiera y realicemos las consultas pertinentes, porque podría ser un fraude.

g) En caso nos soliciten algún tipo de información financiera, debemos verificar si tenemos algún vínculo con esa entidad y si contiene una firma digital (aunque esto tampoco sea de mucha confianza). Generalmente, en los casos de phishing siempre envían mensajes alarmantes para llamar la atención del usuario.

h) Muchas veces los mensajes falsos que recibimos no son personalizados. En cambio, los mensajes de las empresas o entidades financieras son verídicos porque cuentan con identificación del remitente.

i) Instalar un antivirus (y tenerlo actualizado) en nuestra laptop, pc de escritorio, tableta o cualquier dispositivo que usemos para conectarnos a la red. Esto a fin de prevenir el acceso a páginas no confiables o apócrifas.

j) Si contamos con la aplicación de alguna entidad bancaria, siempre verifiquemos el estado de nuestra cuenta, los movimientos y transacciones. Asimismo, la aplicación tiene que estar vinculada con nuestro correo electrónico, para que, cuando se realice alguna operación, nos llegue la notificación.

k) Mantener actualizados las aplicaciones y navegadores de nuestros dispositivos. Las versiones pasadas pueden no contener las medidas de seguridad adecuadas.

l) Acceder siempre a las páginas webs de las entidades financieras digitando la dirección completa en el navegador y no haciendo clic en enlaces recibidos a través de un mensaje electrónico. Muchas veces estos links son falsos.

m) Para las reposiciones de contraseñas o de tarjetas, es recomendable hacerlo presencialmente en el banco. Aunque nos tome más tiempo, es más seguro. Es preferible demorarnos en el banco a ser víctimas de los ciberdelincuentes. Asimismo, no solicitemos tarjetas de crédito o débito vía telefónica, ya que no podemos estar seguros si en realidad nos estamos contactando con un integrante del banco.

1.3.1.9. Medidas anti-phishing para adoptar en los equipos electrónicos

En esta sección vamos a mencionar algunos servicios de correos electrónicos y navegadores que debemos de utilizar y actualizar con la finalidad de evitar virus maliciosos que conlleven a un fraude informático.

1.3.1.9.1. Outlook

Este servicio de correo electrónico nos ofrece eficiencia en la seguridad contra el phishing (Outlook los denomina “mensajes malintencionados”). Para acceder a esta opción, tenemos que ingresar a nuestro correo electrónico, luego hacer clic en “Mensajes no deseados”, “Opciones”, “Deshabilitar los vínculos”. De esta manera podremos evitar mensajes no deseados que intenten sorprendernos y nos hagan víctimas de un fraude informático.

1.3.1.9.2. Gmail

Este servicio de correo electrónico desde hace tiempo viene implementando medidas para evitar que los ciberdelincuentes envíen mensajes con virus a los usuarios. Una de sus soluciones contra el phishing más publicitadas en los últimos meses es el uso de las llamadas “cuentas verificadas”

1.3.1.9.3. Mozilla

Mozilla contiene filtros para prevenir la detección de correos fraudulentos. Señala los mensajes sospechosos, el usuario puede desmarcarlos si no lo es. Para usar esta opción, hay que seguir los pasos siguientes: menú / opciones / seguridad / correo fraudulento.

1.3.1.9.4. Opera

Este navegador web es uno de los que más instalan los jóvenes en sus laptops, celulares y tabletas. Su alta velocidad lo hace indispensable para realizar actividades diarias de estudio o trabajo. Asimismo, tiene herramientas que evitan los virus.

Habiendo mencionado los tipos de navegadores y servicios de correos electrónicos más confiables en el mundo digital, queda a criterio del lector escoger el que más le convenga para su vida cotidiana. Asimismo, debemos tener en cuenta las recomendaciones y pasos ya mencionados a fin de evitar ser víctima de los ciberdelincuentes que tratan de sustraer nuestro bien patrimonial de cualquier forma y por distintas modalidades

No cabe duda que el phishing está en todas partes. El efecto que tiene en la sociedad actual es peligroso y queda ya en manos de los legisladores modificar las normas para garantizar nuestra seguridad informática.

1.3.1.10. Los efectos del phishing en la sociedad

La posibilidad de ser víctima del phishing conlleva a que el usuario tenga reticencia al momento de utilizar los medios tecnológicos propios o de cualquier entidad financiera. Leguizamón indica, de manera puntual, dos impactos importantes del phishing en la sociedad: a) el efecto social y b) el efecto económico.

1.3.1.10.1. Efecto social

El aumento, a nivel mundial, del phishing atenta contra la seguridad y confianza que debe de tener todo usuario al momento de utilizar el internet como medio para hacer operaciones bancarias. De acuerdo a estudios

realizados, lo que una persona valora y desea es la total privacidad de sus estados de cuentas. Así, el 60 % asegura que no realiza compras online por temor a ser estafado. Manifiestan, además, que utilizarían una aplicación de manera frecuente si estas contaran con sistemas de control de seguridad más confiables. El 82 % de los ataques cibernéticos son a través de la modalidad del phishing.

1.3.1.10.2. Efecto económico

Estamos frente a un nuevo delito que requiere para combatirlo una regulación a nivel nacional y mayor cooperación internacional entre los países. En España, por ejemplo, para que se considere delito el fraude informático tiene que superar los 400 euros, si no es así, es considerado como una falta. En Estados Unidos las pérdidas económicas por este delito son más cuantiosas, alrededor de 1000 millones de dólares, por esta razón, el efecto del phishing es considerado grave, pues los ataques de virus causan grandes daños a las entidades financieras y/o usuarios.

En el Perú es usual el fraude informático mediante la modalidad del phishing. Para los delincuentes es atractivo realizar este tipo de delitos debido a que la respuesta de nuestro sistema judicial es tardía. No hay una adecuada regulación que sancione de forma eficaz y pueda resarcir el daño patrimonial ocasionado a la víctima. Es por esa razón que vemos a diario en las noticias y redes sociales una gran cantidad de personas que denuncian haber sido víctimas de estos ciberdelincuentes, quienes se aprovecharon de la poca información de las personas acerca de este tema y de la inseguridad informática para burlar sus códigos financieros y cometer el ilícito penal.

1.3.2. Análisis Legislativo

1.3.2.1. La Ley N° 30096 frente al delito de fraude informático

Materialmente, el delito de fraude informático es un delito de dominio; se encuentra tipificado en el art. 8 de la LDI, en el capítulo de delitos informáticos contra el patrimonio; y, siguiendo ciertos lineamientos del Convenio de Budapest, sanciona al agente que dolosamente procura para sí o para otro un

provecho ilícito en perjuicio de cualquier persona natural o jurídica, “mediante el diseño, introducción, alteración, borrado, supresión o clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático”. La pena conminada oscila entre tres y ocho años de pena privativa de libertad aparejada de multa. Como se puede apreciar, esta redacción genera confusión, pues la mayoría de verbos rectores del fraude informático introducir, borrar, alterar o suprimir datos informáticos también se encuentran en el delito de atentado contra la integridad de datos informáticos (art. 3 de la LDI), que paradójicamente no se encuentra dentro del capítulo de delitos contra el patrimonio.

Por ende, para hacer una diferenciación adecuada corresponde al operador jurídico demostrar el animus doli del agente al llevar a cabo estas conductas, esto es, el beneficio obtenido para sí o para terceros (una suerte de tendencia interna trascendente), toda vez que el atentado contra la integridad de datos informáticos, si bien requiere la concurrencia del animus nocendi, no exige que el agente obtenga necesariamente un beneficio para sí o para terceros. Por lo tanto, si en la investigación no se logra probar el provecho ilícito, nos quedamos con los daños (cuya probanza solo requiere de un peritaje) o con un delito tentado si no se acredita el perjuicio.

Si bien no existe unanimidad en los especialistas, el agente que despliega estas actividades de acuerdo a los verbos rectores mencionados requiere de conocimientos intermedios o avanzados de computación. Puede darse el caso de que la persona que acceda a información sensible de una empresa sea un hacker o cracker. En ese sentido, dada la competencia en el mundo globalizado, nada obsta para que surja la figura del inductor, que sería el verdadero interesado en obtener el know how de sus rivales y/o la base de datos de los clientes de estos.

Por otra parte, para nuestra idiosincrasia, el vocablo “fraude” está ligado a la defraudación, estafa y engaños en todas sus modalidades; sin embargo, el art. 8 de la LDI no alude a ningún elemento propio de la estafa básica, situación que causa problemas a los operadores jurídicos cuando el perjuicio es colectivo y sale a la luz en todos los medios de comunicación, entonces no

les queda más remedio que acudir al tipo básico de estafa en concurso con el art. 9 de la LDI, que trata sobre la suplantación de identidad, toda vez que es usual que los agentes delictivos se escondan tras nombres de terceros, aunque estos terceros sean personas con incapacidad relativa (farmacodependientes) o personas jurídicas dadas de baja por el registro.

Según García (2015) señala que el fraude informático es “un delito común que puede ser cometido por cualquier persona, más allá de la experticia que su ejecución requiere”. Se admite la realización conjunta del delito, pues estamos ante un “delito de dominio”, en donde los agentes se dividen los roles; por ende, la pluralidad de intervinientes da lugar a la coautoría o complicidad y se sanciona “únicamente a título de dolo”.

1.3.2.2. El comercio electrónico en la red de redes y su incremento

En nuestro país el e-commerce está regulado en forma dispersa; pese a las recomendaciones de la Organización Mundial del Comercio (OMC), carecemos de una norma unitaria. Así, tenemos a la Ley N.° 27291, que, en concordancia con el art. 140 del CC, regula la manifestación de voluntad y la firma electrónica en los contratos digitales en la red.

Tenemos también la Ley N.° 29733, Ley de Protección de Datos Personales, y el D. S. N.º 003-2013-JUS, su reglamento, que establecen los requisitos que deben cumplir las empresas que reciben, recopilan, almacenan o suministran información de personas naturales (implementar políticas de privacidad, confidencialidad y medidas de seguridad para evitar la filtración de estos datos personales). Estas normas, asimismo, establecen las condiciones para la validez del consentimiento otorgado por las personas naturales cuando se trata de información sensible. Además, señalan que el Ministerio de Justicia (Minjus), a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales; y, por último, establecen un procedimiento administrativo sancionador.

Otra de estas normas es la Ley N.° 27269, Ley de Firmas y Certificados Digitales, y el D. S. N.º 052-2008- PCM, su reglamento, que regulan el empleo de la firma electrónica en los contratos virtuales, a la cual dotan de la misma

eficacia que la firma a manuscrito. Asimismo, crean el certificado digital, que debiera estar garantizado por una empresa de certificación que confirme la identidad de los usuarios, pero, por la urgencia de la pandemia, estas firmas digitales ahora reciben el respaldo del Registro Nacional de Identificación y Estado Civil (Reniec), lo que contribuye a la seguridad jurídica.

Por último, tenemos la Ley N.° 29571, Código de Protección y Defensa del Consumidor, que establece las obligaciones que debe cumplir el proveedor en estas transacciones de bienes y servicios a través de la red de redes.

Por otro lado, la inmovilización social obligatoria impuesta por el Ejecutivo debido al Sars CoV-2 ha incrementado en forma significativa el comercio electrónico y modificado el comportamiento del consumidor. Así, personas de todas las edades y estratos sociales no familiarizadas con las compras, pagos y tramites online han tenido que aprender sobre la marcha cómo emplear las TIC para abastecerse de bienes y servicios que son ofertados en la red por empresas grandes y pequeñas. Las empresas, a su vez, ante la limitación de su aforo, se han visto obligadas a modificar sus sistemas tradicionales de ventas y pagos para no perder a su clientela tradicional y de paso mantenerse en el mercado. Así, el comercio electrónico, alentado por el confinamiento obligatorio y el temor a los contagios, ha crecido en forma exponencial. Las empresas, incluidas las mypes, se han visto obligadas a potenciar las ventas online, para lo cual, de paso, han hecho labor pedagógica a fin de animar a los indecisos. Asimismo, los distribuidores han tenido que idear nuevas formas de aprovisionamiento para abastecer, por ejemplo, al comercio retail, y estos negocios a su vez han sido muy creativos para hacer entregas por delivery. Aquí se cumple cabalmente el lema “renovarse o morir”; no hay marcha atrás.

Podemos decir también que, como factores de apoyo para el incremento del comercio electrónico, las instituciones financieras, los nuevos medios de pago y la obtención de créditos fuera del marco tradicional no se han quedado a la zaga. Gracias a la pandemia los bancos han triplicado el número de clientes nuevos en sus canales digitales. De igual manera, las transacciones a través de pasarelas de pago y ventas como PayPal, Izipay, e-BAY, Amazon, Niubiz (antes Visanet), etc. crecen a ritmo sostenido. Asimismo, continúan

apareciendo en la red, como novedad financiera, empresas fintech (financial technology) especializadas en otorgar préstamos, venta de seguros, operaciones de factoring, venta de divisas, criptomonedas, etc., dirigidas a sectores no bancarizados o subbancarizados, con el riesgo que ello trae consigo, pues no tienen un marco regulatorio específico en la Superintendencia de Banca y Seguros y AFP (SBS). Adicionalmente, los pagos a través de la billetera móvil o billetera electrónica (BIM y Yape son algunas de ellas) también crecen a ritmo sostenido. La banca móvil permite hacer pagos a través del celular y evitar el uso de efectivo por medio de un código QR. Según voceros de la empresa Pagos Digitales Peruanos, BIM ha cerrado el 2020 con casi un millón de usuarios y cuenta con más de cien mil establecimientos afiliados (Noticias de Business Empresarial, 2021).

En tiempos de pandemia las ventajas del comercio electrónico son evidentes, pues reducen el empleo de papel en toda clase de trámites, los traslados obligatorios a los grandes almacenes, bancos e instituciones de administración de justicia, de manera que se evita la cercanía física de las personas, fuente primigenia de contagios. Así, según el reporte oficial de la industria e-commerce, el Perú, que en el 2019 tenía seis millones de compradores online, paso a tener 11.8 millones en el 2020. Asimismo, se cuadruplico el número de empresas que ingresaron al e-commerce, y el número de envíos e-commerce creció en 300 % (BlackSip, 2020)

Respecto a las regulaciones y control del e-commerce, Arocena (2017) señalan que:

La regulación internacional respecto al comercio electrónico, el tráfico de información y de mercancías en internet se centra en el control y registro de personas jurídicas, mientras que las transacciones en el mercado virtual de personas naturales carecen de regulación o esta es muy laxa, por la imposibilidad de llevar un control.

Sobre este punto, la OMC solo ha brindado recomendaciones generales, que son insuficientes para prevenir el accionar de los ciberdelincuentes. Por ello se dice que los esfuerzos y estrategias para imponer la ley penal en el mundo

real con los tratados de cooperación, extradición y la creación de la Corte Penal Internacional han tenido poco éxito o han sido inadecuadas en el mundo virtual.

1.3.2.3. Problemas detectados y falencias para combatir las nuevas conductas fraudulentas

Aparte de las dificultades tradicionales para identificar a los ciberdelincuentes que subsumen su conducta en los verbos rectores del art. 8 de la LDI, v. gr., diseño, introducción, alteración, borrado, supresión o clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, cabe señalar que a raíz del incremento exponencial del e-commerce por la pandemia han surgido nuevas conductas típicas o se han remozado las antiguas, de tal manera que ahora prima el engaño y el ardid del agente para apoderarse del patrimonio de sus víctimas. Estas actividades delictivas son cometidas a través de la autopista de la información. Las redes sociales (Facebook, Instagram), por su dinámica, se han convertido en el principal vehículo utilizado por los ciberdelincuentes para sorprender a sus víctimas. Así, aprovechando la tendencia de miles de personas que ofrecen por internet toda gama de productos que ya no usan, estos delincuentes con pleno conocimiento de la escasez de balones de oxígeno, la escasez de ciertos fármacos contra el COVID-19, la pérdida de empleos, el reparto de canastas y el pago de bonos a sectores vulnerables de la población colocan anuncios engañosos en páginas de tiendas virtuales inexistentes o crean páginas web falsas en donde ofertan muchos productos a precios por debajo del promedio que supuestamente entregarán a sus víctimas previo pago a través de la billetera electrónica o depósito en una cuenta bancaria.

Una vez recibido el pago a través de sus secuaces (drops), cortan toda comunicación, desactivan o bloquean la página para que el timado no deje comentarios negativos. Asimismo, ofrecen el reparto de canastas a domicilio, previo pago de una pequeña comisión; realizan falsas ofertas de trabajo en el sector privado y público, donde solicitan dinero a sus víctimas con la excusa del pago de derechos para hacer la búsqueda de antecedentes penales y corroboración de datos; se hacen pasar por organizaciones caritativas para

solicitar donaciones para personas enfermas de COVID-19; ofrecen realizar todo tipo de trámites para obtener el ansiado bono del Gobierno; y, simulando ser una empresa fintech, ofrecen préstamos online a bajas tasas de interés. Además, suelen utilizar el clickbait o anzuelo virtual para sus propósitos.

En diversos comunicados, la SBS ha alertado al público sobre este tipo de fraudes. Este organismo ha identificado entidades fraudulentas que, haciéndose pasar por entidades financieras, ofrecen préstamos, servicios financieros o esquemas de negocios que prometen grandes ganancias con la condición de que los interesados abonen previamente depósitos en cuentas bancarias (en el caso de los préstamos, por concepto de seguro de crédito, seguro de desgravamen o gastos), y una vez realizado el depósito, jamás cumplen con desembolsar los préstamos o realizar los servicios ofrecidos. En fin, los ciberdelincuentes tienen una creatividad monumental (Superintendencia de Banca, Seguros y AFP, 2018)

El objeto de nuestro análisis es destacar, entre las conductas típicas que utilizan como medio o como fin las TIC o el internet para apoderarse del patrimonio de sus víctimas, aquellas en las que prima el engaño o ardid del agente. Se debe tener en cuenta que este elemento se encuentra presente en las conductas fraudulentas de los delitos contra el patrimonio según nuestro CP. Por lo tanto, nada obsta para que en los delitos informáticos contra el patrimonio se incluya de lege ferenda cualquier medio o conducta fraudulenta en adición a los verbos rectores contemplados en el art. 8 de la LDI. Partimos del supuesto en donde el factor preponderante en la conducta típica del agente es el ardid o engaño y el empleo de internet y las TIC son el instrumento para hacerse del patrimonio de los sujetos pasivos.

En nuestro ejemplo, si no concurre uno de los verbos rectores del art. 8 de la LDI, dicha conducta tendría que subsumirse en los tipos básicos de estafa previstos en los arts.196 y 196-A del CP, pese a que se han empleado las TIC y/o el internet como medio comisivo. Además, no tendríamos las ventajas de la cooperación que prevé el Convenio de Budapest. Según este convenio los países signatarios son soberanos para adoptar las medidas legislativas necesarias para tipificar como delito toda tentativa deliberada de cometer un

delito informático y/o cualquier otro delito cometido por medio de un sistema informático. Las ventajas de actuar en consonancia con el Convenio de Budapest son evidentes, pues, al tratarse de un delito informático, se puede solicitar toda la cooperación internacional y la asistencia mutua posible

1.3.2.4. Propuesta de lege ferenda

Este estudio ofrece una propuesta de lege ferenda para que la forma básica del delito de estafa se incluya en la ley especial de delitos informáticos con el objeto de evitar vacíos de punibilidad en la conducta de los agentes delictivos que utilizan el ardid y el engaño en todas sus variantes para inducir a error a la víctima y hacer que se desprenda de su patrimonio. No es necesario que todos los verbos rectores del delito de estafa básica se encuentran descritos en el art. 8 de la LDI, basta añadir la frase “cualquier medio o conducta fraudulenta” para comprender todo el universo de fraudes y engaños.

Además, es necesario incluir la agravante de pluralidad de agentes, que se sancionará con pena privativa de libertad no menor cinco ni mayor de diez años, toda vez que estamos ante un delito de dominio en donde intervienen verdaderas organizaciones criminales que se distribuyen los roles para perpetrar sus fechorías. Obviamente, se debe tener en cuenta que el factor preponderante ha de ser el uso de las TIC o el internet, de lo contrario la conducta típica ha de reconducirse a la estafa básica.

Se ha esbozado una visión rápida del fraude informático y sus variantes a la luz de la teoría del delito y el bien jurídico protegido. Independientemente de cualquier opinión doctrinal que se pueda tener acerca del tema, estos ilícitos desbordan la soberanía de un Estado específico, es decir, se trata de un tema transfronterizo que requiere el apoyo y la colaboración de todos los gobiernos democráticos, máxime si se tiene en cuenta que nuestro país ha celebrado acuerdos de libre comercio con numerosos países, incluyendo la Unión Europea. Por ello, a la luz del Convenio de Budapest, resulta deseable propender un debate acerca de uniformizar reglas para combatir en forma eficaz el ciberdelito.

En ese orden de ideas, Balmaceda Hoyos18 afirma que, como es de público conocimiento, el desarrollo del internet ha conseguido almacenar una ingente base de datos sobre empresas e individuos a nivel mundial, información que puede ser utilizada con fines ilícitos por organizaciones delictivas de cualquier tipo. Así pues, se ha creado un mercado universal de acceso ilimitado. Existen diferentes percepciones y razones para regular las redes sociales y el internet. Un ejemplo de ello es el convenio que han firmado Facebook y el Gobierno de Australia, en el que se acuerda que este último pagará a Facebook por la difusión de noticias de dicho país. Podemos decir, entonces, que muchas facetas de la vida humana dependen hoy día de la tecnología de la información. Estas tecnologías se han ido perfeccionando a tal punto que constituyen uno de los adelantos más importantes de la última década. Así, cubren todo tipo de necesidades de empresas e individuos respecto a la obtención de bienes y servicios, y nos permiten conectarnos en forma instantánea con todo el mundo, situación que evita el aislamiento de antaño. Junto a estos factores beneficiosos, el desarrollo de la red de redes también ha traído consigo consecuencias inesperadas para, entre otros bienes jurídicos, la privacidad personal, puesto que estos avances también se utilizan con fines delictivos. La informática está presente en todos los campos de la vida moderna, todas las ramas del saber humano han adoptado las TIC, incluso el arte culinario, que antes resultaba impensable que pudiera robotizarse. Hoy tenemos máquinas que preparan comida para los comensales de una cadena de restaurantes en Singapur. Además, con el uso de la tecnología en telecomunicaciones 5G, se puede transmitir en contados segundos cualquier imagen, sonido o documento.

Por otra parte, en sus estudios sobre el desarrollo de los delitos en la red, Espinosa (2019), indica que las suplantaciones de identidad, los fraudes y los timos se han multiplicado en forma exponencial, sin que sea necesario el contacto físico con la víctima, debido a que las transferencias financieras y el comercio electrónico son blancos demasiado apetecibles para los ciberdelincuentes, quienes, escondiéndose en el anonimato, utilizan los puntos vulnerables de los sistemas de seguridad informáticos o el candor de ciertas víctimas para hacerse de cuantiosos botines.

Como sabemos, el desarrollo de las tecnologías de la información y las comunicaciones ha permitido una mejora en la productividad de las industrias, el comercio internacional, el flujo de capitales, el flujo de conocimientos, etc.; no obstante, este gigantesco crecimiento también ha traído consigo la aparición de nuevas modalidades de cibercrimen, circunstancia que obliga a los Estados a adherirse al Convenio de Budapest y, en consecuencia, adoptar un marco punitivo eficaz contra la cibercriminalidad. No hay que olvidar que la punición de estas conductas deberá realizarse siempre con observancia del debido proceso; v. gr.: en el caso del engaño propio del fraude, este debe ser relevante de acuerdo a la teoría de la imputación objetiva, sin dejar de lado los principios de lesividad, proporcionalidad y de ultima ratio propios de un Estado constitucional de derecho para enfrentar, prevenir y erradicar esta novísima forma de delinquir.

Estos nuevos métodos delictivos son difíciles de combatir debido a que enfrentarlos implica capacitar previamente a policías y fiscales en el manejo de los convenios de cooperación y el seguimiento de tecnologías digitales (las principales empresas cuyo levantamiento del secreto debe solicitarse tienen su sede en el extranjero y la data viene en inglés) (Vargas, 2021, p.98)

El Estado debe proveer de modernos equipos y software original para combatir con éxito el fraude, la estafa, la suplantación de identidad, la pornografía infantil, entre otros delitos. Estas especiales circunstancias y las carencias presupuestales han impedido descentralizar los servicios que brinda la División de Investigación de Delitos de Alta Tecnología de la Dirincri; sin embargo, la creación de la Unidad Especializada de ciberdelincuencia en el Ministerio Público abre una ventana de oportunidades para descentralizar ese servicio en las ciudades más densamente pobladas de nuestro país.

1.3.3. Análisis a la jurisprudencia

1.3.3.1. EXP. N.° 01189-2019-PHC/TC

El presente expediente investiga el delito de fraude informático y la falsificación de firma frente al imputado Marcos Morales Vargas bajo la

defensa del García Rosales W. quien interpone una demanda de habeas corpus contra lo interpuesto por los jueces Luis Antonio La Rosa Paredes, Gabino Alfredo Espinoza Ortiz y Andrés Avelino Cáceres Ortega, el cual la parte imputada solicita que la sentencia interpuesta por diez años de pena privativa de la libertad efectiva, las cuales están conformadas por 8 años del delito de fraude informático y 2 años pena privativa de libertad por el delito de documento se declare improcedente ya que la parte procesada ha sido sentencia con la Ley 30096, la cual no se encontraba en vigencia cuando ocurrieron los hechos, cabe señalar que los actos realizados con base a los delitos informáticos no se encontraban tipificados ya que los actos realizados por la personas investigadas fueron realizados desde el mes de Enero hasta Setiembre del 2013 el cual la Ley N° 30096 entro en vigencia en octubre del mismo año. El tribunal dijo que el principio del derecho penal también se definió como el derecho constitucional subjetivo de todos los ciudadanos. Como principio constitucional, notifica y limita el alcance de las prácticas restrictivas del legislador, así como el alcance de sus acciones al momento de determinar su sanción. Asegura, sin embargo, que la materia del poder subjetivo constitucional prevé las reglas preventivas, estrictas y escritas sobre lo que está prohibido a quien sea sometido a expediente disciplinario, y que las penas estén previstas previamente en el derecho normal.

1.3.3.2. Corte Superior de Justicia (Caso contra Katherine Flor Morales La Cruz)

La presente demanda investiga el delito de hurto sistemático contra el conocido Banco de Crédito, el cual El Juzgado Penal de Turno Permanente de la Corte Superior de Justicia de Lima Norte designo 9 meses de prisión preventiva para las investigaciones correspondientes la cual fue acusada por los delitos informáticos contra el patrimonio, el delito de fraude informático contra los sistemas y datos de dicha empresa bancaria y el acceso ilícito.

En el presente caso se sostiene el hurto de 1 millón 699 mil 990 dólares y 506 mil soles, la cual la parte demandada se defiende bajo los términos que la parte involucrada se encuentra bajo las enfermedades psicológicas y psiquiaticas, sin embargo, en el proceso de la investigación la parte demanda

acepto acogerse a la confesión sincera aduciendo que los actos realizados fueron realizados bajo las circunstancias de amenaza y coacción involucrando a sus hijos y los demás familiares. Finalizada la audiencia la parte demandante se encontró conforme con lo dispuesto por el Juzgado de Turno, mientras la defensa recurrirá al recurso de apelación.

1.3.3.3. Expediente Nº 1219-2003-HD/TC

El 21 de agosto de 2001 la recurrente interpuso una acción de Habeas data contra la Superintendencia de Banca y Seguros (SBS) el 18 de julio de 2001 por dar información rechazada mediante carta notarial. Los investigadores designados por el New World Bank (BNM) por la SBS violaron el acceso a los documentos porque no recibieron copias de los documentos presentados al Bank of America (BIF). Agregó que la orden incluirá una copia de algunos datos informáticos y una clave o código de acceso para la información del BNM que se les transmita.

El demandado alega que es mentira que Banco Nuevo Mondo (BNM) tenga una calidad del 99,9999% de sus acciones porque es infundado y el demandante no está autorizado a demandar. Esto se debe a que la propiedad y / o la legitimidad de hacer reclamos en el proceso no está clara. Agregó que BNM había sido golpeado por un sistema de interferencia solitario y especial, y que la negligencia de BNM incluso había llevado a la apertura de una causa penal contra el representante del Sr. NMH en el Trigésimo Séptimo Juzgado Penal de Lima. Jack Simon Levy Calvo por delitos contra las finanzas y la política monetaria.

El 14º Juzgado Popular de Lima el 12 de agosto de 2002 publicó los datos establecidos por habeas data se tiene en cuenta que el imputado no contaba con los documentos e informes requeridos en la carta de la página 9 y no cuestionaba la existencia del common law. El sistema financiero y el sistema de seguros u otras leyes restringen el ejercicio del derecho a solicitar información sobre la empresa en la que participa la agencia.

1.4. Formulación del problema

¿De qué manera incide la actualización de la legislación peruana frente al delito informático en la modalidad de phishing para tener una eficiente persecución y sanción penal?

1.5. Justificación e importancia

La investigación se ha generado por los nuevos incrementos de delitos informáticos, más aún en la modalidad de phishing, estos delitos que en su mayoría no se encuentra con una penalidad excepcional, dificultan el crecimiento de la población y del mercado cibernético por el robo de información, es así que para poder generar mayor protección se requiere que el delito de fraude informático sea actualidad con la finalidad de determinar la persecución penal e interponer una nueva sanción para poder llegar a contrarrestar el delito en sus diversas modalidad.

Además, debido a los ultimo realces de los métodos técnicos se a propiciado que en su mayoría de casos los más afectados fueron usuarios bancarios, es por ello que también es de necesidad que se tipifique las nuevas modalidades de fraude informático, con el fin de poder contrarrestar el delito e interponer una sanción adecuada, teniendo en cuenta el bienestar social cibernético y la protección jurídica de la norma.

La investigación tiene una finalidad legal de poder modificar la norma para que la persecución penal sea eficiente y para que la sanción vaya de acuerdo a acto ilícito cometido, es por ello que como fin busca que la modalidad de phishing sea incorporada como nuevo delito perteneciente al delito de fraude informático en donde se tipifique penalmente todo acto ilícito de robo cinético.

Así mismo se evidencia que en la mayoría de casos esta investigación va ayudar a poder delimitar el actor del delito y la interposición de la pena, pues también ayudara a los juzgadores penales para determinar la existencia de delito y la actuación penal del sujeto.

1.6. Hipótesis

Si se incorpora el artículo 8-A a la Ley de delitos informáticos entonces se obtendrá una mejor persecución y sanción penal para los delitos informáticos en la modalidad de phishing y sus parámetros delictivos ante el robo de información cibernética.

1.7. Objetivos

1.7.1. General

Aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad de phishing

1.7.2. Específicos

1. Identificar la aplicación de la pena y la sanción del delito de fraude informático
2. Analizar la nueva modalidad de phishing y su falta de incorporar en la legislación peruana
3. Determinar si la norma requiere una actualización legislativa frente a las nuevas modalidades de fraude informático
4. Proponer la actualización del delito de fraude informático ante la modalidad de phishing, para una eficiente persecución y sanción penal

II. MATERIALES Y METODOS

2.1. Tipo y diseño de investigación

Tipo: mixta – propositiva

La investigación mixta es un enfoque cuantitativo y cualitativo de ambas condiciones, eventos, personas, grupos o comunidades que se utiliza para describir y analizar la realidad de lo que se está abordando, así mismo en esta investigación se pretenderá actualizar la legislación que regula los

fraudes informáticos en su modalidad de phishing para la adecuada persecución y sanción penal. Del mismo modo la investigación es de tipo propositivo, debido a que existen lineamientos, los cuales permitirán dar una solución especifica al problema planteado a través de un aporte científico o practico. (Hernández, 2018, p. 10)

Diseño: no experimental

Puede definirse como una búsqueda realizada sin manipulación deliberada de variables. En otras palabras, se trata de estudios en los que no se varían intencionadamente las variables independientes para ver su efecto en otras variables. Lo que se hace en la investigación no experimental es observar o medir fenómenos y variables a medida que ocurren en su contexto natural, para analizarlos. En un experimento, el investigador prepara deliberadamente una situación para que están expuestos a diversos casos o individuos. (Hernández, 2018, p. 174)

2.2. Población y muestra

Población

Según el analista Hernández (2018), la población generalmente se refiere a un grupo de seres humanos que conforman la vida en un espacio o región geográfica específica. Es decir, generalmente se refiere a la población humana. (p. 235). La población en la presente investigación está conformada por los operadores del Derecho, llámense Abogados especialistas en el derecho penal, jueces y fiscales de la Ciudad de Chiclayo.

Muestra

Según Hernández (2018), la muestra es un conjunto de casos de la población, seleccionados por algún método racional, que siempre forma parte de la población. Si tiene una gran población, tiene muchas muestras. (p.235)

Para la determinación de la muestra se ha utilizado el muestreo no probabilístico, el cual no tiene en cuenta fórmulas para delimitar, sino que el investigador es quién la determina. Abogados especialistas en el derecho penal, jueces y fiscales de la Ciudad de Chiclayo, con un total de 50 informantes de la Ciudad de Chiclayo.

Tabla 1. Datos de los informantes según el cargo que desempeñan

Informantes	N.º	%
Abogados especialistas en derecho penal	41	82%
Jueces	3	6%
Fiscales	6	12%
Total, de informantes	50	100%

Fuente: elaborado por el investigador

2.3. Variables

Variable independiente

Fraude informático: Es todo acto realizado por una computadora o instrumento tecnológico que ayude a obtener o alterar datos electrónicos y a la vez es considerado como delito cibernético (Valle, 2017, p.52)

Variable dependiente

Phishing: Es considerado como todo método o acto que se encarga de engañar a una persona y hacer que comparta su clave o contraseña dentro de las actividades a realizar por medio de una computadora, esto sucede ya que este fraude informático se hace pasar como si fuera una entidad o institución de confianza a través de correos electrónicos (Paredes, 2017, p.34)

Tabla 2. Operacionalización de variables

Variables	Dimensiones	Indicadores	Ítem / Instrumento
V. Independiente **Fraude informático**	Ciberdelincuentes Ley N° 30096 Robo de identidad	Organizaciones criminales Manipulación de informática Información confidencial	Encuesta
V. Dependiente **Phishing**	Ciberdelincuencia Suplantación de identidad Fraude informático	Delito informático Correos electrónicos fraudulentos Estafa	

Fuente: elaborado por el investigador

2.4. Técnicas e Instrumentos de recolección de datos, validez y confiabilidad

2.4.1. Técnicas

Observación: Son un conjunto de técnicas y herramientas orientadas a evaluar un fenómeno, un individuo o un grupo de personas. Implican una manera de acercarse a la realidad del sujeto para conocerla. Generalmente se estudian conductas y comportamientos observables. (Hernández, 2018, p. 445)

La encuesta: Método utilizado para realizar este estudio fue una encuesta que consistió en una serie de preguntas sobre una o más variables medidas. (Hernández, 2018. p. 180)

Fichaje: Es una técnica utilizada especialmente por los investigadores. Es un modo de recolectar y almacenar información. Cada ficha contiene una serie de datos extensión variable pero todos referidos a un mismo tema, lo cual le confiere unidad y valor propio. (Hernández, 2018, p. 86)

Análisis Documental: técnica que busca reconocer, recibir y consultar de manera selectiva la biografía y otros materiales que difieran de otros conocimientos y / o información recopilada solo moderadamente de la realidad para que puedan ser útiles para el propósito del estudio. (Hernández, 2018, p. 85)

Técnica de gabinete

El nombre de esta técnica se toma de las reuniones de ministros, guías o directores. La discusión de gabinete tiene como objetivo tratar un tema o problema de especial importancia, entre un grupo de alumnos con determinadas responsabilidades y con el fin inmediato de tomar una decisión. (Hernández, 2018, p. 86)

2.4.2. Instrumentos

Cuestionario: Herramienta de recolección de datos más utilizada, que consiste en una serie de preguntas sobre una o más variables a medir, las cuales deben ser consistentes con la formulación del problema y los supuestos bajo los cuales se utilizan en investigaciones de todo tipo. (Hernández, 2018, p. 250)

Ficha textual: Consiste en identificar, obtener y consultar bibliografías y otros materiales que puedan ser de utilidad para los fines del estudio, así como obtener y recabar información relevante y necesaria relacionada con nuestro problema de investigación. (Hernández, 2018, p. 86)

Ficha bibliográfica: esta investigación aplica fichas para poder indagar y estudiar las leyes y los artículos jurídicos en función al problema planteado (Hernández, 2018, p. 87).

Ficha hemerográfica: es una ficha que se encarga de buscar características peculiares del problema durante las publicaciones recientes, a través de un hallazgo de cualquier medio impreso (Hernández, 2018, p. 87)

Ficha de resumen: guarda información concreta a través de resúmenes personal, donde lo principal consta de lo expresado por el autor en función a la investigación (Hernández, 2018, p. 88)

Ficha paráfrasis: es una interpretación de lo que menciona en autor, esta se plasma con la idea del lector buscando una mejor interpretación en base a la investigación (Hernández, 2018, p. 88)

2.5. Procedimientos de análisis de datos

La recopilación de datos es esencial, pero no se utiliza para medir variables, sacar conclusiones y realizar análisis estadísticos. Estamos intentando obtener

datos (que se convierten en información). Se recopilan para analizarlos y comprenderlos, responder preguntas de investigación y generar conocimiento. Y generalmente, estos datos se expresan en historias de diferentes tipos: escritas, verbales, visuales (como fotos e imágenes), acústicas (sonidos y grabaciones de audio), audiovisuales (por ejemplo, video), artefactos, etc. (Hernández, 2018, p. 443)

2.6. Criterios éticos.

a. **Dignidad Humana:** Se considerará que los expertos siguen los pasos del Informe Belmont para actualizar la legislación que regula los fraudes informáticos en su modalidad de phishing para la adecuada persecución y sanción penal.

b. **Consentimiento informado:** Se le dio una explicación inicial a través de la encuesta, que requirió la firma de quienes expresaron su consentimiento para establecer una adecuada persecución y sanción penal frente a los fraudes informáticos en su modalidad de phishing.

c. **Información:** Con la información rescatada de libros físicos y virtuales se logra la finalidad y el propósito de la investigación con respecto a la búsqueda de participación de expertos.

d. **Voluntariedad:** Este punto es el más importante ya que es la ayuda de los participantes a través de la encuesta para poder colaborar con la investigación con su opinión y así llegar actualizar la legislación que regula los fraudes informáticos en su modalidad de phishing para la adecuada persecución y sanción penal.

e. **Beneficencia:** A través de este punto, se informó a los expertos sobre los beneficios que traerían los resultados de esta investigación, es decir, los riesgos que surgieron durante la investigación también se tuvieron en cuenta.

f. **Justicia:** El estudio parece apropiado porque beneficiará directamente al estado de peruano y la seguridad de la sociedad en su conjunto.

2.7. Criterios de Rigor Científico

Fiabilidad: consiste en la estabilidad de la puntuación que proporciona cuando se administra repetidamente al mismo grupo de personas. Un supuesto implícito en el estudio de la confiabilidad es la estabilidad de la variable a medir.

Muestreo: Se dice que esta investigación toma en cuenta la veracidad científica, por un lado, por otro lado, el muestreo, que es cualquier acto de investigación en el que se utilizan libros e informes, que puede ser un ejemplo de la población para recolectar información.

Generalización: Es un elemento fundamental de la lógica y el razonamiento humanos. Esta es la base esencial para cualquier conclusión válida de deducción. El concepto general se usa ampliamente en muchas disciplinas, a veces con un significado específico según el contexto de la investigación.

Validez: este criterio busca establecer un instrumento de medición que al compararlo con algún criterio externo que pretende medir lo mismo, siendo uno de los más importantes debido a la confiabilidad de la investigación.

Credibilidad: Son los hallazgos verdaderos que se tiene ante el estudio y lo experimentado con la investigación, es decir es la naturaleza de los datos en base a lo investigación y al estudio experimental.

Auditabilidad: Se hace referencia a la forma que el investigador quiere para poder cumplir el objetivo, ante ello es necesario que la documentación presente estudios de ideas esencial que guarden relación con el problema.

III. RESULTADOS

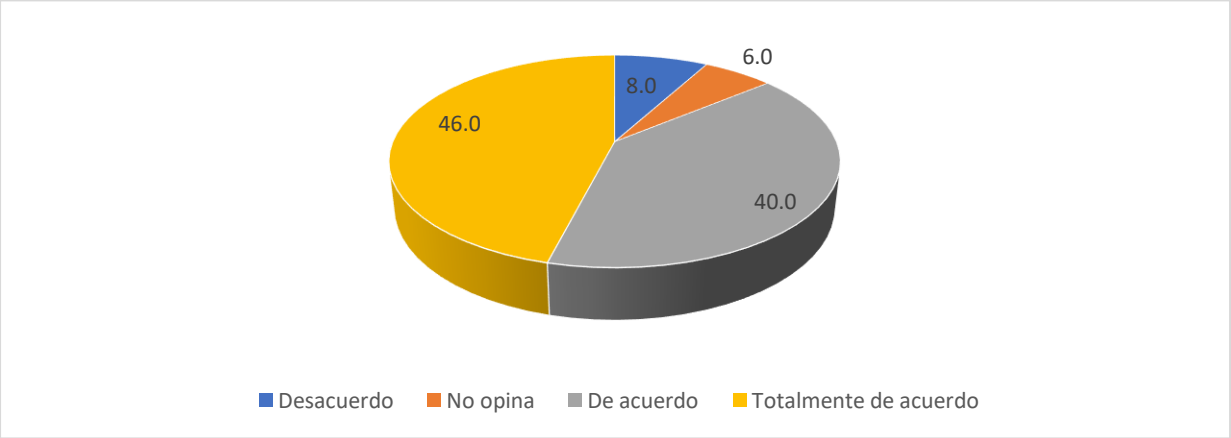
3.1. Resultados en tablas y figuras

Tabla 3. ***Fraude informático en modalidad de Phishing.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	4	8.0
No opina	3	6.0
De acuerdo	20	40.0
Totalmente de acuerdo	23	46.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 1. Fraude informático en modalidad de Phishing.



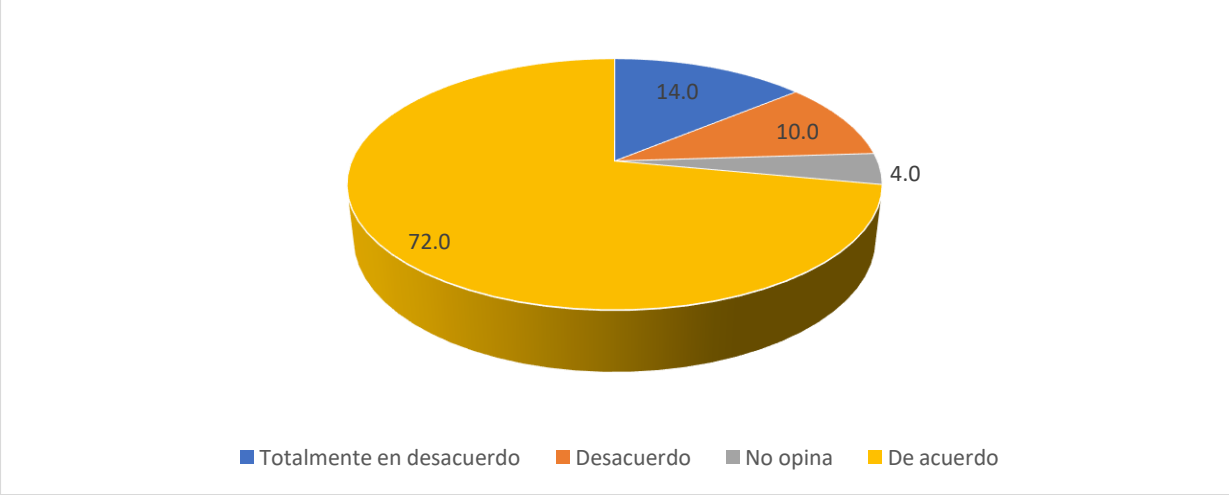
Nota: El 46% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo que el fraude informático en modalidad de Phishing, necesita una adecuada legislación, de igual forma se tiene otro resultado favorable que es el 40% de la población expresan estar de acuerdo, sin embargo, por otro lado, se tiene al 8.0% que expresan estar en desacuerdo y como último resultado se tiene al 6.0% que prefieren no expresar su opinión sobre el tema.

Tabla 4. ***Normatividad del estado peruano.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	7	14.0
Desacuerdo	5	10.0
No opina	2	4.0
De acuerdo	36	72.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 2. Normatividad del estado peruano.



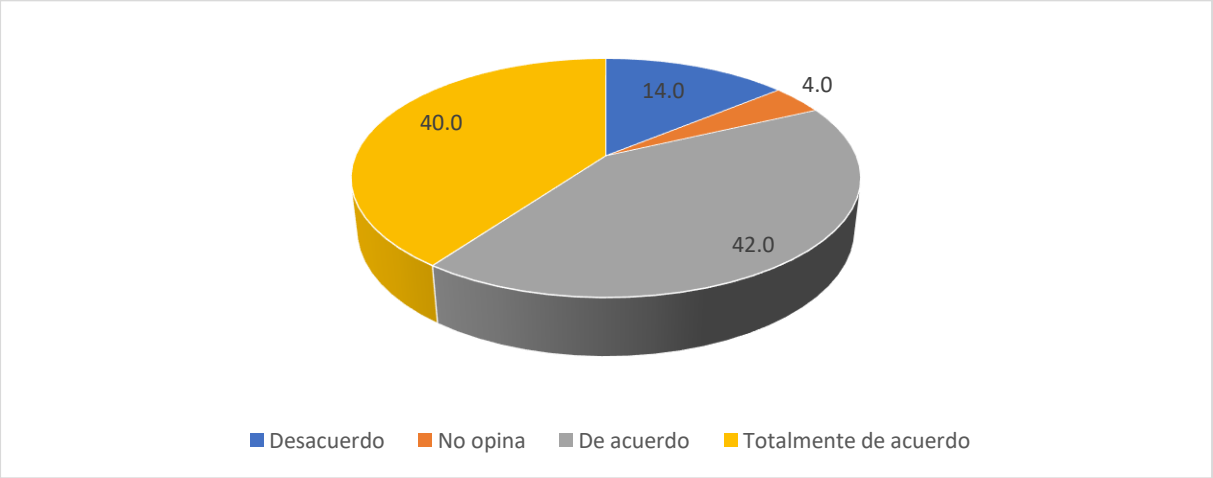
Nota: El 72% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar de acuerdo que, la normatividad del estado peruano no presenta una legislación eficiente frente al fraude informático en modalidad de Phishing, por otra parte, se tiene al 4.0% de la población que prefieren no expresar su comentario, sin embargo, como últimos resultados se tiene al 10% de la población que expresan estar en desacuerdo y el 14% de los encuestados están en total desacuerdo.

Tabla 5. ***Análisis de la legislación peruana.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	7	14.0
No opina	2	4.0
De acuerdo	21	42.0
Totalmente de acuerdo	20	40.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 3. Análisis de la legislación peruana.



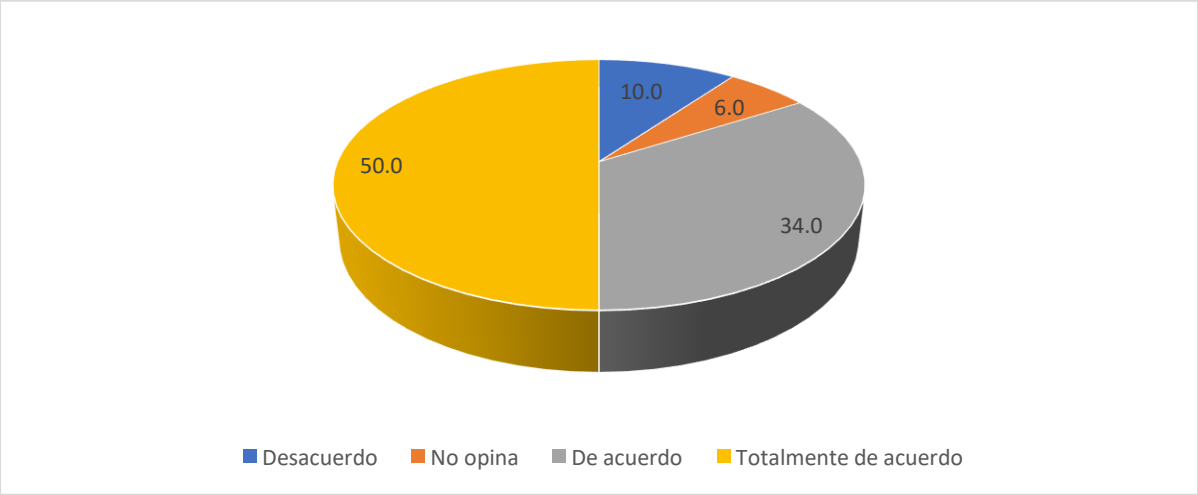
Nota: El 42% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar de acuerdo que es necesario un adecuado análisis de la legislación peruana frente al fraude informático en modalidad de Phishing, de igual forma se tiene otro resultado favorable que es el 40% de los especialistas que manifiestan estar totalmente de acuerdo, por otra parte, existe un 4.0% que prefieren no expresar su opinión, dejando como último resultado negativo al 14% establece estar en total desacuerdo.

Tabla 6. ***Sanción penal del delito de Phishing.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	5	10.0
No opina	3	6.0
De acuerdo	17	34.0
Totalmente de acuerdo	25	50.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 4. Sanción penal del delito de Phishing.



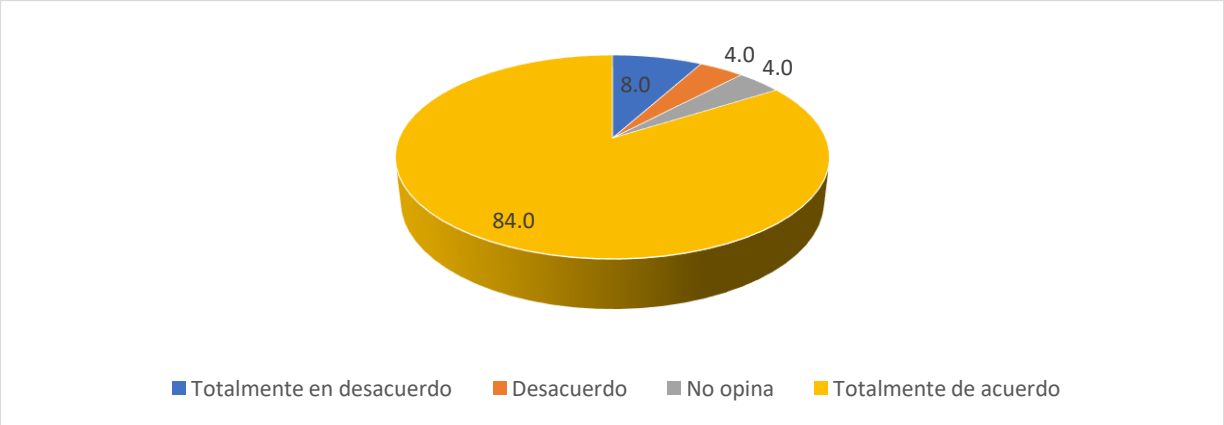
Nota: El 50% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo que no existe una adecuada sanción penal del delito de Phishing, así mismo otro resultado favorable para la investigación es el 34% de los encuestados que expresan estar de acuerdo, por otra parte, existen un 6.0% que prefieren no expresar su opinión, dejando como último resultado al 10% de los encuestados que establecen estar en desacuerdo.

Tabla 7. ***Derechos fundamentales de las personas perjudicadas.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	4	8.0
Desacuerdo	2	4.0
No opina	2	4.0
Totalmente de acuerdo	42	84.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 5. Derechos fundamentales de las personas perjudicadas.



Nota: El 84% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo en que el delito de Phishing vulnera directamente los derechos fundamentales de las personas perjudicadas, por otra parte, se tiene al 4.0% de la población que prefieren no expresar su comentario, dejando como resultados negativos al 4.0% que expresan estar en desacuerdo y por último se tiene al 8.0% de los encuestados que expresan estar en total desacuerdo

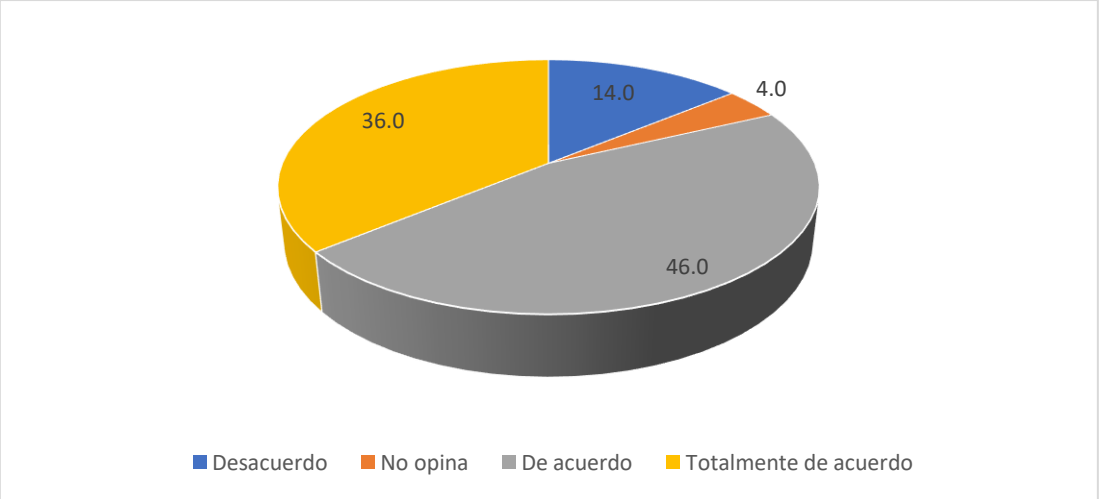
.

Tabla 8. ***Delito de Phising.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	7	14.0
No opina	2	4.0
De acuerdo	23	46.0
Totalmente de acuerdo	18	36.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 6. Delito de Phising.



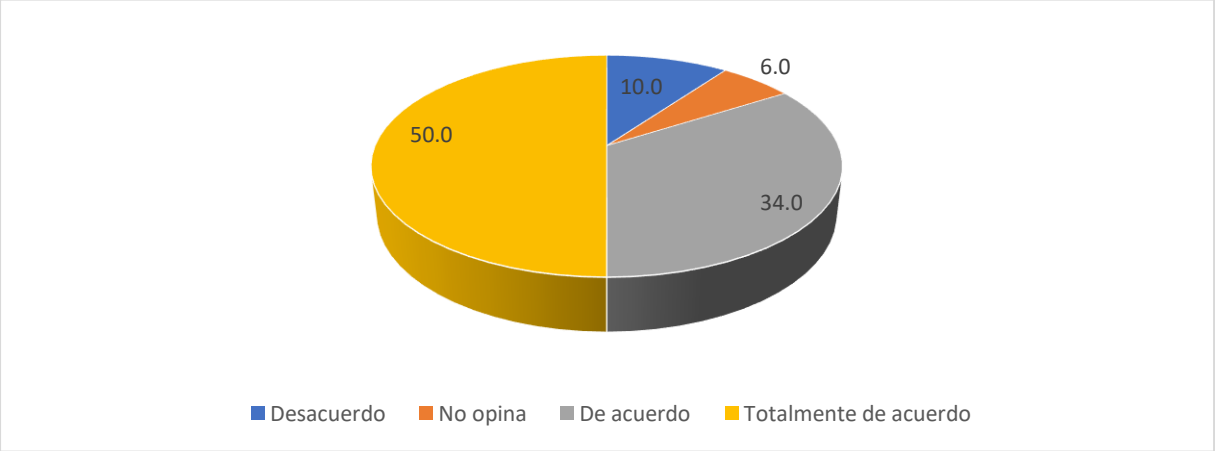
Nota: El 46% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar de acuerdo que los actos ocasionados por el delito de Phising sigue siendo impunes, así mismo otro resultado favorable para la investigación es el 36% de los encuestados que expresan estar totalmente de acuerdo, sin embargo por otra parte se tiene dos resultados distintos el cual el primero es el 4.0% que prefieren no opinar sobre el tema y dejando como último resultado al 14% que están en desacuerdo.

Tabla 9. ***Falta de mecanismos electrónicos.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	5	10.0
No opina	3	6.0
De acuerdo	17	34.0
Totalmente de acuerdo	25	50.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 7. Falta de mecanismos electrónicos.



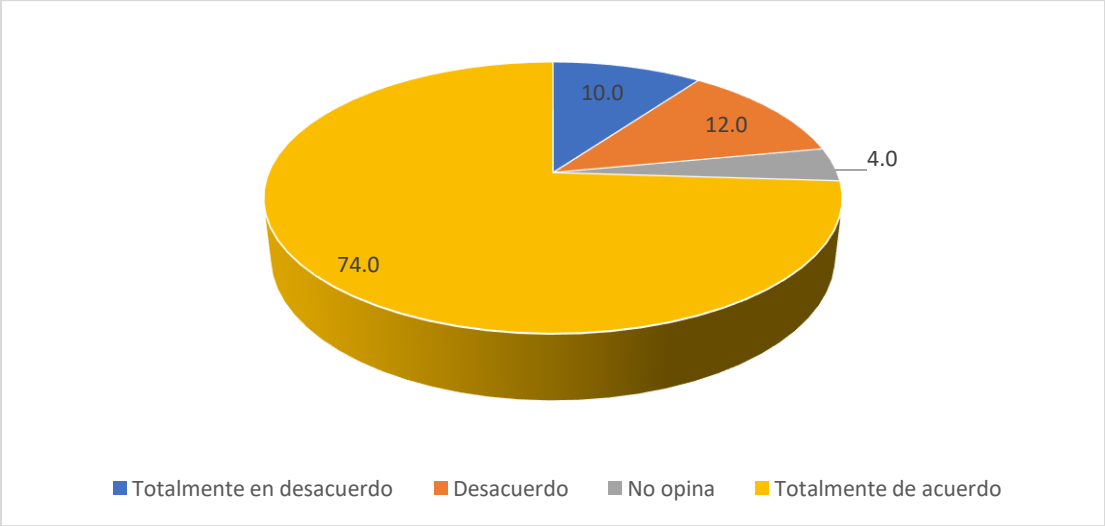
Nota: El 50% de los Abogados especialistas en derecho penal, Jueces y Fiscales, expresan estar totalmente de acuerdo que el delito de Phising es un delito que queda impune por la falta de mecanismos electrónicos para la eficaz persecución y sanción penal, de igual forma se tiene un resultado similar con el 34% que expresan estar de acuerdo, por otra parte, existe un 6.0% que prefieren no opinar sobre el tema, dejando como último resultado restante al 10% que expresan estar en desacuerdo.

Tabla 10. ***El estado peruano deba adherirse a convenios internacionales.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	5	10.0
Desacuerdo	6	12.0
No opina	2	4.0
Totalmente de acuerdo	37	74.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 8. El estado peruano deba adherirse a convenios internacionales



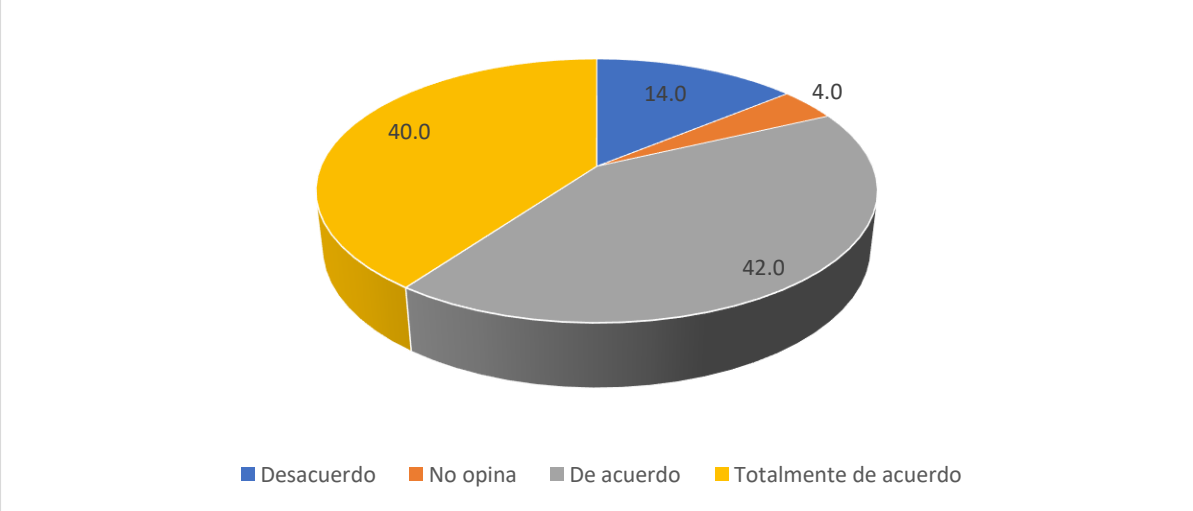
Nota: El 74% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo que el estado peruano deba adherirse a convenios internacionales con el objetivo de luchar adecuadamente contra el delito de Phishing, por otra parte, se tiene al 4.0% de la población que prefieren no expresar su opinión sobre el tema, dejando como últimos resultados al 12% que están en desacuerdo y el 10% que expresan estar totalmente en desacuerdo.

Tabla 11. ***Ineficiencia normativa peruana.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	7	14.0
No opina	2	4.0
De acuerdo	21	42.0
Totalmente de acuerdo	20	40.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 9. Ineficiencia normativa peruana.



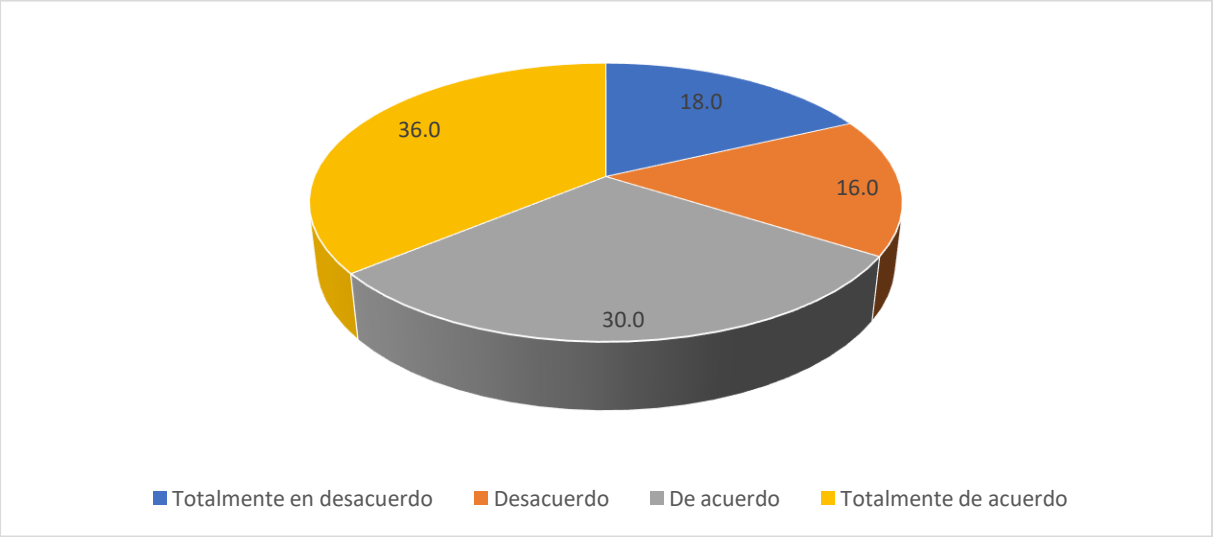
Nota: El 42% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo que por la ineficiencia normativa peruana el delito de Phishing se siguen realizando actos impunes, de igual forma se tiene un resultado favorable que es el 40% que expresan estar de acuerdo, por otra parte, se tiene al 4.0% de la población que prefieren no expresar su opinión, dejando como último resultado al14% que expresan estar en desacuerdo.

Tabla 12. ***Delito de Phishing.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	9	18.0
Desacuerdo	8	16.0
De acuerdo	15	30.0
Totalmente de acuerdo	18	36.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 10. Delito de Phishing.



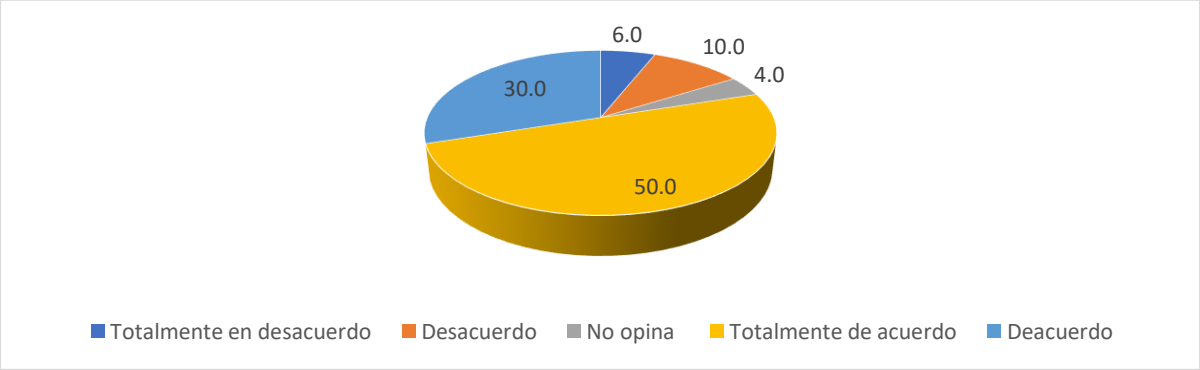
Nota: El 36% de los Abogados especialistas en derecho penal, Jueces y Fiscales, expresan estar totalmente de acuerdo que el delito de Phishing está constituido como un peligro en crecimiento en contra de la sociedad, de igual manera se tiene un resultado favorable que es el 30% que manifiesta estar de acuerdo, por otra parte, existe un 16% de la población que expresan estar en desacuerdo y el 18% restante expresan estar en total desacuerdo.

Tabla 13. ***Vacíos legales.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	3	6.0
Desacuerdo	5	10.0
No opina	2	4.0
Totalmente de acuerdo	25	50.0
Deacuerdo	15	30.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 11. Vacíos legales.



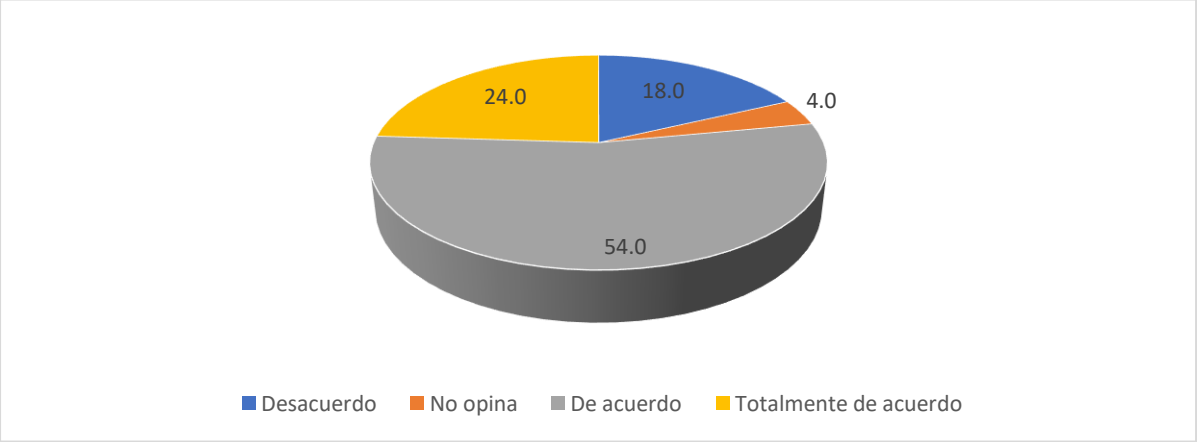
Nota: El 50% de los Abogados especialistas en derecho penal, Jueces y Fiscales, expresan estar totalmente de acuerdo que se deban identificar y subsanar los vacíos legales existente en la normatividad peruana frente al fraude informático del delito de Phishing, de igual forma se tiene al 30% que establecen estar de acuerdo con la correcta identificación de los vacíos legales, por otra parte existe un 4.0% que prefieren no opinar sobre el tema, dejando como últimos resultados al 6.0% totalmente en desacuerdo y el 10% que están en desacuerdo.

Tabla 14. ***Índice de actos impunes.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	9	18.0
No opina	2	4.0
De acuerdo	27	54.0
Totalmente de acuerdo	12	24.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 12. Índice de actos impunes.



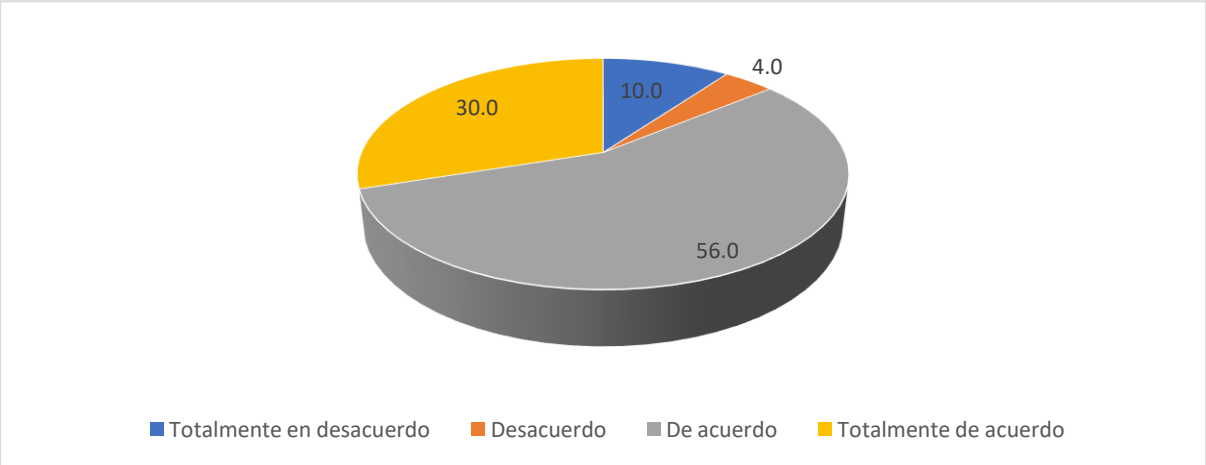
Nota: El 54% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar de acuerdo en que el fraude informático en modalidad de delito de Phishing tiene un gran índice de actos impunes y el estado peruano no aplica mecanismos jurídicos para afrontarlos, de igual forma otro resultado favorable para la investigación es el 24% de la población que expresan estar totalmente de acuerdo con la premisa establecida, por otro lado se tiene al 4.0% de los encuestados prefieren no expresar su comentario, dejando así al último resultado que es el 18% de la población que expresan estar en desacuerdo.

Tabla 15. ***Análisis a los criterios legales de la imputación penal.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	5	10.0
Desacuerdo	2	4.0
De acuerdo	28	56.0
Totalmente de acuerdo	15	30.0
De acuerdo	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 13. Análisis a los criterios legales de la imputación penal.



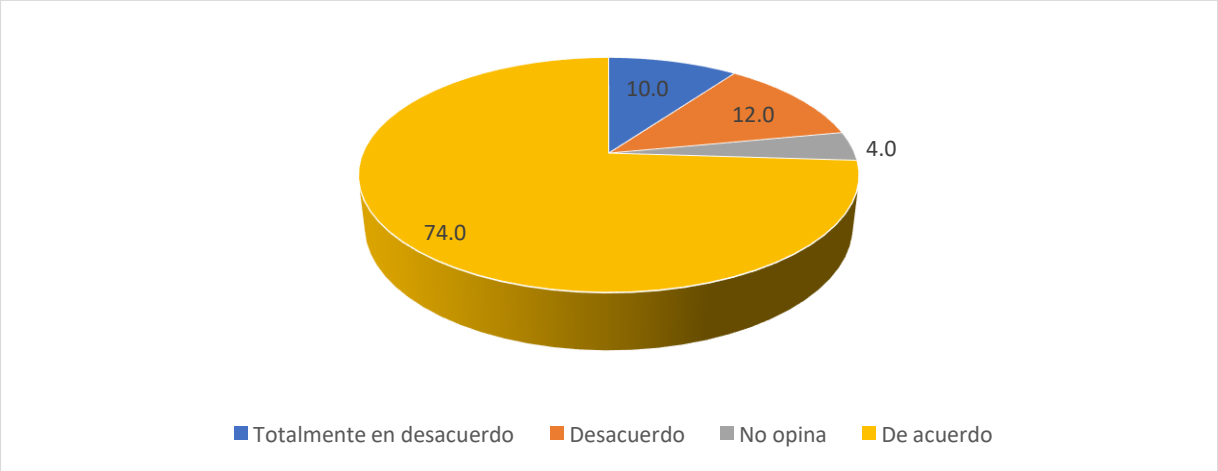
Nota: El 56% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar totalmente de acuerdo que se deba realizar un adecuado análisis a los criterios legales de la imputación penal del delito de Phishing, así mismo otro resultado favorable es el 30% que expresan estar de acuerdo, sin embargo, se tiene como resultado negativo se tiene al 4.0% que expresan estar desacuerdo y al 10% que manifiestan estar totalmente en desacuerdo.

Tabla 16. ***Operadores de justicia.***

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	5	10.0
Desacuerdo	6	12.0
No opina	2	4.0
De acuerdo	37	74.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 14. Operadores de justicia.



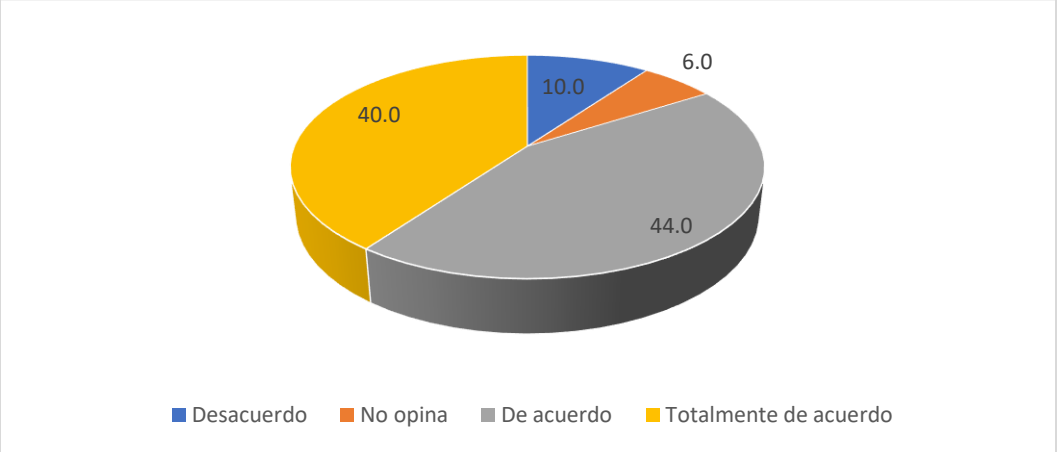
Nota: El 74% de los Abogados especialistas en derecho penal, Jueces y Fiscales, manifiestan estar de acuerdo en que el estado peruano deba capacitar adecuadamente a los operadores de justicia para la adecuada imputación penal el delito de Phishing, por otro lado, se tiene un resultado imparcial que es el 4.0% de la población que prefieren no opinar sobre el tema, dejando así al 12% que están en desacuerdo y como último resultado al 10% que está en total desacuerdo.

Tabla 17. ***Presupuesto anual.***

Descripción	Frecuencia	Porcentaje
Desacuerdo	5	10.0
No opina	3	6.0
De acuerdo	22	44.0
Totalmente de acuerdo	20	40.0
Total	50	100.0

Nota: Encuesta aplicada Abogados especialistas en derecho penal, Jueces y Fiscales.

Figura 15. Presupuesto anual.



Nota: El 44% de los Abogados especialistas en derecho penal, Jueces y Fiscales, expresan estar totalmente de acuerdo que el estado deba invertir anualmente presupuesto para mejorar la tecnología para combatir el delito de Phishing, así mismo otro resultado similar con el 40% que expresan estar de acuerdo, por otra parte 6% de los encuestados prefieren no expresar su opinión sobre el tema, dejando así al 10% de la población expresar que están en desacuerdo.

3.2. Discusión de resultados

Teniendo en cuenta el objetivo general que busca aplicar una correcta actualización de la legislación peruana para obtener una eficiente persecución y sanción penal ante el delito de fraude informático en la modalidad de phishing, es por ello que se tomara en cuenta lo establecido en la figura N°2 el cual señala que el 72% de los especialistas en derecho penal están de acuerdo en que la normatividad peruana no presenta una adecuada legislación frente al fraude informático dando a entender que es ineficiente la actual legislación, por otra parte se tiene al 4.0% de la población encuestada que prefieren no opinar sobre el tema expuesto, dejando así como últimos resultados al 10% de la población manifestando estar en desacuerdo y el 14% de la población restante están totalmente en desacuerdo. Conforme a los resultados obtenidos se puede evidenciar que la legislación peruana es considerada ineficiente ante los actos ilícitos de fraude informático en la modalidad de phishing, es por ello que mediante lo obtenido en la encuesta se puede establecer la necesidad de una adecuada actualización normativa. Es por ello que al compararlo con lo investigado por Valle (2017), en el concluye que en el estado ecuatoriano es considerado ilegal, sin embargo, no se encuentra tipificado correctamente generando así que las personas que tengan conocimientos informáticos incurran en realizar actos impunes obtenido de una manera ilícita beneficios económicos y entre otros aspectos que afectan directamente el bienestar de las personas que se les vulnera sus derechos. De acuerdo a lo obtenido por la encuesta y lo citado por el autor Valle, se puede establecer que a nivel nacional e internacional el delito de phishing es un acto delictivo que hasta el momento no se ha logrado combatir adecuadamente, ocasionando que gente inescrupulosa cometan estos actos ilícitos vulnerando así el bienestar de la sociedad.

Prosiguiendo con los objetivos especifico se tendrá en cuenta el primero que es identificar si existe una correcta aplicación de la pena y una adecuada sanción

del delito de fraude informático, es por ello que se comparara con lo obtenido en la figura N° 11, el cual establece que el 50% de los especialistas que han sido encuestados manifiestan estar totalmente de acuerdo en que se deba realizar una adecuada identificación y subsanar los vacíos legales que existen en la normatividad peruana frente al delito de Phishing, así mismo otro resultado beneficioso para la investigación es el 30% de los encuestados que manifiestan estar de acuerdo con la pregunta establecida, dejando así un 4.0% de la población que prefieren no opinar sobre el tema mencionado, sin embargo se tienen 2 resultados negativos el cual el primero es el 6.0% que expresan estar totalmente en desacuerdo con la pregunta aplicada y el 10% restante expresan estar en desacuerdo. Estos resultados al compararlo con lo sustentado por Herrera (2016) el cual señala que el delito informático en el estado ecuatoriano no se encuentra tipificado, el cual genera una desprotección directa de los ciudadanos, afectando así directamente sus derechos fundamentales es por ello que las tecnologías sociales, de la información y la comunicación se han desarrollado como un elemento de convivencia humana y relaciones sociales, y estos comportamientos han resultado de acciones que violan la propiedad legítima, como la privacidad personal y los derechos de propiedad, en acciones ilegales recurrentes. De acuerdo a lo obtenido por ambas partes tanto por lo sustentado por el autor y lo obtenido por la encuesta es claro la necesidad de identificar si existe una correcta aplicación de la norma, es por ello que a través del alto índice de actos ilícitos de phishing se puede establecer que existe vacíos legales en la norma, desprotegiendo directamente a la sociedad.

Continuando con los objetivos especifico tendremos en cuenta el que busca determinar que mediante las nuevas modalidades de fraudes informático la legislación peruana necesita una correcta actualización, que al compararlo con lo establecido en la figura N° 4, el cual establece que el 50% de los especialistas en el derecho penal expresan estar totalmente de acuerdo que en la actualidad

no existe una adecuada sanción penal frente al delito de phishing, así mismo otro resultado favorable es el 34% de las personas encuestadas que manifiestan estar de acuerdo, por otra parte, existen un 6.0% que prefieren no expresar su opinión, dejando como último resultado al 10% de los encuestados que establecen estar en desacuerdo. Estos resultados dan entender que hoy e día con el avance tecnológico se han incrementado distintas modalidades de fraude informático, afectando directamente a la sociedad, es por ello que al compáralo con lo sustentado Paredes (2017) el cual señala que los intereses comunes de los usuarios de redes sociales comunes pueden determinar su expansión y, según la información bancaria, ahora es más fácil de manejar por teléfono porque las redes sociales son una nueva comunicación. La información bancaria es confidencial para el cliente de una institución financiera y los piratas informáticos la utilizan para cometer delitos informáticos. Esto quiere decir que hoy en día la tecnología ha ocasionado que se mejore y se reduzca el tiempo de cualquier transacción a realizar, sin embargo, estos avances tecnológicos también han ocasionado que se incrementen los actos ilícitos, es por ello la necesidad que la normatividad peruana se actualice adecuadamente con el transcurrir de los años con el objetivo de disminuir exponencialmente estos actos delictuosos.

Para finalizar tendremos en cuenta la propuesta de una actualización normativa del delito de fraude informático ante la modalidad de phishing, con el propósito de una correcta persecución y sanción penal, es por ello que al compararlo con el resultado de la figura N° 13 el cual señala que el 56% de los especialistas en el derecho penal expresan estar totalmente de acuerdo en que se deba realizar un adecuado análisis frente a los criterios legales de imputación penal ante el delito de phishing, de igual forma existe un 30% que expresan estar de acuerdo, sin embargo, se tiene como resultado negativo se tiene al 4.0% que expresan estar desacuerdo y al 10% que manifiestan estar totalmente en desacuerdo. Es claro dar a conocer que el estado peruano necesita no presenta adecuados

criterios legales con el objetivo de contrarrestar los actos ilícitos que quedan impunes. Es por ello que al compararlo con lo sustentado por Mengoa (2021), el cual concluye que el phishing es uno de los principales delitos del fraude en Internet en la actualidad, con información obtenida por el usuario y parodizándolo a través de diversos medios como instituciones de banca online, servicios de pago online y acceso a diversas redes sociales. Conforme a lo establecido en las discusiones anteriores se puede evidenciar que el estado peruano le hace falta una correcta actualización de norma que regula los fraudes informáticos, ya que no afronta directamente este delito que perjudica de una y mil maneras a la ciudadanía.

3.3. Aporte practico

3.3.1. Fundamentación del aporte práctico

En el mundo el avance de la tecnología ha generado de que los robots, la inteligencia artificial y el aprendizaje de las maquinas evolucionen a un paso veloz, dejando mucho de las posibilidades en tela de juicio ante un modelo tradicional, pues todas estas medidas avanzadas facilitan la vida de la persona y mejorar sus relaciones personales y laborales, sin embargo se puede percatar que este avance ha traído consigo varios problemas que afectan a la sociedad principalmente ante su privacidad, debido a que se han generado diversos robos informáticos que han perjudicado la integridad personal, más aun cuanto este tipo de delitos no se encuentra tipificado o actualizado en la norma (Darrell, 2016).

En este contexto, se centra aquí en los aspectos específicos del fraude informático, pues estos incluyen ataques a la integridad y confidencialidad de los datos personales, así como a los activos bancarios y la confianza del titular y la

seguridad del sistema financiero para realizar todo tipo de transacciones civiles y comerciales.

La norma anterior fue modificada de acuerdo con la Ley 30171, publicada en 2014, que prohíbe el acceso no autorizado (artículo 2), los ataques a la integridad de los datos y sistemas informáticos (artículos 3 y 4) y la incautación de datos informáticos (artículo 7), incluido el fraude (artículo 8) y el abuso de los mecanismos y dispositivos informáticos (artículo 10) afirman las palabras “a sabiendas e ilícitamente” que los delitos se han cometido indebidamente y se ha derogado el artículo 6, que se refiere al movimiento ilegal de información (Zevallos, 2020).

Frente a esta normativa el artículo en análisis es el 8 considerado como fraude información, pues a través de esta modalidad, se han presentado diversos medios de robo de información, uno de ellos es el phishing, considerado como un modelo de engaño que se genera con la finalidad de poder robar información bancaria para poder atentar contra el patrimonio de la persona, para ello se presentan diversas paginas falsas, las cuales se presentan en los bancos o en las entidades financieras.

Es así que, ante las restricciones, en la actualidad, la Ley de №. 30096, “Ley de Delitos Informáticos” es de particular importancia, un estándar específico de traición penal que se aplica a los sistemas informáticos y de información, la indemnización y la libertad sexual, la confidencialidad y el secreto de la comunicación, el patrimonio y las creencias públicas en las que se utilizó la Tecnología Criminal, ante la comisión de los diversos delitos penales.

E aquí el problema de información en donde se evidencia que dentro del fraude informático no existe una distinción penal entre la modalidad de fraude y la modalidad de phishing, pues este estos casos la modalidad debería ser distinta

por el hecho de que debería haber mejor persecución penal y la sanción debería ser mayor que el de la pena interpuesta.

Ante esta situación, el Ministerio de Asuntos Públicos se ha propuesto desarrollar un estudio descriptivo reconociendo las fortalezas y debilidades del Estado en el abordaje de estos desafíos de política pública, con datos policiales y tributarios, tanto cualitativos como cuantitativos. Como aporte teórico y normativo, los lineamientos y recomendaciones de la Convención de Budapest, suscrita por el gobierno peruano en 2019, y las definiciones y disposiciones de la Ley de Delitos Informáticos (Ley N ° 30096), que se encuentran vigentes desde 2013, fueron tenido en cuenta (Ministerio Público, 2020).

Finalmente se comprende que la mayor en la que se presenta el delito es a través de mensajes de textos los cuales son publicados por medio de las redes sociales, pues se comprende que este tipo de delitos roba la información necesaria y bancaria de la víctima, es así que se comprende que de todas las denuncias presentadas por los delitos informáticos de la Divindat la mayor parte se genera por el fraude informático (Andina, 2020).

Corroboración del aporte practico

Proyecto de Ley N° …….

PROPUESTA LEGISLATIVA QUE INCORPORA EL ART. 8-A EN LA LEY 30096 PARA PENALIZAR LA MODALIDAD DE PHISHING EN EL DELITO DE FRAUDE INFORMÁTICO

El estudiante de la carrera de Derecho de la Universidad Señor de Sipán, ejerciendo el Derecho de iniciativa Legislativa que confiere el Articulo N. ° 107 de la Constitución Política del Perú, y conforme a lo establecido en el Artículo 75° y 76° del Reglamento del Congreso de la República, presenta la siguiente propuesta legislativa

FORMULA LEGAL

LEY QUE INCORPORA EL ART. 8-A EN LA LEY 30096 PARA PENALIZAR LA MODALIDAD DE PHISHING EN EL DELITO DE FRAUDE INFORMÁTICO

Artículo 1.- Objeto

Incorporación del art. 8-A en la Ley 30096, Ley de delitos informáticos, para penalizar la modalidad de phishing en el delito de fraude informático.

Artículo 2.- Modificatoria

Modifíquese e incorpórese en el artículo en mención:

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, 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.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

Incorpórese:

Artículo 8-A.- Phishing

El que aplica estrategias engañosas para introducir al usuario a realizar un acto de disposición en su perjuicio, a través del uso de las tecnologías de la información o de la comunicación, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de siete años y con sesenta a ciento veinte días multa

DISPOCISIONES COMPLEMENTARIAS

Primera: Adecuación de normas La presente ley se adecuará a la normativa nacional, en un plazo no mayor de 60 días calendarios.

Segundo: Vigencia La presente ley entrara en vigencia al día siguiente de su publicación. Comuníquese al Señor presidente de la Republica para su promulgación.

CONCLUSIONES DE LA PROPUESTA

La incorporación del phishing dentro de la ley ayuda a poder delimitar las nuevas modalidades de fraude informático que se presenta, más aún con el avance de la tecnología dentro de la actual situación pandémica, pues se analiza que esta incorporación permitirá delimitar el acto ilícito e identificar el agente ante la modalidad de robo informático.

ANÁLISIS COSTO BENEFICIO

Esta propuesta no genera costos para el Estado, sino por el contrario, busca poder modificar la norma para que la persecución penal sea eficiente y para que la sanción vaya de acuerdo a acto ilícito cometido, es por ello que como fin busca que la modalidad de phishing sea incorporada como nuevo delito perteneciente al delito de fraude informático en donde se tipifique penalmente todo acto ilícito de robo cinético

IV. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1) De acuerdo a la actualización realizada a la legislación que regula los delitos informáticos se logró obtener una eficiente persecución y sanción penal frente al delito de fraude informático en modalidad de phishing, ya que es evidente que los actos realizados por el fraude informático quedaban impune, por el tan solo hecho de no encontrar a las personas que realizan estos actos que perjudican directamente a la sociedad, dejando así una brecha para que otra personas que tengan conocimiento electrónicos puedan cometer estos actos ilícitos sin que puedan ser sancionados adecuadamente.

2) En legislación peruana se ha identificado que dentro de la Ley N°30096 en su artículo 8 regula todo acto realizado por un agente que actúa de manera ilícita por medio de la tecnología o comunicación informática en contra de una o varias personas con una sanción penal no menor de tres años ni mayor de 8 años con sesenta a ciento veinte días multas, dejando así impunemente la modalidad del delito de phishing.

3) A través de los avances tecnológicos se han incrementado nuevas modalidades de fraudes informáticos he ahí la nueva modalidad del delito de phishing, que en la legislación peruana no se encuentra regulada generando así que personas con conocimientos informáticos cometan estos actos ilícitos en su nueva modalidad, ocasionando así una desprotección directa a la sociedad por su falta de incorporación en la legislación peruana.

4) Conforme a lo establecido en la Ley N°30096 y el incremento de los actos ilícitos realizados por medio de la tecnología se ha logrado determinar que la legislación peruana que regula los delitos informáticos necesita una adecuada actualización legislativa frente a la nueva modalidad de Phishing, ya que es evidente que mediante esta modalidad se han evidenciado actos ilícitos que se han dejado impune y libre de sanción, afectando directamente a la sociedad sin la existencia de una adecuada reparación o sanción penal.

5) A través de la correcta propuesta de actualización de la normatividad que regula el delito de fraude informático se logró incorporar la nueva modalidad de phishing, obteniendo y generando adecuadamente una persecución y sanción penal frente a estos actos que quedaban impunes.

Recomendaciones

1) El poder legislativo deberá aplicar nuevos lineamientos legislativos con el objetivo de incorporar adecuadamente el delito de phishing en la Ley N° 30096, para que de esta manera se logre perseguir y sancionar penalmente a las personas que realizan estos actos delictuosos.

2) El estado peruano deberá mejorar los instrumentos tecnológicos a la división contra delitos informáticos (CICPC), siendo evidente que la tecnología utilizada por estas personas que comenten actos ilegales es considerada más avanzada que la tecnología de las personas encargadas de investigar los delitos informáticos.

3) La normatividad que regula todo delito informático deberá ser analizados anualmente con el propósito de generar adecuadas incorporaciones de las nuevas modalidades que van surgiendo con el transcurrir de los años, para que de esta manera se puedan sancionar estos actos ilícitos que en su mayoría quedan impunes.

REFERENCIAS

Admin (2021). Phishing el delito informático más común en Colombia, Seguridad Atempi, https://www.atempi.co/phishing-el-delito-informatico-mas-comun-en-colombia/

Alvarado, J. (2018). Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de independencia, mediante el uso de phishing 2017. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8170/Alvarado%20Tolentino%20Joseph%20Darwin.pdf?sequence=1&isAllowed=y

Andina (2020). Fraudes en línea son los delitos informáticos más frecuentes en el 2020, Chiclayoenlinea.com, http://www.chiclayoenlinea.com/noticias/tecnologia/08/08/2020/fraudes-en-linea-son-los-delitos-informaticos-mas-frecuentes-en-el

Arocena, L. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española, Bogotá, https://bit.ly/3u8stWt.

BlackSip (2020). Reporte de industria: el e-commerce en Perú 2020, Lima, BlackSip.

Cruzalegui, F. (2016). Plan de preparación forense digital para maximizar la capacidad de recabar evidencia digital en procesos de medios de pago SA, 2016. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/1093/BC-TES-5873.pdf?sequence=1&isAllowed=y

Darrell, W. (2016). Avance tecnológico: riesgos y desafíos, BBVA, https://www.bbvaopenmind.com/articulos/avance-tecnologico-riesgos-y-desafios/

Díaz, C. (2019). La aplicación de la ley Nº. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/51569/D%c3%adaz_BCZ-SD.pdf?sequence=1&isAllowed=y

Efe (2021). Estafa cibernética, el delito de moda que saca los colores a la víctima 20 minutos, https://www.20minutos.es/noticia/4602459/0/estafa-cibernetica-delito-moda-saca-colores-victima/?autoref=true

El peruano (2021). Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad, diario oficial el peruano, https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Espinosa, J. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red", en La Razón Histórica, n.° 44, Murcia https://bit.ly/3tYjR4z.

Espinoza (2017). Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequence=1&isAllowed=y

Flores, C. (2017). El phishing como comportamiento penalmente relevante. http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf

Fuentes, K. (2021). Modificación de la Ley 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8345/Fuentes%20Garrido%2C%20Karla%20Vanessa.pdf?sequence=1&isAllowed=y

García, P. (2015). Derecho penal económico, 2.a ed., t. I, Lima, Instituto Pacífico.

Gestión (2021). Estas son las tres modalidades de fraude informático más usadas para ciberdelitos en Perú, revista jurídica, https://gestion.pe/tu-dinero/estas-son-tres-modalidades-de-fraude-informatico-mas-usadas-para-ciberdelitos-en-peru-noticia/?ref=gesr

Gutiérrez, M. (2017). Atentados contra la información como valor económico de empresa.

Hancco, E. (2018), en su investigación titulada, La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017. http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Hernández (2009). “El delito informático”, en Eguzkilore. Cuaderno del Instituto Vasco de Criminología, San Sebastián: https:// bit.ly/2RYsTBn.

Hernández, L. (2009). El delito informático”, en Eguzkilore. Cuaderno del Instituto Vasco de Criminología. San Sebastián.

Herrera, E. (2016). El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal. http://www.dspace.uce.edu.ec/bitstream/25000/8132/1/T-UCE-0013-Ab-399.pdf

Interpol (2020). Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19, https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Leguizamón, S. (2015). El phishing, trabajo final para alcanzar el grado en Criminología y Seguridad, Castillón, Universitat Jaume.

López, J. (2019). Métodos y técnicas de detección temprana de casos de phishing, Cataluña, Universitat Oberta de Catalunya.

Matos, E. (2021). El fraude informatico en la modalidad de Phishing. Lima, Instituto Pacifico.

Mayer, L. (2017). “El bien jurídico protegido en los delitos informáticos”, en Revista Chilena de Derecho. https://bit.ly/3eUyFgr

Mengoa, M. (2021). Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMM-SD.pdf?sequence=1

Ministerio publico (2020). Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada, OFAEC, https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Mori, F. (2019). Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012. http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3519/UNFV_MORI_QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequence=1&isAllowed=y

Morillas, D. (2017). “Delitos informáticos”, en Material de la maestría en derecho penal económico internacional, Granada, Universidad de Granada.

Noticias de Business Empresarial (2021). Sobre la empresa Pagos Digitales Peruanos, que administra la billetera móvil BIM.

Oxman, N. (2013). Estafas informáticas a través de internet. Acerca de la imputación penal del phishing y el pharming", Valparaíso, Pontificia Universidad Católica de Valparaíso.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming", Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf

Palomino, W. (2014). El intrusismo y otros delitos informáticos regulados en la Ley N.° 30096, Lima, Gaceta Penal & Procesal Penal.

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Paredes, J. (2017). De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Pérez, J. (2019). Delitos regulados en leyes especiales, Lima, Gaceta Jurídica.

Salinas, R. (2013). Derecho penal. Parte especial, 5.a ed., Lima, Grijley.

Servicio de Informática, Guías de seguridad UJA (2018) Phishing, Andalucía, Universidad de Jaén.

Superintendencia de Banca, Seguros y AFP (2018). Advertencia sobre préstamos fraudulentos por internet, en Superintendencia de Banca, Seguros y AFP, Lima, https://bit.ly/3oyG1cJ.

Terán, T. (2016). La necesidad de incorporar en el código penal el tipo penal de falsificación informática (Phishing). https://repositorio.umsa.bo/bitstream/handle/123456789/13890/T4774.pdf?sequence=1&isAllowed=y

Valle, J. (2017). El delito informático de Phishing. https://dspace.uniandes.edu.ec/bitstream/123456789/2819/1/TUQMDPC005-2013.pdf

Vargas, W. (2021). La necesidad de cambios en la Ley de Delitos informáticos a raíz de la pandemia Covid-19. Lima, Instituto Pacifico.

Villavicencio, F. (2014). Delitos informáticos, en Ius et Veritas, n.° 49, Lima, https://bit.ly/3hA565v

Zapata, J. (2019). El delito de estafa en la modalidad “Phishing” a través de internet y sus medios probatorios en Venezuela. http://mriuc.bc.uc.edu.ve/bitstream/handle/123456789/8615/30002B01.pdf?sequence=1

Zevallos, O. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?, Ius 360, https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

ANEXOS

Anexo 1.- ENCUESTA

UNIVERSIDAD SEÑOR DE SIPÁN

FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL

Estimado (a): Se le solicita su valiosa colaboración para que marque con un aspa el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional, puesto que, mediante esta técnica de recolección de datos, se podrá obtener la información que posteriormente será analizada e incorporada a la investigación con el título descrito líneas arriba.

NOTA: Para cada pregunta se considera la escala de 1 a 5 donde:

1	2	3	4	5
TOTALMENTE EN DESACUERDO	**EN DESACUERDO**	**NO OPINA**	**DE ACUERDO**	**TOTALMENTE DE ACUERDO**

ITEM	TD	D	NO	A	TA
1.- ¿Considera usted que el fraude informático en modalidad de Phishing, necesita una adecuada legislación?					
2.- ¿Cree usted que la normatividad del estado peruano no presenta una legislación eficiente frente al fraude informático en modalidad de Phishing?					
3.- ¿Considera usted que es necesario un adecuado análisis de la legislación peruana frente al fraude informático en modalidad de Phishing?					
4.- ¿Cree usted que no existe una adecuada sanción penal del delito de Phishing?					

5.- ¿Considera usted el delito de Phishing vulnera directamente los derechos fundamentales de las personas perjudicadas?					
6.- ¿Cree usted que los actos ocasionados por el delito de Phising sigue siendo impunes?					
7.- ¿Considera usted que el delito de Phising es un delito que queda impune por la falta de mecanismos electrónicos para la eficaz persecución y sanción penal?					
8.- ¿Cree usted que el estado peruano deba adherirse a convenios internacionales con el objetivo de luchar adecuadamente contra el delito de Phishing?					
9.- ¿Considera usted que por la ineficiencia normativa peruana el delito de Phishing se siguen realizando actos impunes?					
10.- ¿Cree usted que el delito de Phishing está constituido como un peligro en crecimiento en contra de la sociedad?					
11.- ¿Considera usted se deban identificar y subsanar los vacíos legales existente en la normatividad peruana frente al fraude informático del delito de Phishing?					
12.- ¿Cree usted que el fraude informático en modalidad de delito de Phishing tiene un gran índice de actos impunes y el estado peruano no aplica mecanismos jurídicos para afrontarlos?					
13.- ¿Considera usted se deba realizar un adecuado análisis a los criterios legales de la imputación penal del delito de Phishing?					

14.- ¿Cree usted que el estado peruano deba capacitar adecuadamente a los operadores de justicia para la adecuada imputación penal el delito de Phishing?					
15.- ¿Considera usted que el estado deba invertir anualmente presupuesto para mejorar la tecnología para combatir el delito de Phishing?					

ANEXO 02: FICHA DE VALIDACION DE CUESTIONARIO

<table>
<tr><td colspan="2">1. NOMBRE DEL JUEZ</td><td>HADDAD JUSEFF CHANAME VASQUEZ</td></tr>
<tr><td rowspan="4">2.</td><td>PROFESIÓN</td><td>ABOGADO</td></tr>
<tr><td>ESPECIALIDAD</td><td>DERECHO PENAL</td></tr>
<tr><td>GRADO ACADÉMICO</td><td>MAGISTER</td></tr>
<tr><td>EXPERIENCIA PROFESIONAL (AÑOS)</td><td>6 AÑOS</td></tr>
<tr><td></td><td>CARGO</td><td>Gerente General</td></tr>
<tr><td colspan="3">FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL</td></tr>
<tr><td colspan="3">3. DATOS DEL TESISTA</td></tr>
<tr><td>3.1</td><td>NOMBRES Y APELLIDOS</td><td></td></tr>
<tr><td>3.2</td><td>ESCUELA PROFESIONAL</td><td>DERECHO</td></tr>
<tr><td colspan="2">4. INSTRUMENTO EVALUADO</td><td>1. Entrevista ( )
2. Cuestionario (X)
3. Lista de Cotejo ( )
4. Diario de campo ( )</td></tr>
<tr><td colspan="2" rowspan="2">5. OBJETIVOS DEL INSTRUMENTO</td><td><u>GENERAL</u>:
Aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad de phishing</td></tr>
<tr><td>a. Identificar la aplicación de la pena y la sanción del delito de fraude informático
b. Analizar la nueva modalidad de phishing y su falta de incorporar en la legislación peruana</td></tr>
</table>

	c. Determinar si la norma requiere una actualización legislativa frente a las nuevas modalidades de fraude informático d. Proponer la actualización del delito de fraude informático ante la modalidad de phishing, para una eficiente persecución y sanción penal

A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que usted los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	6. DETALLE DE LOS ITEMS DEL INSTRUMENTO	ALTERNATIVAS
01	¿Considera usted que el fraude informático en modalidad de Phishing, necesita una adecuada legislación? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
02	¿Cree usted que la normatividad del estado peruano no presenta una legislación eficiente frente al fraude informático en modalidad de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**

	3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	
03	¿Considera usted que es necesario un adecuado análisis de la legislación peruana frente al fraude informático en modalidad de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
04	¿Cree usted que no existe una adecuada sanción penal del delito de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
05	¿Considera usted el delito de Phishing vulnera directamente los derechos fundamentales de las personas perjudicadas? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**

06	¿Cree usted que los actos ocasionados por el delito de Phising sigue siendo impunes? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
07	¿Considera usted que el delito de Phising es un delito que queda impune por la falta de mecanismos electrónicos para la eficaz persecución y sanción penal? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
08	¿Cree usted que el estado peruano deba adherirse a convenios internacionales con el objetivo de luchar adecuadamente contra el delito de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**

09	¿Considera usted que por la ineficiencia normativa peruana el delito de Phishing se siguen realizando actos impunes? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
10	¿Cree usted que el delito de Phishing está constituido como un peligro en crecimiento en contra de la sociedad? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
11	¿Considera usted se deban identificar y subsanar los vacíos legales existente en la normatividad peruana frente al fraude informático del delito de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS:** **NINGUNA**
12	¿Cree usted que el fraude informático en modalidad de delito de Phishing tiene un gran índice de actos impunes y el estado	**A (X) D ( )**

	peruano no aplica mecanismos jurídicos para afrontarlos? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**SUGERENCIAS: NINGUNA**
13	¿Considera usted se deba realizar un adecuado análisis a los criterios legales de la imputación penal del delito de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS: NINGUNA**
14	¿Cree usted que el estado peruano deba capacitar adecuadamente a los operadores de justicia para la adecuada imputación penal el delito de Phishing? 1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	**A (X) D ( )** **SUGERENCIAS: NINGUNA**
15	¿Considera usted que el estado deba invertir anualmente presupuesto para mejorar la tecnología para combatir el delito de Phishing?	**A (X) D ( )** **SUGERENCIAS: NINGUNA**

	1- Totalmente en desacuerdo 2- En desacuerdo 3- Ni de acuerdo, ni en desacuerdo 4- De acuerdo 5- Totalmente de acuerdo	

PROMEDIO OBTENIDO:	**A (X) D ( )**
7.COMENTARIOS GENERALES **CONFORME, PUEDE APLICAR INSTRUMENTO DE RECOLECCIÓN DE DATOS**	
8. OBSERVACIONES: **NINGUNA**	

Juez Experto

ANEXOS 03.- MATRIZ DE CONSISTENCIA

Titulo	Hipótesis	Variable	Objetivo General	Objetivo Especifico
FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL	Si se actualiza la legislación para una eficiente persecución y sanción penal del delito de fraude información, entonces se incorporará la nueva modalidad de phishing y sus parámetros delictivos aplicables ante el robo	**VI:** Fraude Informático **VD:** Phishing	Aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad de phishing	a. Identificar la aplicación de la pena y la sanción del delito de fraude informático b. Analizar la nueva modalidad de phishing y su falta de incorporar en la legislación peruana c. Determinar si la norma requiere una actualización legislativa frente a las

Pregunta de investigación ¿Qué contextos legislativos se aplican al actualizar la persecución y sanción penal del delito de fraude informático ante la modalidad de fishing?	de información cibernética.			nuevas modalidades de fraude informático d. Proponer la actualización del delito de fraude informático ante la modalidad de phishing, para una eficiente persecución y sanción penal.

ANEXOS 04.-JURISPRUDENCIA

TRIBUNAL CONSTITUCIONAL

EXP. N.° 01189-2019-PHC/TC
LIMA
MARCOS MORALES VARGAS, representado por WILLIAM BENARDINO GARCÍA ROSALES

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

En Lima, a los 10 días del mes de diciembre de 2020, el Pleno del Tribunal Constitucional, integrado por los magistrados Ledesma Narváez, Ferrero Costa, Miranda Canales, Ramos Núñez, Sardón de Taboada y Espinosa-Saldaña Barrera, pronuncia la siguiente sentencia. Se deja constancia de que el magistrado Blume Fortini votará en fecha posterior.

ASUNTO

Recurso de agravio constitucional interpuesto por don William Benardino García Rosales, abogado de don Marcos Morales Vargas, contra la resolución de fojas 421, de fecha 5 de noviembre de 2018, expedida por la Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima, que declaró improcedente la demanda de *habeas corpus* de autos.

ANTECEDENTES

Con fecha 18 de julio de 2018, don William Benardino García Rosales interpone demanda de *habeas corpus* a favor de don Marcos Morales Vargas (f. 31) y la dirige contra los jueces integrantes de la Primera Sala Penal de la Corte Superior de Justicia de Lima Norte y la jueza a cargo del Décimo Juzgado Penal de Lima Norte.

Solicita que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017 (f. 3), que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y (ii) la Resolución de 26 de diciembre de 2017 (f. 73), que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y, reformándola, le impuso ocho años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.

Sostiene que mediante la sentencia de 16 de junio de 2017, se condenó al beneficiario a diez años de pena privativa de la libertad efectiva, que resultó de la sumatoria siguiente: ocho años por el delito de fraude informático y dos años de pena privativa de la libertad efectiva y falsificación de firma en documento privado. Posteriormente, mediante la Resolución de 26 de diciembre de 2017, se le redujo la pena a seis años de pena privativa de la libertad efectiva, por ambos delitos.

Precisa que se condenó al beneficiario a través de una norma que no se encontraba vigente al momento que se cometieron los hechos delictuosos, pues tales hechos ocurrieron durante los meses de enero, febrero, marzo, julio, setiembre y octubre de 2013, pero fue

condenado mediante la Ley 30096, que entró en vigencia el 23 de octubre de 2013, por lo que la norma aplicable era el artículo 185 del Código Penal, que en su forma agravada era el artículo 186, numeral 3 del referido código.

La procuradora pública adjunta encargada de los asuntos judiciales del Poder Judicial (f. 61), solicita que la demanda sea declarada improcedente. Alega que el actor fue condenado mediante la Ley 30096, que sanciona el delito informático, la que estaba vigente desde el 23 de octubre de 2013; que se trata de un tipo penal prexistente al momento de lo comisión del evento delictivo; y que identificaba de forma clara la conducta objeto de investigación y su posterior juzgamiento.

Los jueces demandados, señores Luis Antonio La Rosa Paredes, Gabino Alfredo Espinoza Ortiz y Andrés Avelino Cáceres Ortega a fojas 82, 136 y 138 de autos, expresan que el delito de fraude informático fue cometido por el beneficiario el año 2014, cuando ya se encontraba vigente la Ley 30096, por lo que solicita que la demanda sea desestimada.

La jueza demandada Belinda Isabel Mercado Vílchez (f. 271) refiere que los hechos delictuosos se cometieron desde el mes de julio de 2013 hasta el mes de marzo de 2014, y la Ley 30096, que sanciona del delito de fraude informático entró en vigencia el 22 de octubre de 2013, por lo que dicha norma se encontraba vigente al momento en que se perpetró el delito que comenzó en el año 2013, pero terminó en el año 2004. Agrega, que si bien en un primer momento el Ministerio Público subsumió los hechos en el primer párrafo del artículo 8 de la mencionada Ley; empero, solicitó una ampliación para que se concuerde dicho artículo con la agravante establecida en el inciso dos del artículo 11 de dicha ley, lo cual se le puso en conocimiento a la defensa del actor e incluso su instructiva fue recibida después de la ampliación del auto de inicio del proceso.

El Decimonoveno Juzgado Penal de Lima, con fecha 3 de setiembre de 2018 (f. 387), declaró improcedente la demanda, por considerar que los hechos delictuosos se cometieron en el mes de marzo de 2014, periodo en la que ya estaba en vigencia la Ley 30096, ley de Delitos Informáticos, que entró en vigencia el 23 de octubre de 2013, esto es, antes de la fecha que se produjeron tales hechos.

La Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima por Resolución de 5 de noviembre de 2018, confirma la apelada por similares consideraciones. Agrega que el recurrente no puede acudir a la vía constitucional para que ésta revise si la norma penal le fue debidamente aplicada o no; y que la subsunción de la conducta en un determinado tipo penal, la verificación de los elementos constitutivos del delito, la dilucidación la responsabilidad penal y la valoración de pruebas y su suficiencia le competen a la judicatura ordinaria.

FUNDAMENTOS

Delimitación del petitorio

1. El objeto de la demanda es que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017, que condenó a don William Benardino García Rosales por los delitos de fraude informático y falsificación de firma en documento privado; y, (ii) la Resolución de 26 de diciembre de 2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y reformándola, le impuso seis años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.

Análisis del caso

2. El principio de legalidad penal se encuentra consagrado en el artículo 2, inciso 24, literal "d" de la Constitución, según el cual

> Nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté (...) previamente calificado en la ley, de manera expresa e inequívoca, como infracción punible, ni sancionado con pena no prevista en la ley.

3. Este Tribunal considera que el principio de legalidad penal se configura también como un derecho subjetivo constitucional de todos los ciudadanos. Como principio constitucional, informa y limita los márgenes de actuación de los que dispone el Poder Legislativo al momento de determinar cuáles son las conductas prohibidas, así como sus respectivas sanciones; en tanto que, en su dimensión de derecho subjetivo constitucional, garantiza a toda persona sometida a un proceso o procedimiento sancionatorio que lo prohibido se encuentre previsto en una norma previa, estricta y escrita, y también que la sanción se encuentre contemplada previamente en una norma jurídica.

4. Por tanto, resulta igualmente claro que la dimensión subjetiva del derecho a la legalidad penal no puede estar al margen del ámbito de los derechos protegidos por la justicia constitucional, frente a supuestos como la creación judicial de delitos o faltas y sus correspondientes supuestos de agravación o, incluso, la aplicación de determinados tipos penales a supuestos no contemplados en ellos. El derecho a la legalidad penal vincula también a los jueces penales y su eventual violación posibilita obviamente su reparación mediante este tipo de procesos de tutela de las libertades fundamentales.
5. En el caso de autos, conforme se advierte del considerando primero

9. Entonces, conforme se aprecia de la Resolución de fecha 26 de diciembre de 2017, al actor se le impuso en total ocho años de pena privativa de la libertad efectiva por los delitos de fraude informático y falsificación de firma en documento privado, vigente al momento de los hechos y que se encontraba dentro del marco normativo del primer párrafo del artículo 8 de la Ley 30096 y del primer párrafo del artículo 427 del Código Penal.

Por estos fundamentos, el Tribunal Constitucional, con la autoridad que le confiere la Constitución Política del Perú,

HA RESUELTO

Declarar **INFUNDADA** la demanda.

Publíquese y notifíquese

SS.

LEDESMA NARVÁEZ
FERRERO COSTA
MIRANDA CANALES
RAMOS NÚÑEZ
SARDÓN DE TABOADA
ESPINOSA-SALDAÑA BARRERA

PONENTE SARDÓN DE TABOADA

ANEXOS 05.-CARTA DE ACEPTACIÓN

AUTORIZACIÓN PARA EL RECOJO DE INFORMACIÓN

Chiclayo, junio del 2020

Quien suscribe:

Haddad Juseff Chaname Vásquez

Abogado Particular en estudio jurídico

AUTORIZA: Permiso para recojo de información pertinente en función del proyecto de investigación, denominado: **FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL**.

Por el presente, el que suscribe Haddad Juseff Chaname Vásquez, Abogado Particular en estudio jurídico, AUTORIZO a las alumnas: Nazario Delgado Nora Ysabel y Villanueva Sánchez Lucia Victoria, estudiantes de la Escuela Profesional de DERECHO y autoras del trabajo de investigación denominado: **FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL**, al uso de dicha información para efectos exclusivamente académicos de la elaboración de tesis de pre – grado enunciada líneas arriba. De quien solicita.

Se garantiza la absoluta confidencialidad de la información solicitada.

Atentamente.