ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE DOCTORADO EN DERECHO

Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad en el Perú

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Doctor en Derecho

AUTOR:

Vargas Miñan, Wilson (ORCID: 0000-0001-6558-0235)

ASESOR:

Dr. Quispe Ichpas, Rubén (ORCID: 0000-0003-2710-323X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA - PERÚ

2022

Dedicatoria

A mis padres por su cariño, abnegación

y apoyo incondicional

Agradecimiento

A mi familiares y seres queridos
por su apoyo constante y por su paciencia
en mis momentos de flaqueza espiritual.

Índice de contenidos

Índice de Tablas

Página

Índice de gráficos y figuras

Índice de abreviaturas

Abreviatura	Descripción
APA:	Asociación de Psicología Americana
Código Penal	C.P.
e-commerce	Comercio electrónico
DIVINDAT	División de delitos de alta tecnología
LDI:	Ley de Delitos Informáticos
OCDE:	Organización para la cooperación y desarrollo económico
OMC:	Organización Mundial de Comercio
PNP:	Policía Nacional del Perú
SAR-CoV-2:	Severe acute respiratory síndrome coronavirus 2
TIC:	Tecnologías de la información y comunicación

RESUMEN

El presente estudio tiene como objetivo sustentar los fundamentos socio-jurídicos para tipificar de *lege data* la estafa básica en el capítulo de delitos patrimoniales de la Ley de Delitos Informáticos, con lo cual se sancionaría a los agentes delictivos que usan el Internet y las TIC para engañar e inducir a error a sus víctimas con el objeto de apoderarse de su patrimonio.

La problemática se evidenció al observar durante la pandemia que la enorme cantidad de ofertas fraudulentas que aparecen en las redes, no están tipificadas en la Ley N° 30096, lo cual imposibilita hacer el ejercicio de subsunción de esas conductas en dicha norma. Este nuevo escenario criminal dificulta la labor de la policía y el Ministerio Público, por cuanto los agentes luego de cometer sus fechorías se esconden en el anonimato, generando impunidad.

Por ello, se plantean esquemas y alternativas para que la fiscalía y la policía enfrenten de modo eficaz a la ciberestafa. Creemos que el Estado, está a tiempo de implementar una estrategia integral que le permita contrarrestar los impactos negativos de este fenómeno delictivo y sobre todo plantear mecanismos para prevenirlo.

Palabras clave: delitos informáticos, estafa informática, impunidad, cooperación internacional.

ABSTRACT

The objective of this study is to support the socio-legal foundations for the typification of the basic scam in the chapter of crimes against the patrimony of the Computer Crimes Law, which would punish criminal agents who use the Internet and ICT to deceive and mislead their victims by seizing their asset.

The problem was evidenced by observing during the pandemic that vast amount of fraudulent offers that appear on the networks are not typified in Law N° 30096, which makes impossible to carry out the exercise of subsumption of this behavior in the law. This new criminal stage hinders the work of the police and the Public Prosecutor´s Office, because the agents after to make their villainy hide in anonymity generating impunity.

For this reason, schemes and alternatives are proposed for the public prosecutor and the police to confront cyberfraud more effectively. We believe that the Government is on time to implement a comprehensive strategy that allows it to counteract the negative impacts of this criminal phenomenon and above all to propose mechanisms to prevent it.

Keywords: cybercrime, computer fraud, impunity, international cooperation.

I. INTRODUCCIÓN

El presente estudio surgió al evidenciar a raíz de la pandemia que los delitos cometidos a través del internet se han incrementado debido a que sujetos inescrupulosos aprovechando el desarrollo del comercio electrónico (en adelante *e-commerce*), por el aislamiento social obligatorio hacen de las suyas valiéndose del engaño y los vacíos de la ley para sorprender a diestra y siniestra a numerosas víctimas, ya que estas conductas delictivas no están tipificadas en la Ley N° 30096, Ley de Delitos Informáticos (en adelante, LDI) .

En el contexto internacional, Posada (2017) y Temperini (2018) en sus estudios sobre el cibercrimen, sus alcances y los efectos de las TIC, (en adelante tecnologías de la información y comunicación), indican que se han multiplicado en forma alarmante las suplantaciones de identidad, los fraudes y los timos sin que sea necesario el contacto físico entre víctima y victimario. Las transferencias financieras y los beneficios del *e-commerce* son blancos demasiado apetecibles para los ciberdelincuentes, que utilizan los puntos vulnerables de los sistemas de seguridad o el candor de ciertas víctimas para hacerse de cuantiosos botines. Esta situación obliga a los Estados a adoptar acuerdos de colaboración en el marco del convenio de Budapest.

En el contexto nacional se ha abordado con visión global, el desarrollo del *e-commerce* y la influencia de las TIC en el crecimiento del ciberdelito. También, se ha abordado los problemas que enfrentan los operadores jurídicos en la persecución de estos delitos, verbi gratia: dificultades para conseguir resultados positivos de la evidencia digital para poder ir a juicio, lograr la colaboración internacional y conseguir la autorización judicial para levantar el secreto bancario y/o de las comunicaciones para identificar al agente.

En el contexto local, en Lima Norte que tiene una población cercana a los tres millones de habitantes, se advierte que los timos se concentran en zonas cercanas a hospitales y centros comerciales, ya que los ciberdelincuentes utilizan a jóvenes desempleados para repartir volantes en donde consignan páginas web y direcciones electrónicas falsas. Asimismo, se ha constatado que aún no existe ninguna fiscalía ni unidad de la Policía Nacional (en adelante PNP) especializada en ciberdelitos, ya que la División de Delitos de Alta Tecnología-

DIVINDAT tiene su sede en el Cercado de Lima, situación que torna más difícil el trabajo de los operadores punitivos de esta zona pues no cuentan con equipos modernos ni la capacitación necesaria para llevar a cabo su labor.

Cabe señalar que las empresas y los centros comerciales debido a los aforos limitados, según Luyo y Paz (2021) han diversificado su oferta en el espacio virtual, elaborando publicidad, (etapa precontractual) habilitando canales de comunicación y plataformas (etapa contractual) y haciendo entrega de sus productos por *delivery* (etapa poscontractual), todo ello para evitar salir del mercado. De esa situación se aprovechan los ciberdelincuentes para ofertar por internet diversos bienes y servicios cuya demanda ha crecido por la pandemia, por ejemplo: balones de oxígeno, fármacos para combatir el COVID, vacunas, trámites para cobrar bonos, y hasta camas de cuidados intensivos.

Analizando los fundamentos socio-jurídicos de esta situación, resulta evidente que el problema estriba de que en la medida que no se incluya el tipo básico de estafa en la LDI, se imposibilita formalizar una investigación penal al amparo de dicha norma, pues el fiscal en virtud del principio de legalidad tendrá que reconducir estas conductas a la estafa común, (cuyo ratio de pena es menor), generando con ello cierto sabor de impunidad e incrementando la sensación de inseguridad que favorece a los agentes que utilizan las TIC para embaucar a sus víctimas.

Del desarrollo de los párrafos precedentes surge la interrogante central: ¿Cuáles son los fundamentos socio-jurídicos para tipificar la estafa básica en el capítulo de delitos contra el patrimonio de la LDI? Habida cuenta que debido a la pandemia los timos se han incrementado. Como consecuencia de ello, emergen problemas específicos tales como la creciente sensación de inseguridad e impunidad y la falta de capacitación de los operadores punitivos para combatir el ciberdelito. Estos problemas específicos se formulan de la siguiente manera: ¿Cuán necesaria es la tipificación de la estafa básica en la LDI para reducir la impunidad? ¿Qué problemas afrontan los Fiscales y la PNP para combatir con eficacia el ciberdelito? Toda vez que en la PNP solo existe una unidad especializada y en el Ministerio Publico, recién en enero de 2021 se

ha creado una Unidad Fiscal Especializada en Ciberdelincuencia, empero aun esta fase experimental y no se ha descentralizado[1].

El estudio establece como objetivo principal: Sustentar los fundamentos socio-jurídicos para tipificar de *lege data* la estafa básica en el capítulo de delitos contra el patrimonio de la LDI, con lo cual se sancionaría con más severidad a los agentes que usan el Internet y las TIC para engañar e inducir a error a sus víctimas, además el fiscal contaría con las herramientas que le proporciona la Ley N° 30077, Ley contra el Crimen Organizado, ya que los delitos informáticos están comprendidos en dicha norma. Como objetivos específicos se tiene: 1) Determinar los problemas que afrontan policías y fiscales en la investigación del ciberdelito y, 2) Esbozar la necesidad de incrementar la pena cuando interviene pluralidad de agentes.

El estudio se justifica teóricamente por que propugna hacer más permeable a los cambios a la LDI, permitiendo que elementos de la estafa común la enriquezcan. Desde el punto de vista práctico la investigación se justifica porque coadyuvará a reducir la impunidad, la sensación de inseguridad y la cifra negra de la criminalidad al permitir que se imponga sanciones más severas a los agentes. El estudio tiene relevancia social pues gracias a la especialización, la evidencia digital y la cooperación internacional se podrá identificar con más facilidad a los ciberdelincuentes, lo cual repercutirá en la mejora de la percepción ciudadana sobre la administración de justicia. Por último, el estudio es viable en el tiempo y factible en el espacio toda vez que, como fiscal de Lima Norte, se ha tenido la posibilidad de constatar in situ durante la pandemia el volumen de casos que ingresan al sistema, así como intercambiar pareceres con las partes, jueces, fiscales, abogados y policías.

[1] La Resolución N° 1503-2020-MP-FN publicada el 01 de enero de 2021, ha creado la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Publico, con competencia a nivel nacional.

II. MARCO TEÓRICO

Para acreditar los fundamentos socio-jurídicos en que se basa nuestra propuesta se analizaron como antecedentes internacionales los trabajos de Gonzales (2013) y Devia (2017) quienes abordan el estudio de la estafa informática en España utilizando un diseño sistemático, destacando la rápida evolución de estos delitos que los ha hecho autónomos luego de haber sido tipos marginales. Uno de sus objetivos es destacar los vacíos punitivos y la ineficacia para combatir el ciberdelito para que se revierta el daño a los bienes jurídicos protegidos. Concluyen que en tanto no se logre mayor cooperación internacional la impunidad seguirá campeando. El análisis que hacen sobre los daños informáticos es rescatable para nuestra investigación pues refleja el temor que sienten las empresas cuando son timadas debido a que entra en juego la reputación de sus sistemas de seguridad ante la opinión pública.

En sus trabajos sobre los retos procesales de la criminalidad informática Arocena y Esparza (2017), haciendo estudios de caso, señalan que los gobiernos a través de la Organización Mundial de Comercio (en adelante OMC) se han empeñado en regular el comercio electrónico y el tráfico de mercancías en Internet; sin embargo, las principales directrices están dirigidas al control y registro de personas jurídicas, mientras las transacciones en el mercado virtual de personas naturales, carece de regulación o esta es muy laxa por la imposibilidad de llevar un control, brindándose solo recomendaciones que son insuficientes para prevenir el accionar de los delincuentes informáticos. Sus conclusiones evidencian las falencias de los operadores de justicia para combatir el ciberdelito, lo cual ha sido muy útil en nuestra investigación.

Atienza y Bermejo (2020) y Espinosa (2019) en sus estudios sobre el delito informático, indican que su trascendencia es de tal envergadura que se compara con cambios históricos tales como la transición de la comunicación oral a la escrita o a la posterior invención de la imprenta, la cual ha quedado rezagada ante la comunicación virtual que es reacia a las regulaciones, pero prescinde del papel evitando la deforestación de bosques. Utilizando el análisis fenomenológico señalan las percepciones de los grupos investigados ante la posibilidad de compartir en tiempo real gracias a las TIC cualquier información con personas que viven en el hemisferio opuesto.

Ávila et al. (2018) en su investigación descriptiva sobre las diferencias entre la estafa común y la estafa informática en la legislación penal salvadoreña, hacen un recuento de la evolución de este delito incidiendo en sus caracteres y los bienes jurídicos que merecen tutela. Uno de sus objetivos ha sido señalar la necesidad de incluir esta figura delictiva básica en la Ley Especial de Delitos Informáticos y Conexos. Los autores concluyen que el logro de este objetivo permitirá combatir más eficazmente estas modalidades delictivas que han crecido en forma alarmante en El Salvador. En el desarrollo de su trabajo emplean una metodología de tipo descriptiva con estudio de casos, lo cual refuerza sus conclusiones. El trabajo bajo comento es significativo pues revela los símiles entre el problema planteado por los autores con los que se esboza en nuestra investigación.

Gonzales (2014) en su trabajo de investigación denominado Fraudes en internet y estafa informática, utilizando análisis documental pone énfasis en los problemas de subsunción de los tipos analizados cuando concurren con la estafa común. Puntualiza la evolución y el tratamiento que le da el Código Penal español a los programas utilizados para cometer fraudes. Dentro de sus objetivos destaca las diferencias entre estas figuras para evitar los concursos reales aparentes. En ese sentido acota que solo estamos ante una ciberestafa cuando el agente privilegie el uso de las TIC en su accionar delictivo, sin que sea necesario el engaño previo para inducir en error a la víctima, lo cual es muy útil para esta investigación pues nos permite ver los planteamientos que discrepan con nuestra propuesta.

Bustos y Zúñiga (2013) haciendo un análisis documental comparado del delito informático en la legislación penal chilena con las legislaciones de Francia, España y Alemania, señalan que su estudio tiene como objetivo enfatizar las deficiencias de la ley penal chilena para sancionar las nuevas conductas nocivas que afectando a sistemas informáticos no están reguladas en forma expresa, situación que genera impunidad ante la dificultad de identificar a los agentes que se escudan en el anonimato u operan desde el extranjero. Concluyen que es necesario modificar la Ley 19.223 para recoger el enfoque europeo en la lucha contra la ciberdelincuencia a la luz del convenio de Budapest. La investigación es útil pues nos permite advertir las deficiencias de nuestra LDI la misma que a pesar de contemplar la posibilidad de convenios multilaterales, éstos aún no se hacen efectivos.

Por su parte García (2018) en su trabajo sobre el *Phishing* como modalidad de estafa informática, comentando una Sentencia de la Audiencia de Valencia, señala que el agente utiliza el engaño para clonar datos logrando que la víctima acceda a un *link* fraudulento, consiguiendo las claves de sus cuentas bancarias para luego realizar transferencias ilícitas. Utiliza la investigación descriptiva, siendo uno de sus propósitos que se establezca la responsabilidad cuasi objetiva de la institución financiera que provee estos servicios para proteger a los usuarios de la falta de diligencia de estas entidades que suelen protegerse con contratos lesivos que los exime de responsabilidad. Concluye que la protección a los usuarios es indispensable para que las entidades bancarias mejoren sus sistemas de seguridad y coadyuven a detectar estas conductas. El estudio es importante pues nos permite advertir que en España la estafa informática es el género y el *phishing* la especie, mientras en la LDI el fraude informático es el género y la estafa informática que se pretende incluir vendría a ser la especie.

Balmaceda (2011) en su estudio sobre la estafa informática en Europa, explica que el fraude y la estafa comparten el uso de artimañas para lograr un beneficio personal en perjuicio ajeno; sin embargo, el fraude informático es una categoría criminológica más amplia pues contempla intereses económicos heterogéneos no solo patrimoniales; en cambio, la estafa informática alude solo a defraudaciones patrimoniales realizadas por medios informáticos. Su objetivo es que a ambas figuras se le brinde un tratamiento homogéneo pese a la existencia de posiciones doctrinarias dispares en lo referente a los límites de ambas. El autor utiliza el estudio de casos emblemáticos acontecidos en Europa para arribar a la conclusión de que el legislador chileno debería tipificar al delito de estafa informática para otorgar mayor seguridad jurídica.

Jain y Shrivastava (2014), en su artículo sobre el ciberdelito señalan que si bien el internet es una herramienta maravillosa que nos ha cambiado la vida, también ha traído consigo riesgos y amenazas para los que navegan y hacen transacciones por la red, debido al crecimiento exponencial de los fraudes, las extorsiones, los acosos y la pornografía infantil, por lo que proponen la adopción de estrategias preventivas globales y campañas de divulgación para alertar sobre los riesgos del cibercrimen, lo cual nos permite colegir que esas estrategias pueden ser de aplicación en el contexto nacional.

Quevedo (2017) en su tesis doctoral sobre la investigación y la prueba del delito informático, utilizando el estudio de casos formula recomendaciones para evitar que se frustre la recolección de pruebas cuando colisionan con derechos fundamentales. Detalla cómo ha de practicarse la investigación preliminar para superar los juicios de licitud y fiabilidad y luego analiza la valoración judicial de la prueba informática en base a profusa jurisprudencia europea sobre la materia. Sus conclusiones son útiles porque nos permite avizorar las dificultades a las que han de enfrentarse los operadores de justicia en la recolección de la prueba.

Romeo (1996) en su estudio sobre los delitos informáticos patrimoniales, alerta sobre la dificultad de subsumir estas conductas en los delitos tradicionales, si no se quiere afectar las garantías del principio de legalidad, habida cuenta que el medio preponderante empleado son las TIC; sin embargo, según recomendaciones de la Organización para la Cooperación y el Desarrollo Económico, para evitar lagunas punitivas el legislador debe actuar con cautela si trata de incorporar las modalidades tradicionales en los delitos informáticos, pues se tiene que prever que esas conductas aparte del engaño deben implicar la introducción, alteración, supresión, diseño, o clonación de datos informáticos en el espacio virtual.

García y Peña (2017) definen a la cibercriminalidad como las acciones típicas que se despliegan en el espacio virtual, utilizando ordenadores o herramientas tecnológicas que permiten acceder, alterar, clonar o manipular datos informáticos, invadiendo la esfera privada de los ciudadanos y afectando su patrimonio, asimismo, opina que las modalidades delictivas tradicionales como hurtos y estafas que se cometan a través de ordenadores deben permanecer en los tipos tradicionales.

Como antecedentes nacionales tenemos el estudio de Chávez (2018), quien en su tesis doctoral sobre los delitos contra datos y sistemas informáticos que transgreden la intimidad, señala que estos ilícitos vulneran la información reservada y confidencial de personas naturales y jurídicas lo cual afecta su privacidad. Su propósito ha sido demostrar la incidencia de estas conductas lesivas en el derecho a la intimidad y qué deberían hacer los operadores punitivos para poner coto a estas acciones. Utiliza el enfoque cuantitativo y concluye que el acceso indebido a datos personales a través de sistemas informáticos lesiona el derecho a la intimidad de los sujetos estudiados. El estudio es útil para verificar las variadas formas de engaño usadas por los ciberdelincuentes.

Por su parte, Pardo (2018), en su tesis de maestría sobre el tratamiento jurídico de los delitos informáticos contra el patrimonio, señala que los agentes emplean diversas modalidades para atentar contra los sistemas informáticos, el patrimonio y la privacidad de las personas. Su objetivo es lograr una regulación expresa en la Ley N° 30096 para el hurto, la estafa y el sabotaje informático. Afirma que el artículo 8 de la LDI, es genérico ambiguo y vago en su interpretación, sin que la sanción corresponda con la gravedad de la conducta desplegada. Utiliza el enfoque cualitativo y la teoría fundamentada, asimismo, usa la entrevista con su respectiva guía como instrumento. Su principal conclusión indica que la regulación de los delitos informáticos contra el patrimonio es deficiente, toda vez que engloba como fraude informático toda clase de modalidades delictivas lo cual genera incertidumbre. Por ello, recomienda tipificar por separado esas conductas.

Por otro lado, Hancco (2017), en su tesis referente a la tipificación del bien jurídico protegido en el delito informático, señala que su objetivo es demostrar la deficiente regulación de la LDI y la escasa claridad sobre el bien jurídico protegido, lo cual causa confusiones y genera impunidad. El estudio es útil porque resalta las deficiencias y vacíos de la LDI, lo que guarda relación con las críticas que hemos desarrollado al respecto. Concluye que la falta de tipificación del bien jurídico protegido es el aspecto medular de la deficiente regulación de esta ley, con lo cual no concordamos toda vez que el bien jurídico protegido es una cuestión doctrinaria que figura en la exposición de motivos de la ley y es desarrollada por los Acuerdos Plenarios y la jurisprudencia.

Paredes (2013) en referencia a los ilícitos cometidos con el empleo de sistemas informáticos en Lima, analiza el impacto que ha tenido en el derecho penal el uso de las TIC como instrumentos para facilitar la comisión de esos delitos. Uno de sus objetivos es demostrar la facilidad con que se vulnera el bien jurídico protegido, así como los conflictos entre seguridad y privacidad. Concluye proponiendo modificaciones legales en el capítulo de delitos contra el patrimonio, contra los derechos intelectuales, contra la fe pública y en la LDI. La tesis es útil pues detalla la evolución histórica del ciberdelito, describiendo con prolijidad las modalidades más comunes, así como los vacíos y deficiencias de la ley, situación que ha sido tomada en cuenta para abordar nuestra realidad problemática.

Reyna (2016) en su trabajo sobre criminalidad informática formula una diferencia metodológica entre los delitos informáticos propiamente dichos y los delitos computacionales, toda vez que un sector de la doctrina tradicional asevera que el delito informático alude a los delitos tradicionales que han encontrado merced a las TIC nuevas formas de realización, por lo que descartan la existencia de un nuevo bien jurídico digno de tutela; sin embargo, otro sector de la doctrina señala que la irrupción de estas nuevas formas de comisión delictiva por medio de las tecnologías de la información y comunicación, importa la aparición de un nuevo interés social digno de tutela, en donde no solo se afectan los bienes jurídicos tradicionales sino también el softwar, la información y la confianza de las personas en los sistemas informáticos.

Villavicencio (2014) en su artículo Delitos informáticos- *Cybercrimes,* analiza estas nuevas formas de criminalidad, haciendo exegesis artículo por artículo de la LDI. Aborda las más importantes concepciones jurídicas de los derechos patrimoniales y su engarce con la LDI, desglosando las teorías ligadas a los derechos subjetivos patrimoniales, los ataques al patrimonio y las falsedades, así como la tesis que propugna la defensa de la buena fe en el tráfico jurídico. Concluye que estas doctrinas con ciertas modificaciones pueden servir de base para lograr la autonomía de los delitos informáticos. Añade que no todo ilícito informático puede ser clasificado como tal por el solo hecho usar la computadora. Su enfoque ha sido muy útil para deslindar los pros y los contras del trabajo que desarrollamos y también para analizar la naturaleza jurídica del bien jurídico protegido en la LDI.

Elías (2014) en su informe sobre la lucha contra la delincuencia informática en el país, hace un recuento cronológico de la evolución del delito informático en nuestro país hasta convertirse en una ley especial bajo los parámetros del Convenio de Budapest. Resalta los defectos de técnica legislativa al promulgar la Ley N° 30171 que modifica a la LDI, al incorporar la frase “deliberada e ilegítimamente” en diversos artículos incluyendo el fraude informático, toda vez que resulta innecesario emplear ese término ya que el artículo 12 del Código Penal, prevé que las penas establecidas se aplican siempre al agente que obra con dolo directo o de primer grado, en cambio la infracción culposa solo es punible en los casos específicamente regulados por la ley.

Por su parte, Sánchez (2016) en su Manual Auto Instructivo sobre delitos informáticos alerta sobre los riesgos de *cyber* seguridad y el peligro del uso de las TIC en la sociedad de la información, debido a que los ciudadanos ponen en manos de terceros (proveedores de servicios) gran cantidad de información que tiene que ver con su identidad, su patrimonio y su vida privada, por lo cual propugna que se mantenga incólume el Derecho al Secreto de las Comunicaciones y el uso restrictivo de esa información en base de datos privadas; ergo, la información con contenido personalísimo debe ser tratada mediante protocolos preestablecidos.

Ahora bien, respecto a las bases teóricas, éticas, axiológicas epistemológicas y filosóficas de la problemática investigada, partiendo de las categorías de la tesis, trataremos sobre la impunidad o vacíos de punibilidad teniendo en cuenta que ésta sería una consecuencia de la falta de tipificación de una conducta en el capítulo de delitos contra el patrimonio de la Ley N ° 30096. Esta deficiencia puede deberse a la falta de plenitud de un ordenamiento jurídico o por la existencia de lagunas.

Respecto a los vacíos normativos cabe señalar que estos son inaprehensibles, toda vez que la realidad supera a cualquier tipo de previsión de la cual no escapa el derecho. En ese sentido Segura (1989) y Vicente (2017) señalan que el vacío normativo en un ordenamiento jurídico crea lagunas, esto es, cuando el sistema no tiene una norma que prohíba una determinada conducta ni una norma que lo permita, pero el problema se agudiza cuando esa situación se torna recurrente. En el derecho penal los vacíos conllevan a la impunidad, debido a que resulta inadmisible la interpretación extensiva y el uso de la analogía *in mallam partem* en perjuicio del imputado, lo cual es una garantía en un Estado de derecho. En tales casos la misión del intérprete es formular recomendaciones al legislador o acudir a la ratio legislatoris por medio de una reducción teleológica sin trasgredir el principio de legalidad, punto de vista que compartimos.

En lo concerniente al ordenamiento jurídico pleno, cabe indicar que éste es un concepto dogmático, por el cual un sistema jurídico debe tener una norma para regular cada caso que se presente ante la justicia, dado que la ausencia de una norma que prevea un caso específico se denomina laguna, contrario sensu “plenitud” significa ausencia de vacíos o lagunas. Por lo tanto, un ordenamiento jurídico es completo cuando el juez encuentra en él una norma que regule cada caso que conozca. De esta definición se desprende el nexo entre plenitud y

coherencia, ésta última indica que no es posible demostrar la existencia en el sistema de una norma y de su contradictoria; por consiguiente, nos encontramos ante una antinomia cuando en el sistema coexiste una norma que prohíbe un comportamiento y otra que lo permite; empero, el dogma de la plenitud, ha sido uno de los pilares del positivismo jurídico decimonónico (Bobbio, 2005).

De acuerdo a nuestro ordenamiento jurídico, el juez no puede dejar de administrar justicia por vacíos o defectos en la ley, éste es un principio que tiene rango constitucional. Refiriéndose a las lagunas y vacíos de punibilidad García (2015) y Solano (2016) afirman que la imposibilidad de aplicar sanciones directas a una persona por defectos o vacíos en la legislación conlleva a situaciones de impunidad a veces intolerables, por ejemplo cuando los elementos del tipo no se verifican completamente en el sujeto de imputación, como acontece en los delitos concursales; empero, el juez a-quo sin vulnerar el principio de legalidad tiene que completar los vacíos pues no puede dejar de administrar justicia. En algunos casos es posible utilizar cláusulas de extensión de punibilidad sin caer en la responsabilidad objetiva. Lo más recomendable es acudir al legislador con propuestas de *lege ferenda;* sin embargo, ese camino es largo y tortuoso mientras tanto la sensación de impunidad es manifiesta, ya que no se puede sancionar al agente en virtud del principio *nullum crimen sine lege praevia.*

Por nuestra parte compartimos esta conclusión dogmática ya que lo contrario contravendría el principio de legalidad. No obstante, debido al incremento de la criminalidad esta sensación de impunidad por los defectos de la ley va in crescendo pues según un Informe del Ministerio Publico sobre la Ciberdelincuencia en el Perú. De octubre de 2013 a julio de 2020 las fiscalías penales registraron 21,687 denuncias, de las cuales 40% corresponden al año 2019, (antes de la pandemia). En ese periodo se archivó el 58% de los casos y solo se emitieron 108 sentencias, generando una importante carga fiscal y una sensación de impunidad e inseguridad (Informe N°4, 2021).

Respecto a la utilización de la pena como instrumento de disuasión para los potenciales delincuentes, nuestro país ha adoptado el sistema de prevención general negativa; sin embargo, Zaffaroni (2014) en *La cuestión criminal*, apunta que la pena no es disuasiva y no debe aplicarse en ningún caso en tanto no se legisle sobre una conducta específica, toda vez que el derecho penal es inaplicable por

analogía, por el carácter fragmentario de la norma punitiva y por respeto al principio de legalidad, propio de un estado de derecho, de lo contrario la pena impuesta se convierte en arbitraria y en un mal por sí misma; por lo tanto, una conducta dañosa no prevista en una norma penal no es un problema del juez sino del legislador, empero, en virtud del principio *alterum non laedere* nada obsta para que el agente este obligado al resarcimiento respectivo en la vía extrapenal.

A nivel macro el menú de alternativas para evitar la impunidad en los delitos informáticos, desde la óptica del convenio de Budapest implica formular políticas preventivas frente al cibercrimen, lograr consensos, partiendo de lo más simple a lo más complejo, por ejemplo, aquello que tiene menor nivel de compromiso integrador como la simple cooperación, mientras lo más difícil de alcanzar, esto es, la unificación normativa se lograría en forma paulatina. Los puntos intermedios serían los procesos de asimilación, armonización y tratamiento de los tipos penales, en tanto la unificación aparece como una suerte de aspiración utópica (Sain, 2018).

Respecto a la estafa y los delitos informáticos, Jiménez (2017), señala que éstos emergen con la aparición del internet, a través del cual sujetos inescrupulosos u organizaciones criminales escudándose en nombres hipocorísticos, utilizan el espacio virtual y las TIC para lesionar la información tratada y almacenada en los sistemas informáticos, así como el software que hace posible este almacenamiento. Por otra parte, también se protege bienes jurídicos tradicionales como el patrimonio, la fe pública y la propiedad intelectual, la conducta criminal implica la burla de los dispositivos de seguridad implementados en el e-commerce, en empresas especializadas en *retail*, y en empresas del sistema financiero (Pérez, 2019). En el gráfico que remitimos a los anexos (Figura 1) se aprecia los alcances conceptuales y tipológicos de los delitos cibernéticos.

La frontera entre estafa informática y phishing es muy difusa lo que ha provocado discusiones doctrinarias, cierto sector propugna que estas conductas deben alejarse de la clasificación tradicional e ingresar a la ciberestafa, siempre y cuando el agente privilegie en su accionar el uso de las TIC. En ese sentido, Rico (2013) define a la ciberestafa como la conducta ilícita que a través del engaño utilizando el soporte de las TIC genera perjuicio patrimonial al sujeto pasivo, provocando que este se desprenda de su patrimonio a favor del agente o de un tercero. Añade, que las variadas conductas fraudulentas cuasi similares por la

expansión del internet, ha dificultado encuadrar estos nuevos supuestos en los tipos penales tradicionales, lo cual ha provocado la revisión y modificación de la legislación penal para evitar la impunidad de estas conductas en donde media el engaño a la víctima.

Ahora bien, sobre la criminalidad informática Mayer (2018) opina en sentido amplio y en sentido estricto, el primero suele utilizarse para englobar conductas realizadas a través de computadoras lesionando bienes jurídico tradicionales, (patrimonio, intimidad, fe pública). En sentido estricto, alude a conductas que inciden en los sistemas informáticos (almacenamiento de información, sistemas operativos o *software*). Añade, que el termino cibercriminal suele emplearse para aludir a delitos cometidos a través del internet en sentido amplio y estricto, empero, solo debe considerarse como delito informático aquellas conductas que afectan los sistemas informáticos, los demás como por ejemplo los daños al hardware deben reconducirse a los delitos comunes contra el patrimonio. A modo de ejemplo se detalla la ruta y los mecanismos que utilizan los ciber-delincuentes para cometer sus delitos. (los cuales se grafican en la Figura 2 que se remite a los anexos).

Como se puede vislumbrar ambas categorías guardan estrecha relación toda vez que la ausencia de tipificación de la ciberestafa en nuestra LDI, provoca que numerosos agentes queden impunes o reciban penas muy benignas, debido a que los operadores punitivos reconducen estas conductas a la estafa básica con la consiguiente frustración de las víctimas, pues la pena en ese supuesto es menor. El esquema de la estafa informática puede seguir la siguiente secuencia: oferta fraudulenta en un sitio web falso; difusión en las redes; victimas atraídas incurren en error y por último se produce el desplazamiento patrimonial a favor del agente o de un tercero. (Se gráfica este esquema en la Figura 3 que se remite a los anexos).

Ante esta situación, diversos países han establecido mecanismos para evitar los delitos informáticos, como es el caso de Chile, que brinda diversos consejos (Figura 4) que se detallan para conocimiento de la ciudadanía, la cual se remite a los anexos. Consideramos que estos ciber-consejos para evitar los delitos informáticos, son necesarios para no caer en las trampas de los ciberdelincuentes que permanentemente van creando nuevas formas de engaño para personas naturales y jurídicas. Por lo tanto, se recomienda no confiar en correos desconocidos, ni abrir archivos, ni utilizar enlaces que estén dentro de un correo

enviado por un desconocido y nunca ingresar nuestras credenciales a un sitio web desconocido. También se han planteado una serie de estrategias y consejos para enfrentar los delitos cibernéticos. (Los cuales se detallan en la Figura 5 que se remite a los anexos).

En resumidas cuentas, los fraudes y estafas cibernéticas se han masificado y extendido de manera considerable, por eso mismo conviene diferenciarlos e identificarlos para una mayor efectividad en su abordaje. (el esquema que hace esa diferenciación, se grafica en la Figura 6 que se remite a los anexos).

En lo referente a los supuestos éticos de los delitos informáticos, debemos referirnos a las bondades y peligros del uso de las TIC. En ese sentido Ascott (2014) en su ensayo El futuro es ahora: Arte, tecnología y conciencia, publicado en Reino Unido, señala que la era digital producirá una generación de seres múltiples cuyas actividades serán más productivas y menos contaminantes, lo que maximizara las utilidades de las empresas usuarias, por lo que debe primar la tecno ética para evitar excesos de empresarios, usuarios y *hackers*, ya que tecnología no es intrínsecamente neutral, propugna darle rostro humano a la tecnología lo cual es la clave para lograr la empatía de los demás, ya que gracias al internet se ha democratizado el saber y el mundo está más interconectado.

El desarrollo del e-commerce está ligado a la expansión de la tecnología en todas las actividades productivas y ramas del saber y de eso de aprovechan los ciberdelincuentes para hacer de las suyas amparándose en el anonimato. En ese sentido, Mitcham (2015) al tratar sobre la filosofía y la ética de la tecnología, opina que ésta última tiene vínculos indisolubles con la economía, por que está orientada a la reducción de costos, lo que obviamente trae beneficios para la empresa y para cualquier actividad a gran escala; por lo tanto, para evitar caer en excesos, se debe establecer un contrato social para la ciencia y la tecnología. Añade, que otro peligro es la distorsión de la información y el uso inadecuado del marketing digital, situación que puede causar perjuicio masivo, (consumismo fatuo), por lo que se debe perfilar una visión humanística de la tecnología con respeto a los derechos humanos, además si bien el cambio tecnológico genera variación de costumbres y hábitos en la sociedad, ello no debe alterar los principios éticos básicos de una comunidad.

No todos los teóricos académicos comparten esta posición, por cuanto Heidegger (2001) en su conferencia La pregunta sobre la técnica, asevera que la invención o cualquier innovación tecnológica no es más que ciencia aplicada para resolver un problema concreto, el germen de la idea innovadora que generalmente nace para satisfacer una necesidad es básicamente neutral, por lo tanto, la aplicación práctica no es un problema del creador sino de los ingenieros y los tecnócratas de los gobiernos. Agrega, que el cambio tecnológico en si no es ni bueno ni malo, su éxito y difusión es un asunto social y económico lo cual no compete al creador.

Sobre las TIC, el insigne profesor canadiense Luppicini (2020) indica que la distorsión de la información y el uso inadecuado de la tecnología empleada en el marketing digital puede causar perjuicio masivo, por lo tanto, es factible y deseable la intervención de los órganos reguladores que sin afectar la libertad de expresión perfilen una visión humanística de las TIC con respeto a los derechos humanos, toda vez que el cambio tecnológico genera variación de costumbres y hábitos en la sociedad, lo cual no debe alterar los principios éticos básicos. Lo contrario puede conllevar a un excesivo egoísmo e individualismo.

Si bien es comprensible que el Estado a través del órgano legislativo regule cualquier conducta que se torne nociva por el uso indiscriminado de la tecnología, no todos comparten ese aserto, por ejemplo Nozick (1988) en su obra *Anarchy, State and Utopia,* señala que es moralmente injustificable la intervención del Estado en cualquier actividad de los particulares, pues su rol debe estar enmarcado es mantener el orden interno, costear los servicios colectivos con la recaudación impositiva y dotar de reglas claras y precisas a los actores de la sociedad, por lo tanto, solo se necesita un Estado mínimo.

Respecto al análisis axiológico del fenómeno informático, Echevarria (2013) señala que desde una perspectiva sistémica los valores emergentes se aplican en conjunto de modo que, al valorar un aspecto positivo del cambio tecnológico por influjo de la informática, ponemos en juego otros valores los cuales van surgiendo conforme surgen las dificultades inherentes a un mundo digitalizado. En ese sentido la percepción social de los riesgos no es uniforme, se diferencian de acuerdo al estamento sobre el cual recaen, ya sea por cuestiones culturales o económicas.

En sentido también contrapuesto Russell (1961) en *The Scientific Outlook*, siguiendo la tradición de Hume y Heidegger reafirma la neutralidad axiológica da la ciencia y tecnología, dentro de la cual destaca la informática, enfatizando que son los usos y los hechos derivados de esa praxis lo que subjetiviza a la ciencia y a la tecnología lo cual no es responsabilidad del creador. En ese orden contextual señala que el desarrollo de las armas nucleares y los misiles intercontinentales que llevan aparejados sofisticados sistemas informáticos para dar con el blanco son claros ejemplos del mal uso de la ciencia y tecnología, cuyo gasto se incrementa por razones militares y políticas, dejando de lado el buen uso de la energía nuclear para dotar de energía a precios razonables y al alcance del tercer mundo.

Monterrosa et al (2015) en su ensayo Por una revaloración de la filosofía de la técnica, sostienen que por razones esencialistas los científicos e ingenieros emplean cálculos coste -beneficios a la hora de escoger la mejor propuesta innovadora, la misma que incluye valores como la aplicabilidad, simpleza en el manejo y seguridad en la óptica de la responsabilidad social de la empresa. Antes de ello basándose en la estricta racionalidad muchos científicos coincidían en la idea de que la tecno-ciencia por su carácter objetivo estaba libres de valores los cuales dependen de criterios subjetivos, esta concepción cambio cuando Thomas Kuhn publicó La estructura de las revoluciones científicas.

Por su parte, Wessel y Helmer (2020) en su ensayo sobre la crisis ética en las innovaciones tecnológicas, aseveran que las cadenas de valor en torno a las nuevas tecnologías exacerban las preocupaciones de las industrias por ganar más usuarios compitiendo ferozmente entre sí, incidiendo en los componentes emocionales, situación que es aprovechada por los fabricantes de *fakenews* y por los ciberdelincuentes.

Respecto al análisis sociológico Arteaga et al (1995) en su ensayo sobre las dimensiones sociales del cambio tecnológico, señala que desde el punto de vista de la informática si bien la naturaleza del cambio es de naturaleza tangible, su impacto en una comunidad determinada es difícil de cuantificar por que priman los intereses políticos y económicos. El proceso de cambio es el efecto combinado de varias actividades diferenciadas que nacen de una carencia y proponen una solución que de hecho provoca cambios en los hábitos de las personas y en el entorno social, por ejemplo, en la actualidad es impensable que los adolescentes prescindan de sus

celulares. Además, el cambio tecnológico implica la trasformación de los modelos de producción y trae consigo el aumento de la productividad lo que suele traer como consecuencia la reducción de empleos.

Staudenmaier (2002) comentando sobre las tendencias recientes en la historia de la tecnología, señala que el constructivismo contrapone a la visión lineal y simplista del cambio tecnológico, una concepción compleja que es fruto de las tensiones que se producen entre los actores que intervienen en el proceso de innovación tecnológica, la cual no se produce de modo inmediato, por el contrario el proceso de cambio tecnológico fructifica cuando los grupos de interés llegan a un consenso sobre los objetivos del cambio, solo cuando se logra ese consenso se consigue la estabilización del entramado social.

Gainza (2015) apunta desde el punto de vista sociológico que el desarrollo de las TIC no siempre va acompañado del desarrollo del entorno social, especialmente de los sectores marginados, por lo que es difícil medir el impacto y la evolución de estos cambios, en tal sentido se requiere parámetros de control. También indica que el proceso de difusión de estos cambios depende del éxito obtenido en la aplicación y transformación de los viejos modelos y la aceptación mayoritaria de los estratos sociales.

Bauman (2016) en su obra Liquid Times, critica el impacto de las redes sociales sobre el individuo, puntualiza que éstas son una herramienta para crear una comunidad sustituta donde los conflictos puede generar virulencia en torno a intereses específicos, empero, no se requieren habilidades sociales para mantenerse en esa comunidad y por lo tanto el capital afectivo se mide por el número de contactos que se tiene en las cuentas de Facebook, Instagram entre otras.

Port otra parte, las lagunas y vacíos punitivos también son analizados desde el punto de vista filosófico, para evitar cuestionamientos de orden moral ante la inoperatividad del Estado. En ese sentido, desde la perspectiva filosófica Hart (1983) se ubica dentro de la corriente de la Filosofía analítica del derecho, destacando el papel de la filosofía lingüística, en donde el análisis del lenguaje resulta un elemento fundamental para dotar de solución a los problemas jurídicos. Señala que ante vacíos normativos el juez está facultado para utilizar la integración o la analogía.

Dworkin (2014) atacó frontalmente el positivismo jurídico de Hart, afirmando que su teoría del derecho está infectada por el aguijón semántico en clara alusión a la filosofía analítica. También cuestiona la metodología utilizada por Hart, señalando que la labor de la filosofía no es la descripción neutral de fenómenos jurídicos, sino la justificación del mejor concepto de derecho según las circunstancias históricas, debiendo prevalecer los preceptos morales ante lagunas o vacíos normativos o lagunas de la jurisprudencia. Agrega que no se puede descartar a priori el fundamento moral al momento de resolver un caso donde no se haya legislado o no exista jurisprudencia.

Como se puede apreciar un vasto sector de la doctrina sostiene que el desarrollo de la tecnología no puede estar desligado de la ética. En ese sentido, Singer (2018) en su conferencia sobre ética y tecnología, señala que desde el punto de vista ético hay que maximizar los intereses de las mayorías con el auxilio de la tecnología para promover el bienestar y reducir el sufrimiento. Respecto a la propiedad intelectual en relación a la producción de fármacos asevera que estos derechos son intrínsecamente naturales por lo que se debe permitir la producción de versiones genéricas para salvar vidas de los menos favorecidos.

Martin (2018) indica que no basta el uso de la tecnología para solucionar problemas prácticos, se debe también incidir en las técnicas de producción que eviten desbordes sociales o problemas de contaminación ambiental, sino tendremos un nuevo *Frankenstein* incontrolable. Partiendo del materialismo filosófico de Gustavo Bueno, propone el cruce de tres criterios dicotómicos: uno gnoseológico, uno ontológico relacionado a la diferencia de las técnicas empleadas en la innovación tecnológica y uno axiológico relacionado a las cuestiones sociales, debiendo priorizarse al más idóneo.

Desde el punto de vista metodológico Hernández-Sampieri y Mendoza (2018) sostienen que el enfoque cualitativo es el más usado en ciencias sociales, debido a la dificultad de cuantificar los fenómenos sociales, permite comprender la realidad mediante modelos que explican las causas o motivos por los cuales se producen dichos fenómenos. Añaden que la investigación cualitativa posee una dinámica que permite la interrelación y el regreso a etapas previas del proceso.

Gómez (2016) señala que una idea se convierte en problema de investigación cuando el investigador encuentra alguna dificultad en una situación específica y quiere resolverla y para que una idea se traduzca en un problema de investigación además de la revisión preliminar de la literatura, deben identificarse a las variables intervinientes.

Por último, Feyerabend (2010) asevera que la metodología científica universalmente valida es un contrasentido, puesto que no hay conocimientos ciertos y no se sabe que paradigmas dominaran la ciencia del futuro, ésta es una empresa esencialmente anarquista, porque el anarquismo teórico es más humanista y más adecuado para estimular el progreso por su esencia de libertad sin ataduras basadas en la ley y el orden. Agrega, que no hay reglas metodológicas libres de excepciones que rijan el progreso de cualquier ciencia, puesto que si esta funciona con normas fijas y universales no será realista, por el contrario, devendría en perniciosa y perjudicial.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El tipo de investigación empleada en el presente estudio es la aplicada por que está orientada a resolver un problema específico, en el caso sub examine, la necesidad de sancionar con mayor drasticidad los fraudes cometidos a través de la red de redes, situación que de lograrse traería como correlato la reducción de la impunidad. Según Ñaupas et al (2011) este tipo de investigación surge de la necesidad de mejorar, perfeccionar u optimizar el funcionamiento de un sistema ante la aparición de un problema trascendente que causa perjuicios económicos y/o sociales. El enfoque usado es el cualitativo, el cual según Arbaiza (2016) es el más usado en ciencias sociales debido a la dificultad de cuantificar y/o reproducir estos fenómenos como acontece en las ciencias naturales. Este enfoque permite comprender la realidad circundante mediante modelos que explican a profundidad las causas por las cuales se producen esos fenómenos.

El diseño que se ha asumido es la Teoría Fundamentada, en la cual el investigador produce una explicación o hipótesis respecto a un fenómeno que responde a un contexto específico y surge de los datos empíricos obtenidos en el trabajo de campo (Taylor y Francis citados por Hernández y Mendoza, 2018). Obviamente es bastante difícil alcanzar ese nivel por la magnitud del trabajo de campo y/o por el tamaño de la muestra, lo cual no es óbice para elaborar un modelo teórico que explique el fenómeno observado. Esta investigación se ha realizado desde el paradigma interpretativo, el cual surge como alternativa al paradigma positivista, toda vez que en las disciplinas sociales existen diferentes cuestiones y problemas que no se pueden explicar ni comprender a profundidad desde la órbita del enfoque cuantitativo, por lo tanto, el investigador debe aprehender la realidad circundante a partir de su interacción con ésta (Martínez, 2013).

3.2. Categorías. Sub categorías. Matriz de Categorización

Tabla 1

Matriz de categorización

CATEGORIAS	SUBCATEGORIAS
La estafa básica en la Ley de Delitos Informáticos	La ciberestafa y su relación con el Ciberdelito
	Delitos informáticos en la legislación nacional
Impunidad por falta de tipicidad	Rol de los operadores jurídicos
	Vacíos de Punibilidad o Lagunas del Derecho

3.3. Escenario de estudio

El escenario de estudio se ubicó en Lima Norte, lugar de donde se recabó la información requerida y además porque el autor tiene facilidades para acceder ella por su condición de fiscal en dicha sede. Cabe señalar que por su densidad poblacional se trata de una jurisdicción importante en el país, según los datos del último censo del INEI tiene una población aproximada de tres millones de habitantes. Comprende los distritos de Independencia, Los Olivos, San Martin de Porres, Comas, Carabayllo y la provincia de Canta, empero, la circunscripción territorial de la sede central de Lima Norte comprende los distritos de Comas, Independencia, parte de Los Olivos y parte de San Martin de Porres.

3.4. Participantes

La muestra de participantes e informantes estuvo conformada por un grupo de jueces, fiscales, abogados y policías escogidos en forma no probabilística o no aleatoria. Fueron escogidos por que tienen conocimiento de la problemática estudiada y/o están inmersos en ella, ya que trabajan en unidades especializadas o conocen muchos de estos casos por su actividad profesional.

3.5. Técnicas e instrumentos de recolección de datos

La técnica que se utilizó en el presente estudio es la entrevista y el análisis de fuente documental. Los instrumentos son: la Guía de Entrevista y la Guía de Análisis de Fuente Documental. El análisis de fuente documental, se centra en la revisión y selección de documentos independientemente del soporte en que se encuentren con el objeto de extraer la información pertinente requerida para el estudio (Ramírez, (2010). En esta investigación se analizó básicamente carpetas fiscales. Respecto a la entrevista ésta fue semiestructurada y además fue validada por expertos, la cual según Ñaupas et al (2011) es aquella que se basa en una guía flexible no tan formal ni rígida, lo que permite al investigador lograr cierta empatía con el entrevistado introduciendo algunas interrogantes para esclarecer vacíos o puntos controvertidos que pueden surgir durante el recojo de información, es decir, no todas las preguntas están predeterminadas.

3.6. Procedimientos

El procedimiento utilizado para el presente estudio es el siguiente: (1) Identificación del problema; (2) Delimitación del marco espacial y temporal; (3) Acopio de la información existente; (4) Selección de expertos y entrevistados; (5) Procesamiento de la información obtenida, (6) Contrastación de la información; (7) aplicación de un método de análisis de los resultados, (8) Presentación de resultados y discusión, (9) Formulación de conclusiones y recomendaciones; (10) Levantamiento de observaciones; (11)Sustentación de la investigación.

3.7. Rigor científico

Se ha asegurado el rigor científico de la investigación porque se siguieron parámetros metodológicos adecuados, con un diseño y tipo de estudio apropiados, se usó una técnica de recolección de datos pertinente, teniendo como instrumentos el uso de guías, siendo ellas previamente validadas por expertos. Por esas razones consideramos que se trata de una investigación científica pues posee las siguientes características: **a) Dependencia**. La cual es paralela a la confiabilidad cuantitativa, posee consistencia lógica e indica el grado en que otros investigadores recolectando datos similares en el campo y efectuando análisis sucedáneos, han obtenido resultados equivalentes; **b) Credibilidad**. Es equivalente a la validez, surge del análisis de los datos recogidos en el escenario. En nuestro caso particular se captó el significado de las experiencias de los participantes, específicamente aquellas que guardan relación con el planteamiento del problema (Hernández y Mendoza, 2018, pp.503-504). La credibilidad tiene que ver con la correspondencia entre la forma en que el participante percibe los conceptos vinculados al problema y la manera como el investigador retrata esos puntos de vista, evitando caer en subjetividades; **c) Transferencia.** Esta no implica la aplicabilidad de resultados a poblaciones más amplias, ya que este no es el objetivo de la investigación cualitativa; empero, su esencia puede aplicarse a fenómenos similares; **d) Confirmabilidad**. Este presupuesto tiene estrechos vínculos con la credibilidad, sirve para demostrar que el investigador ha minimizado los sesgos, subjetividades y tendencias, lo que implica rastrear las fuentes y explicar la lógica que se empleó para interpretar los resultados.

Tabla 2

Certificado de Validación de expertos

Nombre	Grado Académico	Aplicabilidad del instrumento
Dr. Carrasco Campos Marco, Antonio	Dr. en Educación	Si aplica
Dr. Velazco Levano, Nilton César	Dr. en Derecho	Si aplica
Dr. Gonzales Barbadillo, Miguel Ángel	Dr. en Derecho	Si aplica

3.8. Métodos de análisis de datos

Para efectuar un correcto análisis de la información se partió del estrecho vínculo existente entre la conformación de la muestra, la recolección de datos y el subsecuente análisis, tampoco se ha perdido de vista que el recojo de datos según Coleman y Unrau citado por Hernández-Sampieri et al (2014, p.419) debe guardar relación directa con las categorías y objetivos del tema estudiado. Para facilitar el trabajo se organizó los datos recogidos, se les transcribió y codifico, para lo cual se confecciono una matriz especificando las relaciones entre los datos con sus respectivas categorías y subcategorías lo que permitió que se mantenga la coherencia argumentativa y metodológica.

3.9. Aspectos éticos

Se ha obtenido la información de fuentes confiables, tanto documentales, como la proveniente de los entrevistados. En el primer caso se hizo citando escrupulosamente la fuente y su autor independientemente del soporte en que se encuentren, siguiendo las normas de la Asociación de Psicología Americana (APA), requisito exigido por la Universidad. Respecto a los entrevistados la información se obtuvo luego de informarles previamente el propósito y objetivos de la investigación y una vez obtenido su consentimiento. Cabe señalar que el suscrito no tiene conflicto de interés alguno con el tema ni con los entrevistados, ni con el marco espacial elegido, con lo cual se aseguró que se trata de una información objetiva, libre de ser tendenciosa, manipulada o plagiada. Los autores fueron debidamente citados respetando los derechos de autor y la propiedad intelectual.

IV. RESULTADOS Y DISCUSIÓN

4.1. Procedimientos de recolección de datos

De acuerdo a Hernández et al (2014) los resultados se caracterizan por ser el reporte de la investigación, de acuerdo con el enfoque seleccionado, teniendo en cuenta que la presente es una investigación cualitativa, se asumió el siguiente procedimiento de recolección de datos: En primer lugar, se sometió el formulario de preguntas a un juicio de expertos, luego de lo cual fueron validados por el docente. Acto seguido, se coordinó con los informantes clave y con cada uno de los entrevistados a fin de recoger la información. Todos ellos fueron debidamente informados de la naturaleza y alcances del estudio por lo que dieron su consentimiento para ser entrevistados.

En el presente caso se utilizó una entrevista semiestructurada la cual por su flexibilidad permite al investigador ajustar la guía de acuerdo a las variaciones del caso, por la información que proporciona el participante o por la aparición de categorías emergentes, por lo que las nuevas interrogantes deben adecuarse a los objetivos del trabajo de investigación. Los entrevistados fueron seleccionados debido a su experiencia en el tema y su nivel de involucramiento en ella, por ello, su información resultó relevante. Se fijaron diversas fechas para llevar a cabo las entrevistas, las cuales se realizaron desde el 20 de septiembre al 05 de noviembre de 2021. Estas se llevaron a cabo de modo presencial respetando los protocolos de bioseguridad. Una vez obtenida la información, se procedió a sistematizarla, analizarla y procesarla para su debida presentación como resultados y discusión.

4. 2. Análisis e interpretación de los instrumentos de recolección de datos

Guía de entrevistas aplicada a jueces.

Subcategoría 1: La ciberestafa en relación con el ciberdelito.

A continuación, se consignan los datos obtenidos de la técnica de entrevista realizada a jueces, tomando en cuenta la sub categoría ciberestafa en relación con el ciberdelito. Respecto a la primera su característica principal es que se trata de un ilícito contra el patrimonio donde media el engaño o cualquier conducta fraudulenta que despliega el sujeto activo con el objeto de embaucar al agraviado para que éste realice una disposición patrimonial a favor del victimario o de un

tercero. En ese sentido, los jueces consideran que la estafa informática viene a ser un delito sucedáneo que carece del nivel de sofisticación que presenta el ciberdelito.

Sub categoría 2: Delitos informáticos en la legislación nacional

Sobre cuál es la característica principal del delito informático, los jueces señalan que son conductas criminógenas de cuello blanco que se realizan a distancia pues no hay contacto físico entre víctimas y victimarios. El sujeto activo para realizar su cometido viola la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos de los usuarios. El acceso es ilícito porque el agente luego de sorprender a la víctima accede sin autorización a sus claves o passwords e incluso violenta medidas de seguridad. La característica más importante de este delito es el uso de las TIC para acceder a las cuentas de los usuarios. Sobre si consideran que existen deficiencias en la ley de delitos informáticos, señalan que hay problemas en la falta de precisión en el capítulo de delitos contra el patrimonio y deficiencias técnicas de redacción legislativa, lo que dificulta la labor de los operadores jurídicos al momento de hacer la subsunción, además las penas que se imponen no se condicen con la vulneración del bien jurídico protegido, además no se ha regulado la propiedad intelectual y el espionaje industrial en esa ley especial.

Sub categoría 3: Rol de los operadores jurídicos

Respecto a las principales dificultades que enfrentan los operadores jurídicos (jueces, fiscales y PNP) en la persecución del delito informático, señalan que es complicado identificar a los sujetos activos pues estos nunca usan su verdadero nombre, por eso para identificarlos hay que pedir el levantamiento del secreto de las comunicaciones. La Policía Nacional solo cuenta con una unidad especializada que es la DIVINDAT y se requieren más unidades de atención a nivel nacional, así como capacitación para policías y fiscales. Otra desventaja es la rápida evolución de las modalidades que emplean los ciber-delincuentes para embaucar a sus víctimas y luego esconderse en el anonimato, lo que dificulta identificarlos. Sobre si es necesario capacitar a policías y fiscales para combatir con mayor eficacia el ciberdelito, señalan que la capacitación debe ser permanente por que el refinamiento delictivo también crece. La capacitación y mejora de equipamiento

son básicos para detectar, prevenir, perseguir y lograr que sean sancionados en sede judicial. Asimismo, consideran indispensable que policías y fiscales cuenten con herramientas tecnológicas y equipos modernos para combatir estos delitos.

Sub categoría 4: Vacíos de Punibilidad o Lagunas del Derecho

Respecto a los vacíos de punibilidad o lagunas del Derecho y si consideran que se ha incrementado esta modalidad delictiva a raíz de la pandemia, los entrevistados señalan que sí han aumentado las estafas informáticas porque las personas compran mucho más por internet debido a la pandemia y además no existen mecanismos de control en esas compras. Al no existir protocolos no hay forma de hacer seguimiento a la comisión de estos delitos, lo que se aprecia cuando las personas requieren ser atendidas vía web en bancos y centros comerciales y para recibir sus pedidos por delivery, ya que no pueden saber cuándo están ante un ciberdelincuente o ante un empleado de esas empresas. Concluyen que hay vacíos en la Ley de Delitos Informáticos por que no se puede sancionar a los agentes delictivos que usan el internet para defraudar a sus víctimas, debido a que esa modalidad no está tipificada en dicha ley.

Guía de entrevistas aplicada a fiscales

Sub categoría 1: La ciberestafa en relación con el ciberdelito

Sobre si considera que la ciberestafa se incrementó a raíz del aislamiento social obligatorio, los entrevistados señalan que si se ha incrementado debido a las restricciones del gobierno por la emergencia sanitaria. Los usuarios por necesidades personales o empresariales usan este medio para hacer compras. Las empresas han tenido que realizar transacciones por internet para continuar con sus actividades. Aseveran que si se han incrementado las estafas porque casi toda la ciudadanía tiene que adquirir lo que consume a acceder a los servicios que necesita usando el internet. Sobre cómo evalúan el papel de las TIC en el desarrollo del comercio electrónico, señalan que estas son herramientas importantes para el desarrollo del comercio, pero también lo es para el sistema financiero y empresarial como acontece en los países desarrollados. Aseveran que estas tecnologías son muy necesarias de eso no cabe duda, de lo contrario las empresas colapsarían, por las restricciones que ha impuesto el gobierno debido a la pandemia.

Sub categoría 2: Delitos informáticos en la legislación nacional

En relación a los delitos informáticos en la legislación nacional señalan que la Ley ha tenido ciertos avances peros subsisten las dificultades para gestionar el levantamiento del secreto bancario y de las comunicaciones a través del Poder Judicial, por lo que sugieren que se debe otorgar más facultades a la Unidad de Inteligencia Financiera para coadyuvar a la persecución del ciberdelito. Sobre si la pandemia ha contribuido a generalizar el uso del internet para cometer defraudaciones, la mayoría de entrevistados señala que hay otros factores como la crisis económica y el desempleo. Otro grupo de entrevistados señalan que debido a la pandemia se ha generalizado el uso del internet y por ende se ha incrementado el número de delitos por las redes. Añaden que muchos han tenido que aprender a usar estas herramientas para sobrevivir en esta era del COVID-19. En relación a cuáles son las principales dificultades que enfrenta la PNP y el Ministerio Público en la persecución del delito informático, señalan que la principal dificultad es la falta de capacitación, la falta de especialización y la falta de equipos modernos.

Sub categoría 3: Rol de los operadores jurídicos

Los fiscales entrevistados reconocen que tanto ellos como los demás operadores jurídicos carecen de recursos logísticos, presupuestarios, personal e infraestructura para llevar a cabo las investigaciones que tienen a su cargo. Muchas veces las investigaciones y procesos se frustran porque no se cuenta con herramientas ni softwrare moderno para identificar a los ciberdelincuentes que muchas veces operan desde el extranjero. Esa situación no solo dificulta la labor de investigación sino que la pone en peligro pues si los casos no se resuelven en los plazos establecidos en la ley, campea la impunidad y crece la insatisfacción ciudadana respecto al sistema de administración de justicia.

Sub categoría 4: Vacíos de Punibilidad y Lagunas del Derecho

Sobre la existencia de lagunas del derecho, los fiscales entrevistados señalan que hay vacíos de punibilidad pues mientas no se modifique la Ley de Delitos Informáticos no se puede sancionar a los agentes que defraudan a través de las redes, por que se debe respetar el principio de legalidad. Además, los operadores jurídicos no cuentan con mecanismos eficaces para contrarrestar el uso de

programas modernos que emplean los ciberdelincuentes para acceder indebidamente a los correos y cuentas de los agraviados. Los delitos informáticos son ilícitos nuevos difíciles de probar por que se llevan a cabo en forma rápida y sin dejar huella, por lo que el Estado debe hacer campañas de divulgación y proporcionar equipos modernos a los operadores punitivos para proteger a la población.

Guía de entrevistas aplicada a abogados

Sub categoría 1: La ciberestafa en relación con el ciberdelito

Sobre cuál es la característica principal del ciberdelito, los abogados señalan que este es un delito sofisticado donde prima el uso de programas maliciosos para acceder indebidamente a las cuentas de usuarios incautos y apoderarse de su patrimonio. Señalan que la principal característica de la ciberestafa es el engaño que utilizan los delincuentes para sorprender a los agraviados. De acuerdo a las estadísticas el envío de links falsos y el engaño son las principales maniobras que utilizan los ciber-delincuentes. Sobre si consideran que se ha incrementado esta modalidad delictiva a raíz de la pandemia, señalan que sí han aumentado estos delitos porque la gente bajo la guardia por los altos índices de la pandemia, además tienen que comprar sus cosas por internet. La pandemia ha generado nuevas oportunidades para la delincuencia, los engaños se han multiplicado por el distanciamiento social y porque la gente no puede salir libremente de su casa por los impedimentos de tránsito que ha decretado el gobierno.

Sub categoría 2: Delitos informáticos en la legislación nacional

En relación a cuál es la característica principal del delito informático, mencionan que lo principal es el uso de tecnología que hace el hacker para apoderarse de datos del usuario básicamente de sus cuentas o claves para hacer transferencias no autorizadas a favor de sus cómplices, además usan programas maliciosos para infiltrarse en otras computadoras y robar información o claves de cuentas bancarias y asimismo envían enlaces fraudulentos a través de las redes y ultimadamente utilizan el engaño en todas sus variantes para apoderarse del patrimonio de sus víctimas, la mayoría de ellos señalan que la ciberestafa debe integrarse a la Ley de Delitos Informáticos para que estos hechos no queden impunes, aunque una

minoría opina lo contrario prefiriendo que esa conducta se mantenga en la estafa básica y también opina que no se debería incrementar la pena.

Sub categoría 3: Rol de los operadores jurídicos

Sobre cuáles son las principales dificultades que enfrentan los jueces, fiscales, la PNP y el Ministerio Publico en la persecución del delito informático, la principal dificultad que señalan es identificar al delincuente porque no es un delito cometido en flagrancia, mejor dicho, nunca se sorprende al delincuente en flagrancia porque hacen sus cosas a través de una computadora. La principal dificultad es identificar y ubicar a estos delincuentes escurridizos y la otra dificultad es superar las dificultades legales para continuar con éxito la investigación. La falta capacitación permanente no solo debe ser para las unidades especializadas sino también en provincias donde no hay estas unidades. Lo mismo debe ocurrir en el Ministerio Público.

Sub categoría 4: Vacíos de Punibilidad o Lagunas del Derecho

Respecto a las lagunas del Derecho los entrevistados sí creen que existen lagunas que se han hecho evidentes con la pandemia pues al generalizarse el uso del internet, los delincuentes han aprovechado esa oportunidad para cometer sus fechorías sin tener contacto directo con sus víctimas por lo tanto han tenido que usar las redes para perpetrar sus fraudes, pero como esa conducta no está tipificada en la ley especial no se les puede sancionar con esa norma por ende hay una laguna y subsistirá hasta que se modifique la ley.

Guía de entrevistas aplicada a policías

Sub categoría 1: La ciberestafa en relación con el ciberdelito

Los policías señalan que el ciberdelito es de carácter sofisticado pues los hackers se especializan en el uso de tecnología y programas para acceder a las cuentas de sus víctimas. Para combatirlos la DIRINCRI cuenta con una División Especializada de Delitos Informáticos que se encarga de investigar y hacer seguimiento a la ciberdelincuencia; sin embargo, reconocen que en las demás unidades la logística e infraestructura es precaria y en algunos casos obsoleta, por ello señalan que la policía requiere hacer una reingeniería de sus mecanismos de investigación, operativos y protocolos de intervención para combatir estos delitos.

Aseveran que la policía debe estar a la vanguardia en el uso de las tecnologías de la información y comunicación para que su labor sea más efectiva en la lucha contra los hackers.

Sub categoría 2: Delitos informáticos en la legislación nacional

Los policías entrevistados señalan que sí se cuenta con una legislación para sancionar los delitos informáticos, el problema es que no se cuenta con mecanismos y logística apropiadas para combatirla. Es decir, no es suficiente contar con instrumentos legales, sino que además se requiere equipos modernos que permitan a los operadores jurídicos llevar a cabo las investigaciones necesarias para lograr que se condene a los ciberdelincuentes. Añaden que los delitos informáticos seguirán en aumento si es que el Estado no cuenta con estrategias integrales que la enfrenten.

Sub categoría 3: Rol de los operadores jurídicos

Sobre cuáles son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático, señalan que es la falta de preparación tanto de policías como de fiscales y la falta de equipos modernos. Añaden que las investigaciones demoran mucho casi nunca se encuentra al culpable. No hay personal capacitado suficiente en las provincias, distritos y conos, por lo que la capacitación se debería descentralizar y crear unidades especializadas en todos los conos porque la población aumenta. Mientras no se superen estas dificultades no se reducirá la impunidad.

Sub categoría 4: Vacíos de Punibilidad o Lagunas del derecho

Los policías creen que la impunidad es el principal problema de la ley de delitos informáticos pues es difícil identificar a los ciberdelincuentes. Hay muchos requisitos para conseguir el levantamiento del secreto de las comunicaciones y ahora con la pandemia se ha incrementado el número de estafas en las redes que no siempre se pueden investigar en base a la ley especial. Además los ciberdelincuentes tienen experiencia en manejo de software y programas que les permite acceder a información sensible de las personas, sobre todo, aquellas ligadas a negocios, empresas y actividades comerciales por lo que los

ciberdelincuentes hacen un seguimiento y reglaje permanente que no está tipificado en la ley.

4.3. Análisis, discusión e interpretación de las categorías apriorísticas y emergentes relacionadas con los objetivos de la investigación

Sobre el objetivo específico 1, en base al análisis de las entrevistas se aprecia que la totalidad de informantes señalaron que tanto la policía como el Ministerio Publico afrontan serios problemas en la investigación del delito informático por la falta de capacitación oportuna y permanente de sus miembros en investigación informática, lo que debe conllevar a la necesaria especialización. Agregan que policías y fiscales no cuentan con equipos ni software moderno para combatir a la ciberdelincuencia, ya que estos delincuentes cuentan con herramientas sofisticadas para acceder ilícitamente a las cuentas de sus numerosas víctimas, mientras la fiscalía tiene serias deficiencias en equipamiento.

Por otro lado, la mayoría de los informantes coincidieron en señalar que la policía carece de recursos logísticos, infraestructura y presupuesto necesario para llevar a cabo su labor de modo efectivo. Aseveran que como la policía trabaja de la mano con el Ministerio Público, sus deficiencias y limitaciones afectan también la labor de la fiscalía. Por ello algunos participantes indicaron que se requiere mayor decisión política e institucional para corregir estas deficiencias ya que se requiere fortalecer las capacidades operativas de estos órganos de línea para lograr condenas. Añaden que existen vacíos en la Ley de Delitos Informáticos que imposibilita sancionar a los agente delictivos que usan las redes y el espacio virtual para embaucar a los usuarios con ofertas fraudulentas o el envío de links falsos. Los informantes policías señalaron por su parte que no por eso se debe dejar de sancionar severamente a los delincuentes que incurren en estas prácticas pues de lo contrario campearía la impunidad; versión que no fue compartida por los abogados, quienes indicaron que ello vulneraría el principio de legalidad pues se afectaría el derecho de defensa. Los jueces y fiscales se mostraron más cautos señalando que se puede reconducir estas conductas a la estafa básica y no por ello se deja de sancionar a los agentes delictivos, además el problema

más álgido es identificar al sujeto activo pues siempre actúan bajo las sombras.

Sobre el objetivo específico 2, luego de analizar e interpretar las entrevistas, la mayoría de informantes señalaron que es necesario que se sancione con más severidad a los ciberdelincuentes, incrementando las penas por que éstos nunca actúan solos para cometer sus fechorías, además estos delitos han crecido en forma desmesurada por la pandemia por lo que también ha crecido la sensación de inseguridad ciudadana, debido a que las personas se ven obligados a usar el internet para realizar sus compras o acceder a ciertos servicios, toda vez que la atención personal se ha restringido por el aislamiento social obligatorio. Sin embargo, algunos jueces y abogados no estuvieron de acuerdo con el incremento de las penas, señalando que éstas de por sí yan son drásticas y además no disuaden a los delincuentes. Como se advierte los resultados de estos objetivos específicos guardan relación con el objetivo general, respecto a la necesidad de modificar la Ley de Delitos Informáticos.

Sobre el objetivo general, del análisis y triangulación de las entrevistas, se desprende que casi todos los informantes señalaron que efectivamente existen deficiencias en la Ley de Delitos Informáticos que amerita modificaciones, habida cuenta que debido a la pandemia las estafas en las redes se han multiplicado en forma considerable, precisamente una de las deficiencias estriba en lo referente a la tipificación de las nuevas modalidades delictivas que han surgido por el aislamiento social obligatorio. También señalan que hay errores de técnica legislativa en lo referente a las penas, debido a que todos los delitos contra el patrimonio sancionan como mayor rigor al supuesto de pluralidad de agentes, situación que no acontece en esta ley especial. Cabe mencionar que una absoluta minoría opino que no es necesario la modificación de esta ley especial para incluir a las modalidades de estafa básica por el simple uso del internet. Esta opinión fue expuesta con claridad por Villavicencio (2014) quien asevera que no todo ilícito informático puede ser definido como tal por el solo hecho de haber usado una computadora. No obstante ello, los participantes señalaron que el gobierno debe efectuar

campañas de prevención para advertir a la población de estas nuevas formas delictivas para no convertirse en fáciles blancos de la ciberdelincuencia.

Como categorías emergentes se identificaron las siguientes: Desarrollo del comercio electrónico, hackers, transacciones virtuales, desplazamiento patrimonial, links fraudulentos y ciberdelincuentes. Se trata de categorías muy usuales en la actividad informática, por lo que son de pleno conocimiento por los operadores del Derecho. En ese sentido Jiménez (2017) asevera que desde la aparición del internet sujetos inescrupulosos escudándose en el anonimato utilizan el espacio virtual y las TIC para acceder a la información tratada y almacenada en bases de datos para luego sacar provecho de esa información.

Como categorías apriorísticas se identificaron las siguientes: Tecnologías de la información y comunicación, ciberdelito. Se trata de categorías que tienen que ver con la delincuencia informática que cada vez va en aumento y se hace más sofisticada precisamente por el uso de estas nuevas tecnologías para embaucar a sus víctimas.

4.4. Discusión de los resultados

Sobre el primer objetivo específico, a partir del análisis de la técnica de la entrevista aplicada se advierte que casi todos los entrevistados coinciden en señalar que es necesario incluir los verbos rectores de la estafa básica en la LDI para reducir la impunidad y la creciente sensación de inseguridad en la ciudanía ante la ola de timos cometidos a través de las redes. Las respuestas difieren solo en grado ya que los entrevistados poseen un concepto preciso de la estafa, conocen sus modalidades e implicancias y saben que las nuevas modalidades han crecido en forma exponencial por la pandemia. Todos coinciden que el contexto del COVID 19 ha ocasionado que los ciudadanos usen el internet para adquirir bienes y servicios, lo cual es aprovechado por los delincuentes para defraudar a las víctimas. También señalan que los delincuentes se han sofisticado porque usan recursos tecnológicos que les permite seguir operando en el anonimato por lo que se les debe poner coto para sancionar más severamente sus conductas y que éstas no queden en la impunidad.

Sobre estos vacíos de punibilidad García (2015) y Solano (2016) afirman que la imposibilidad de aplicar sanciones directas a un agente delictivo por vacíos defectos en la ley conlleva a veces a situaciones intolerables porque campea la impunidad, por ejemplo, cuando los elementos del tipo no se subsumen a plenitud en la conducta del sujeto de imputación, como acontece en ciertos delitos concursales; sin embargo, el a-quo sin vulnerar el principio de legalidad tiene que completar los vacíos pues no puede dejar de administrar justicia por defectos de la ley. En algunos casos puede utilizar cláusulas de extensión de punibilidad sin caer en la responsabilidad objetiva. Por nuestra parte somos de la opinión que estos problemas advertidos por los entrevistados pueden solucionarse con una modificación legislativa. Obviamente este no es el camino más corto, mientras tanto para evitar que la impunidad siga in crescendo, las autoridades deberían realizar campañas de divulgación a través de los medios de comunicación para advertir a la ciudadanía de las artimañas usadas por los ciberdelincuentes, habida cuenta que conforme lo prevé el artículo 139 inciso 8 de la Constitución, los jueces no puede dejar de administrar justicia por vacíos o deficiencias de la ley.

Sobre el segundo objetivo específico, acerca de los problemas que afrontan los fiscales y la policía nacional para combatir el ciberdelito, todos los informantes coinciden en señalar que aparte del crecimiento de la ciberdelincuencia, uno de los problemas más álgidos de policías y fiscales es la falta de capacitación y especialización en criminalidad informática, lo cual se ha vuelto más urgente por la pandemia, ya que los delincuentes hacen de las suyas al saber que resulta difícil detectarlos. Esta versión se corrobora con los resultado del Informe N° 4 sobre la Ciber-delincuencia en el Perú, publicado por la Oficina de Análisis Estratégico contra la criminalidad del Ministerio Publico, en cuya Tabla (que se incluye en los anexos), se aprecia el crecimiento del delito informático en las fiscalías penales, comunes y mixtas de todo el país del año 2013 al 2020. La falta de capacitación impide a los operadores punitivos perseguir con eficacia el ciberdelito; además, los entrevistados advierten que tanto fiscales como la policía enfrentan otro problema que es la falta de logística, en el caso de la policía el asunto es más acuciante pues solo tienen una unidad especializada que opera en el centro de Lima, en el resto de dependencias la policía trabaja con equipos

obsoletos, lo mismo pasa con las fiscalías penales comunes que operan en el resto de Lima y a lo largo y ancho del país.

Respecto a la discusión de estos resultados, de acuerdo a las cifras que maneja la policía una persona al ingresar al internet está expuesta a más de 50 ataques por minuto, por ello, en la estadística de casos reportados por la DIVINDAT a la Oficina de Análisis Estratégico contra la criminalidad de la Fiscalía de los años 2013 a 2020, se aprecia que de 12,169 casos registrados, el 78.2% corresponde a delitos contra el patrimonio, es decir, fraude informático en sus diversas modalidades, lo que constituye el grueso del trabajo de investigación, por lo cual recomiendan no abrir link extraños, ni responder a correos de personas desconocidas.

En ese orden de ideas Paredes (2013) analiza el impacto que ha tenido en el avance del ciberdelito el uso de las TIC para facilitar la comisión de esos delitos, así como los conflictos entre seguridad y privacidad, por ello, aparte de recomendar modificaciones legislativas puntualiza que la especialización es imprescindible. Concordamos con esa conclusión pues es imperativo dotar de mejores herramientas técnicas (capacitación) y tecnológicas tanto a la policía nacional como a la fiscalía para combatir con mayor eficacia el ciberdelito.

Acerca del objetivo general, en torno a los fundamentos socio-jurídicos para tipificar la estafa básica en el capítulo de delitos contra el patrimonio de la LDI, la señora juez codificada como J2, señaló como casi todos los informantes que la pandemia, el distanciamiento social y el aislamiento social obligatorio fueron los factores sociales que obligaron al común de las personas a utilizar el internet para proveerse de bienes y servicios que necesitaban para satisfacer sus necesidades básicas. También se vieron obligados a usar el internet para informarse de los programas de vacunación, el cobro de bonos y las restricciones de tránsito que imponían las autoridades. Las empresas por su parte tuvieron que adecuar su producción, sus ofertas y su cadena de distribución a esta nueva realidad para evitar caer en la bancarrota; por lo tanto, de esa problemática social surgió una nueva veta de posibilidades, tanto las que se relacionaban con la dinamización de la tecnología para afrontar estos nuevos retos, una de ellas, es el trabajo remoto, así como las que se relacionaron con la gran cantidad de ofertas fraudulentas que emergieron por las redes, supuestamente para satisfacer a

miles de usuarios que imposibilitados de acudir a los tradicionales centros comerciales, tenían que usar el internet para continuar su vida cotidiana.

Vale decir que la tecnología y las plataformas informáticas fueron usadas para el bien y para el mal. En ese orden de ideas Mitcham (2015) al tratar sobre la filosofía y la ética de la tecnología, señala que la tecnología tiene vinculación estrecha con la economía, debido a que está orientada básicamente a reducir los costos, situación que acarrea beneficios para la empresa y su entorno; empero, para evitar caer en excesos, se debe establecer un nuevo contrato social para la ciencia y la tecnología, para evitar los peligros del mal empleo de estas últimas y/o la distorsión de la información. Recomienda por ende perfilar una visión humanística de la tecnología con respeto a los derechos humanos.

Sin embargo, no todos los teóricos comparten esta posición, por cuanto Heidegger (2001) en su conferencia La pregunta sobre la técnica, señalo que cualquier innovación tecnológica no es más que ciencia aplicada para resolver problemas concretos, la idea innovadora nace para satisfacer necesidades concretas y por eso es neutral, por ello la aplicación práctica y los malos usos de la tecnología no es un problema del creador sino de los ingenieros y tecnócratas del gobierno de turno. Por nuestra parte compartimos la posición de Mitcham ya que si bien es el ser humano quien usa para bien o para mal las nuevas tecnologías, por ejemplo el mal uso que hacen de las TIC los ciberdelincuentes, no por ello las autoridades se deben quedar con los brazos cruzados, pues el derecho como ciencia normativa debe intervenir para regular desde la órbita penal este tipo de situaciones que causan perjuicios a los usuarios de buena fe.

4.5. Conclusiones aproximativas

Del análisis de las cifras publicadas por la Policía Nacional y el Ministerio Publico se aprecia que el problema es álgido, pues los ciberdelincuentes sabedores de lo difícil que resulta detectarlos continúan desplegando sus nefastas maniobras en las redes, ofreciendo sus servicios para facilitar el cobro de bonos a personas de extrema pobreza o a personas que han perdido su empleo, en donde luego de propiciar el engaño suplantan la identidad de sus víctimas. Cabe indicar que el debate de incluir o no los verbos rectores de la estafa básica en la Ley de Delitos Informáticos existía desde hace varios años, empero, ha sido la coyuntura de la

pandemia ocasionada por el COVID 19 y la adaptación a una vida social digitalizada y realizada en entornos remotos lo que propicio que los fraudes y timos crezcan en forma exponencial en perjuicio de miles de usuarios.

Por ende, en este acápite se identifican las debilidades y fortalezas de la problemática estudiada, pues hubo un reducido número de entrevistados (abogados) que opino no estar de acuerdo en que se incluyan los verbos rectores de la estafa básica en la Ley de Delitos Informáticos ni que se incremente la pena ante la intervención de pluralidad de agentes, señalando básicamente que no todo conducta puede enmarcarse en esa ley especial por el mero hecho de utilizar una computadora, por lo que esas conductas deben permanecer en estafa tradicional coincidiendo con la posición del tratadista Felipe Villavicencio (2014). Añadieron que las penas ya de por si son severas y que no son disuasivas por lo que en nada contribuyen para reducir la impunidad.

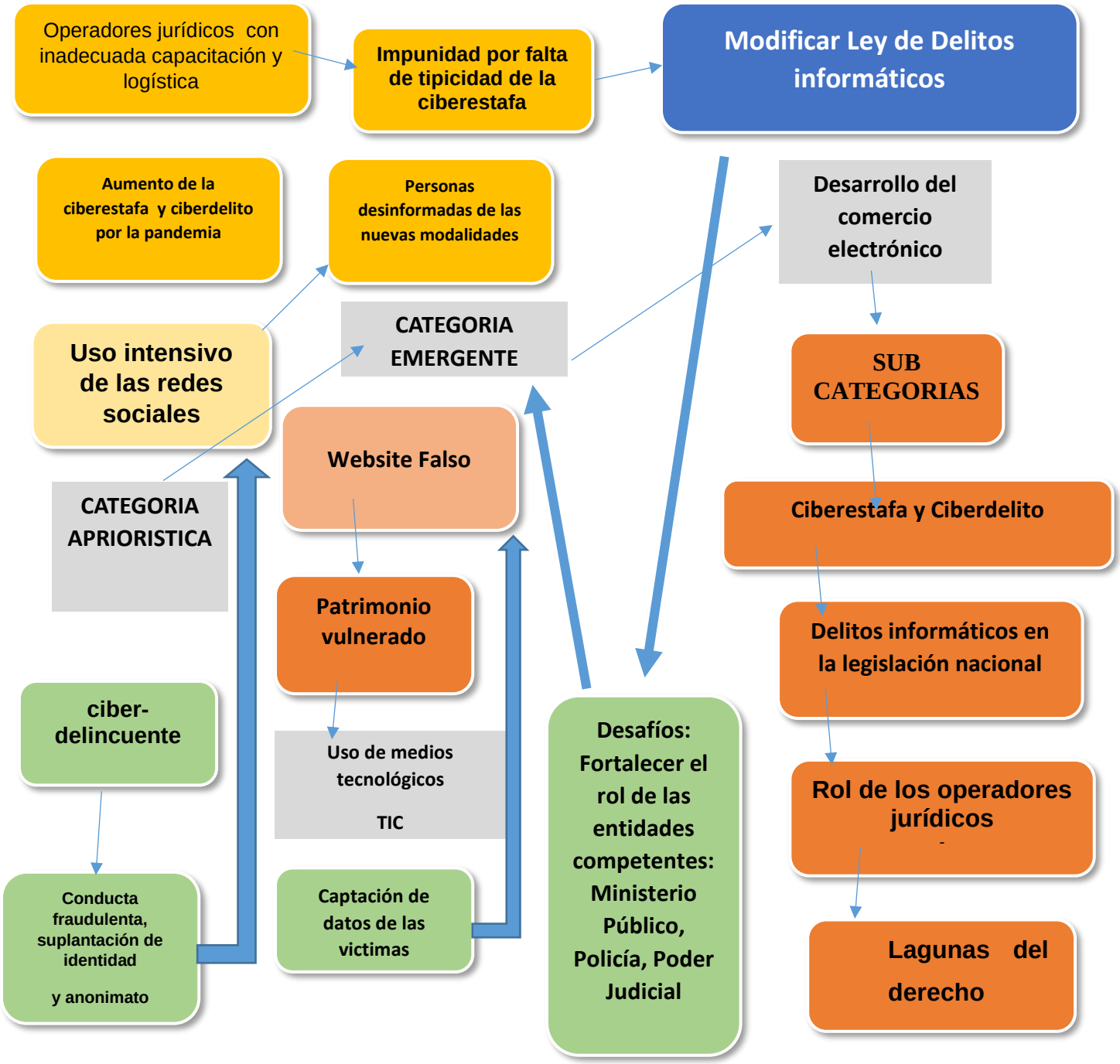
No se comparte esta posición porque si bien se apoya en la opinión de un ilustre jurista como lo es el Dr. Villavicencio, su estudio data del año 2014, fecha en la que no había surgido esta necesidad imperiosa de utilizar el internet para adquirir bienes y servicios, ya que la pandemia surgió en marzo de 2020, por lo que al ser distintas las situaciones fácticas, distintas también deben ser las soluciones al problema planteado. Por otra parte, de la revisión de fuente documental (teorías y doctrina) existente y a partir del análisis de la técnica de la entrevista, son pocos los autores que señalan compartir la posición de Villavicencio, por ejemplo Gonzales (2014) asevera que solo estamos ante una ciberestafa cuando el sujeto activo privilegia el uso de las TIC sin que sea necesario el engaño previo. Por su parte, Rico (2013) señala que la multiplicidad de conductas fraudulentas por la expansión del internet ha dificultado encuadrar estas conductas en los tipos penales tradicionales, por lo que el legislador ha debido revisar y adecuar la legislación penal existente para evitar la impunidad de estas conductas en donde el factor principal es el uso de las TIC y el engaño a la víctima para provocar el desplazamiento patrimonial.

Otro autor que asume una postura contraria a la nuestra es Balmaceda (2011) quien analizando la legislación española, explica que el fraude informático y la estafa informática comparten el uso de artimañas para lograr un beneficio personal en perjuicio ajeno; sin embargo para este autor, el fraude informático es

una categoría criminológica más amplia pues involucra maniobras técnicas e intereses económicos heterogéneos no solo patrimoniales, en cambio, la estafa informática alude solo a defraudaciones patrimoniales realizadas por medios informáticos. La propuesta del autor es que a ambos supuestos se les brinde un tratamiento homogéneo pese a la existencia de posiciones doctrinarias dispares en lo referente a los límites de esas conductas.

Figura 1:

Conclusiones aproximativas. Codificación selectiva



4.6. Validez del estudio

En este estudio se han empleado diversos criterios de rigor científico para arribar a las conclusiones. Así luego de obtener la validación de los instrumentos por un juicio de expertos, se escogió a los entrevistados atendiendo a su experiencia en el tema. Acto seguid se procedió a analizar las entrevistas de modo individual y conjunta contrastando las respuestas por subcategorías y objetivos. Esto nos permitió tener una visión amplia del tema y comprender las implicancias que conlleva nuestro propuesta de modificar la LDI. Los entrevistados mostraron interés en la problemática y alcances del estudio, y solicitaron que sus aportes sean dados a conocer a fin de que se puedan implementar. A partir de los resultados se identificó sub categorías apriorísticas y emergentes, las que tienen como eje articulador el problema de investigación, el mismo que se ha detallado en la figura que antecede a través de una codificación selectiva. El resultado pues posee las siguientes características:

a) Dependencia. Nos ha permitido revisar los resultados de otros investigadores que han examinado la problemática desde otras aristas, por ejemplo Pardo (2018) en su estudio sobre los delitos informáticos propone diversas modificaciones en la LDI, aseverando que la conducta de los agentes no solo afecta al patrimonio sino también la privacidad de las personas, sin que la sanción prevista corresponda con la afectación del bien jurídico protegido; **b) Credibilidad**. Surge del análisis de los datos recogidos en el campo, tiene que ver con la correspondencia entre la forma en que el participante percibe los conceptos vinculados al problema y la manera como se retratan esos puntos de vista, evitando caer en subjetividades; **c) Transferencia**. Este presupuesto no implica generalizar las conclusiones a una población más amplia; empero, su esencia puede aplicarse a fenómenos similares; **d) Confirmabilidad**. Tiene estrechos vínculos con la credibilidad, sirve para demostrar que el investigador ha minimizado los sesgos, subjetividades y tendencias, lo que implicó rastrear las fuentes, los instrumentos usados y explicar la lógica que se empleó para interpretar los resultados.

V. CONCLUSIONES

PRIMERA:

Los fundamentos socio-jurídicos para tipificar de *lege data* la estafa básica en el capítulo de delitos contra el patrimonio de la LDI, tienen que ver con la aparición de la pandemia originada por el Covid 19, originándose desde ese momento una alta incidencia de casos y denuncias tanto ante la policía como ante el Ministerio Publico, lo cual evidencia que la delincuencia ante este nuevo escenario se ha sofisticado y hace uso de la internet y las TIC para desplegar su conducta nociva, por lo que se hace necesario que se sancione con más severidad a los agentes delictivos que engañan e inducen a error a sus víctimas apoderándose de su patrimonio.

SEGUNDA:

La tipificación de la estafa básica en la LDI coadyuvará a reducir la impunidad de los delitos informáticos, ya que se englobarán en una misma ley los limites difusos con otras figuras fraudulentas como el vishing, el smishing y el phishing. En todas estas figuras media el engaño como elemento central, por lo que deben recibir el mismo tratamiento punitivo como política criminal del Estado.

TERCERA:

Los problemas que afrontan policías y fiscales en la investigación del ciberdelito tienen que ver con falta de personal idóneo y capacitado, falta de equipos informáticos y logística adecuada que le permita obtener evidencia digital con dictámenes periciales positivos para llevar a juicio a los ciberdelincuentes.

CUARTA:

El trabajo empírico y de los aportes de la gran mayoría de entrevistados se desprende la necesidad de incrementar la pena cuando interviene una pluralidad de agentes en la comisión de delitos contra el patrimonio de la LDI. Este aumento de la pena concuerda con lo previsto en los demás delitos contra el patrimonio; empero, debe estar integrado a una política criminal del Estado.

VI. RECOMENDACIONES

PRIMERA: El Ministerio Público y la PNP deben implementar una estrategia conjunta para prevenir la comisión de los delitos informáticos. Esto conlleva a la capacitación permanente de personal, la creación de un sistema de alertas tempranas y un laboratorio especializado en el tratamiento de la evidencia digital que cuente con equipos modernos. Esta labor en equipo coadyuvará a reducir la impunidad en estos delitos.

SEGUNDA: Los proyectos destinados a cerrar las brechas de las lagunas de punición en los delitos informáticos y en los de criminalidad organizada formuladas al amparo de la Ley Nº 29807 deben discutirse en la Comisión de Justicia del Congreso de la Republica. Estos debates deben tener la debida prioridad en el marco de la política criminal del Estado en la lucha contra el ciberdelito, como manifestación de un eficaz control social y solución preventiva de conflictos.

TERCERA: Descentralizar las funciones de la Unidad Fiscal Especializada en Ciber-delincuencia del Ministerio Publico materia de la Resolución N° 1503-2020-MP-FN, así como las labores del Laboratorio de Ciberdelincuencia, en el Norte, Sur, Centro y Oriente del país a fin de que no todo se centralice en Lima, además dicha dependencia debe celebrar convenios de cooperación con las principales redes internacionales como Ciber Red, Redcoop, Iber Red, etcétera, con el objeto de obtener información en tiempo real del ciberdelito transfronterizo.

CUARTA: Descentralizar las labores de la DIVINDAT, en el Norte, Sur, Centro y Oriente del país con su respectivo laboratorio de Análisis Digital Forense dedicado a analizar la evidencia digital con el objeto de que no todo se centralice en Lima, por los consabidos cuellos de botella, para lo cual el Ministerio del Interior como titular del pliego debe gestionar la asignación de presupuesto necesario.

QUINTA: Desde el punto de visto académico se recomienda investigar las discordancias punitivas existentes entre la conducta descrita en el artículo 183 B del C.P. (proposiciones a menores con fines sexuales) con la sanción prevista en el artículo 5 de la LDI (proposiciones a menores con fines sexuales por medios tecnológicos), falencia que fue advertida por una jueza entrevistada.

VII. PROPUESTA

En el presente estudio se plantea la modificación de *lege data* del artículo 8 de la Ley de Delitos Informáticos a fin de que se incluyan los verbos rectores de la estafa básica en la precitada norma y se incremente la pena si interviene una pluralidad de agentes, lo cual redundará en la reducción de la impunidad en el país, por lo que se ha esbozado una exposición de motivos para modificar dicha ley.

Asimismo, se plantea fortalecer la capacidad operativa del Ministerio Público-Fiscalías Especializadas y de la Policía Nacional-DIVINDAT desde los siguientes aspectos:

Aspectos logísticos e institucionales en la lucha contra el ciberdelito.

Dotar de capacitación permanente al personal fiscal y a los efectivos policiales especializados en la lucha contra el ciberdelito.

Fortalecer y promover buenas prácticas en la investigación del ciberdelito, así como aprobar protocolos de actuación conjunta y estándares de ciberseguridad para obtener sin cuestionamientos la evidencia digital, lo que permitirá llevar a juicio los casos investigados.

Contar con mecanismos de prevención, reactiva y proactiva para cautelar la privacidad y confidencialidad de la información que se obtenga en bases de datos de personas naturales y jurídicas afectadas por la comisión del ciberdelito.

En ese sentido entre los principales objetivos se tiene:

1) Cruzar información interinstitucional en todo lo relativo a la ciberdelincuencia.

2) Administrar un sistema de cooperación y base de datos conjunta para combatir con mayor eficacia el ciberdelito.

3) Promover la aprobación de protocolos de actuación interinstitucional que incluya al Poder Judicial para agilizar los procedimientos y la obtención de medidas cautelares en el marco de la lucha contra la ciberdelincuencia; 5) Promover campañas de concientización ciudadana sobre ciberseguridad, a fin de evitar que sean presa fácil de los ciberdelincuentes.

Criterios y lineamientos en la lucha contra el ciberdelito.

Promover y fortalecer las buenas prácticas en ciberseguridad de los operadores punitivos y de los órganos de administración de justicia a fin de que se tenga cuidado en mantener la privacidad de la información obtenida en la ejecución de las medidas cautelares, que no tengan o guarden relación directa con el objeto de investigación.

Contar con mecanismos adecuados para incrementar la capacidad de respuesta del sistema ante incidentes de ciberseguridad que afecten la privacidad y confidencialidad de la información sensible de las personas, dentro de los parámetros de la seguridad digital del Convenio de Budapest.

La Agencia Peruana de Cooperación Internacional, la Oficina de Proyectos y Cooperación Técnica Internacional del Ministerio Publico, así como el Consejo Nacional de Política Criminal creado en virtud de la Ley Nº 29807 deben asumir un rol más proactivo, para que la Autoridad Central en materia de cooperación jurídica internacional celebre convenios con agencias gubernamentales como el Programa Global de Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito, en el marco del Convenio de Budapest para recibir asesoría técnica e intercambiar información sobre el ciberdelito transfronterizo.

EXPOSICION DE MOTIVOS DEL PROYECTO DE LEY QUE MODIFICA EL ARTICULO 8° DE LA LEY N° 30096

I FORMULA LEGAL

Artículo 1º Objeto de la ley

Modificar el artículo 8º de la Ley Nº 30096, Ley de Delitos Informáticos.

II EXPOSICION DE MOTIVOS

1.Fundamentación jurídica

De conformidad al artículo 75 del Reglamento del Congreso, se expresan los fundamentos jurídicos y socio-económicos que hacen viable la modificación de una ley ordinaria, teniendo en cuenta que el artículo 102 inciso 1 de la Constitución prevé como atribución del Congreso de la República, expedir leyes y resoluciones legislativas, así como interpretar, derogar o modificar las existentes.

En ese sentido se ha advertido que a raíz de la pandemia generada por el SARS-Cov-2, han surgido una serie de conductas nocivas en el ciberespacio que causan severos perjuicios a los ciudadanos que se ven urgidos de utilizar el internet para adquirir diversos bienes y servicios, por el aislamiento social obligatorio impuesto por el gobierno central por razones de salud pública.

De esta situación se aprovecha la ciberdelincuencia para timar a ciudadanos incautos o a aquellos que por aspectos culturales o generacionales tienen dificultad para identificar las plataformas digitales y/ o sitios web reales de los falsos, siendo una práctica usual de los ciberdelincuentes el envío de ofertas fraudulentas a través de las redes sociales, paralelo al envío de links impregnados de malware para que las personas atraídas por estas ofertas remitan dinero a cuentas bancarias creadas ex profeso o envíen sus datos personales y números de cuenta que van a dar a manos de estas organizaciones criminales.

2. Justificación de la propuesta legislativa

Los límites entre la estafa propiamente dicha, cometida en el espacio virtual con otras figuras delictivas como el phishing, el vishing y el smishing son muy difusas, en todas ellas prima el engaño como elemento central, la diferencia es de grado o por la TIC empleada por el agente, lo cual causa severas dificultades al operador jurídico al momento de realizar la subsunción correspondiente para sancionar dicha conducta, generándose una suerte de impunidad intolerable. En ese sentido, la modificación se justifica, habida cuenta las numerosas denuncias que se divulgan en forma copiosa en los medios de comunicación, situación que acrecienta la sensación de inseguridad en la ciudadanía.

La propuesta modificatoria y el resto de la exposición de motivos se remite a los anexos.

REFERENCIAS

Arbaiza, L. (2016). Cómo elaborar una tesis de grado. Esan ediciones.

Ascott, R. (2014). *The future is now: Art, technology and consciousness*, University of Plymouth Press.

Arocena, L. y Esparza, I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. *Novum Jus*,11, (1), 39-72 https://doi.org/10.14718/NovumJus.2017.11.1.2

Arteaga, A., Medellin, E .y Santos, M. (1995). Dimensiones sociales del cambio tecnológico [versión electrónica] *Revista de ciencias sociales Nueva Antropología*, (47), 9-22.

Atienza, G. y Bermejo, D. (2020). *Ciberdelitos*, Experiencia ediciones. https://books.google.com.pe/books?hl-es.els-&id-wfcqEAAAQ

Avila Umaña, J., Barrera Argueta, A., Monjaras Diaz, F. (2018). Elementos diferenciadores del delito de estafa regulado en el artículo 215 del Código Penal con la estafa informática regulada en la ley contra delitos informáticos y conexos. (Trabajo de grado para obtener el título de licenciado, Universidad de El Salvador).https://ri.ues.edu.sv/id/eprint/16675/1/%20.pdf

Balmaceda, G. (2011). El delito de estafa informática en el derecho europeo continental [versión electrónica]. Revista de Derecho y Ciencias Penales de la Universidad San Sebastián (17), 111-149.

Bauman, Z. (2016). Liquid Times: Living In An Age Of Uncertainty. Cambridge: Polity Press.

Bobbio, N. (2005). Teoría General del Derecho (3a. ed.). Temis.

Bustos, A. y Zúñiga, C. (2013). Análisis de los delitos informáticos en el derecho chileno y comparado [Tesis de Licenciatura], Universidad Andrés Bello. http://repositorio.unab.cl/xmlui/bitstream/handle/rio/

Cámara Peruana de Comercio Electrónico de Lima (2019). Reporte Oficial de la Industria E- commerce en Perú, crecimiento de Perú y Latinoamérica 2009-2019. Capeco.

Chávez, E. (2018). El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de Lima Norte 2017. (Tesis doctoral, Universidad Nacional Federico Villareal).

Devía, E. (2017). Estafa informática del artículo 248.2 del Código Penal (Tesis doctoral, Universidad de Sevilla). http://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%completa%final%2031

Dworkin, R. (2014). Sovereign Virtue: The theory and practice of equality. Cambridge MA: Harvard University Press. http://isbn:84-49314364.sovereign/virtue/com/view

Elias, R. (2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú, (Documento de trabajo N° 1), Hiperderecho, organización civil sin fines de lucro. http://www.hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informatica-en-peru

Espinosa, J. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. *Revista La Razón Histórica*, (44) 153-173. https://www.dialnetunirioja.es/servlet/articulo?codigo7368868

García, P. (2015). Derecho Penal Económicom (Volumen 1, 2° edición). Instituto Pacifico editores.

García, D. (2018). El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero. *Revista Boliviana de Derecho Iuris* Tantum ISSN-2070-8157 (25) 42-65. https://www.Scielo.php2scrip-sci_arttextxt&pid-s2070-8157201800025

García, J. y Peña, D. (2017). Cibercriminalidad y Postmodernidad: La cibercriminología, respuesta al escenario contemporáneo. https://www.perso.unifr.ch/derpenal/assets/files/art/a_20170408_03.pdf

Gonzales, J. (2013). Delincuencia informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma (Tesis doctoral) Universidad Complutense de Madrid, https://www.dialnet.unirioja.es/serlet/Tesis?codigo-39078

González, M. (2014). Fraudes en internet y estafa informática. (Trabajo de fin de Master) Universidad de Oviedo.

htpps://www.documents/doctor%quispe%20Tesis/TFM_gonzalez%pdf

Feyerabend, P. (2010). *Tratado contra el método*. (2° ed.) Tecnos, S.A.

Hancco, E. (2017). La tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la Ley 30096. (Tesis de licenciatura) Universidad Nacional de San Agustín.

Hart, H. (1983). Essays in jurisprudence and philosophy. Oxford University Press, htpps://oxforduniversitypress.scholarship.com/view/978019824/acpro:oso/

Heidegger, M. (2001). Conferencias y artículos de Martin Heidegger (2da ed.). Traducción de Eustaquio Barjau. Ediciones del Serbal S.A.

Hernández, L. (2009). El delito informático. *Revista Jurídica Eguzkilore*, 23

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación* (6ta ed.). Mc Graw Hill/interamericana editores S.A.

Hernández-Sampieri, R. y Mendoza, P. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* Mcgraw-Hill Interamericana.

Jain, N. y Shrivastava, V. (2014). Cyber Crime changing everything- An empirical study. International Journal of Computer Application, 4 (1). 62-77. http://www.republication.com/ijica_index.htm

Jiménez, J. (2017). Manual de Derecho Penal Informático. Jurista editores.

Luppicini, R. (2020). Digital transformation and innovation explained: Ascoping review of an evolving interdisciplinary field.University of Ottawa Press.

Luyo, M. y Paz, D. (2021). El comercio electrónico a raíz de la pandemia. Oportunidades de mejora en materia de protección al consumidor en el Perú. *Revista Actualidad Jurídica*, 327 (1), 169-182.

Martin, L. (2018). Filosofía de la técnica y de la tecnología. ISBN 9788478485987. http://www.helicon.es/pen/7848598.htm

Martínez, V. (2013). Paradigmas de investigación. Manual multimedias para el dessarrollo de trabajos de investigación. Una visión desde la epistemología dialéctica crítica. Manual biblioteca UDG virtual. http://www.148.202.167.116:8080/mlui/bitstrem/handle/123456789/3790.

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos [versión electrónica]. *Revista Ius et Praxis de la Universidad de Talca*, 24 (1),159-206.

Mazuelos, J, (2001). Los delitos informáticos, una aproximación a la regulación del Código Penal peruano. *Revista de Doctrina y Jurisprudencia Penales*.

Ministerio del Interior del Perú (2016). Ciberpolicías contra delitos informáticos.

https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Mitcham, C. (2015). *Ethics, science, technology,engineering: A global resource*, (2° ed.). J. Britt Holbrook, Published by Mac Millan Reference USA.

Monterrosa, A., Escobar, J. y Mejía, J. (2015). Por una revaloración de la Filosofía de la Técnica [versión electrónica]. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad*, 10 (30), 265-275.

Morillas, D. (2017). Delitos Informáticos. Material de la Maestría en Derecho Penal Económico Internacional. Universidad de Granada.

Nozick R. (1988). *Anarchy, State and Utopia*. Harvard University Press

Ñaupas, H., Mejía, E., Novoa, E. y Villagomez, A. (2011). *Metodología de la investigación científica y asesoramiento de tesis*. (2da ed.). Editorial de la Universidad Nacional Mayor de San Marcos.

Oficina de Análisis Estratégico Contra La Criminalidad-Ministerio Público (2021). Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada (Informe de Análisis N° 04).

Palacio, S. (2018). El desafío de la ciencia, el cambio tecnológico y la innovación, Revista de Ciencia y Tecnología. Infotec. htpp://www.Infotec.repositorio institucional.mx/bitstream/handle/21805/pdf

Palomino, W. (2014). El intrusismo y otros delitos informáticos regulados en la Ley N° 30096. *Gaceta Penal & Procesal Penal*, 56.

Pardo, A. (2018). Tratamiento Jurídico Penal de los delitos informáticos contra el patrimonio, distrito judicial de Lima (Tesis para optar el grado de Maestro en Derecho Penal y Procesal Penal, Universidad César Vallejo).

Paredes, J. (2013). De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010 (Tesis para optar el grado de Maestro en Derecho Penal). Universidad Nacional Mayor de San Marcos. http://www.cybertesis.unmsm.edu.pe/handle/20.500.12672/10314

Pérez, J. (2019). Delitos Regulados en leyes especiales. Editorial Gaceta Jurídica.

Pinedo, C. (2021). Crimen organizado y lavado de dinero mediante criptoactivos en el contexto del fenómeno expansivo Fintech en Perú. *Gaceta Penal & Procesal Penal*, (139) 12-27.

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de la realidad física a una realidad virtual. [versión electrónica]. *Revista Nuevo Foro Penal*, 13 (88), 72-112.

Quevedo, J. (2017). Investigación y prueba del ciberdelito (Tesis doctoral) Universitat de Barcelona.

https://www.Tdx.ciet/bitstream/handle/10803/665611/JQG_Tesis.pdf?

Ramírez, E. (2010). Proyecto de investigación cómo se hace una tesis. Fondo editorial AMADP.

Reyna, L. (2016). Criminalidad informática, crimen organizado e internacionalización del delito. En: L. Zúñiga y F. Mendoza (Eds.), Ley Contra El Crimen Organizado-Ley N° 30077. (pp.199-236). Instituto Pacifico.

Rico, M. (2013). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. Revista IUS 1 (31), 19-35.

Romeo, C. (1996). Delitos informáticos de carácter patrimonial [versión electrónica]. *Revista Iberoamericana de Informática y Derecho* (9) 413-442.

Russell, B. (1961). The Scientific Outlook, Essay, London UK, George Allen & Unwind Press.

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal. *Revista Erreius Suplemento Especial*, 7-32, htpps://www.errepar.com/resources/descargacontenido/cibercrimen.pdf

Salinas R. (2013). Derecho Penal Parte Especial (5° edición). Grijley.

Sánchez, J. (2016). Manual Auto instructivo-Curso Delitos Informáticos. Academia de la Magistratura.

Segura, M. (1989). El problema de las lagunas en el derecho. *Anuario de Filosofía del Derecho, 6*, 285-312, htpps://www.dialnet.unirioja.es/servlet/articulo?codigo-1985307.pdf

Singer, P. (2018). Ethics, technology and the future of mankind [Conference]. June 10, 2018, At headquarter of World Intellectual Property Organization, Geneva Switzerland. htpps://www.wipo_magazine/en/2018/04/article_005.html

Solano, H. (2016). Introducción al estudio del derecho. Editorial Universidad Pontificia Bolivariana.

Staudenmaier, J. (2002). Rationality, agency, contingency: Recent trends in the history of technology. *Review in American History*, 30, 165-181, htpps://doi.org/10.1353/researchgate. net/publication/ 236765461

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. *Revista Erreius Suplemento Especial*, 49-68, htpps://www.pensamientopenal.com.ar/system/files/2018/09/doc46963.pdf

Vicente, F. (2017). Las lagunas del derecho. (Trabajo de fin de grado en filosofía del Derecho). Universidad de Salamanca, htpps://www.grado.usal.es/bitstream/handle/10366/132775/TG_vicente avila_lagunas.pdf

Villavicencio, F. (2014). Delitos Informáticos. *Revista Ius et Veritas*, 24 (49), 284-304.

Wessel, M. y Helmer, N. (2020). A crisis of ethics in technology innovation, Magazine Spring Issue march, MIT Sloan Management Review, htpps://sloanreview.mit.edu/article/a crisis-of-ethics/birstreamhandle/

Zaffaroni, E. (2014). *La cuestión criminal.* (2° ed.). Editorial Planeta.

Zevallos, O. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E commerce?, *Ius 360*, htpps://www.ius360.com/estudios-muniz/delitos-informáticos.

ANEXOS

ANEXOS

Anexo 1: Matriz de categorización específica

Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad en el Perú

Categorías apriorísticas	Subcategorías apriorísticas	Indicadores	Preguntas
Tipo básico de estafa en la Ley de Delitos Informáticos	La estafa básica	1) Definición de la estafa básica 2) Incremento de esta modalidad delictiva por la aparición de la pandemia 3) Conductas típicas más frecuentes	1) ¿Cuál es la característica principal de la estafa como delito contra el patrimonio? 2) ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia por covid 19? Explique su respuesta 3) ¿Cuáles son las modalidades más usuales utilizadas por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión qué se puede hacer al respecto?
	El delito informático	4) Definición de delito informático 5) Deficiencias en la Ley de Delitos Informático 6) Características de los agentes delictivos	1) ¿Según su criterio, cuál es la característica principal del delito informático? Explique su respuesta. 2) Considera usted que existen deficiencias en la actual Ley de Delitos Informáticos? Explique su respuesta. 3) Considera usted que se requieren conocimientos avanzados de informática para provocar estafas a través del internet?
Impunidad por ausencia de la tipificación propuesta	Vacíos de punibilidad en la Ley de Delitos Informáticos	7) Vacíos en la Ley de delitos Informáticos 8) Necesidad de incluir la estafa básica en la ley especial 9) Necesidad de incrementar la sanción punitiva	1) ¿Considera usted que existen vacíos en la actual Ley de Delitos Informáticos para sancionar conductas delictivas? ¿Precise cuáles? 2) ¿Considera usted que es necesario incluir el tipo básico de estafa en la Ley de Delitos Informáticos? Explique su respuesta. 3) ¿Considera usted necesario que se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta.
	Desarrollo del comercio electrónico a raíz de la pandemia	10) El aislamiento social obligatorio 11) El papel de las TIC en el E-commerce 12) Uso generalizado del Internet para realizar defraudaciones	1) ¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio impuesto por el gobierno central? Explique su respuesta. 2) ¿Cómo evalúa usted el papel de las tecnologías de información y comunicación en el desarrollo del comercio electrónico? 3) ¿Cree usted que la pandemia por el COVID 19 ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.
	Rol de los operadores de justicia	13) Dificultades de los operadores punitivos 14) Falta de especialización 15) Falta de logística	1) ¿Según su criterio cuáles son las principales dificultades que enfrenta la Policía Nacional y el Ministerio Publico en la persecución de los delitos informáticos? 2) ¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito? 3) ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?

Anexo 2: Matriz de consistencia

Título: Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad

<table>
<tr><th>Formulación del problema</th><th>Objetivos</th><th>Categorías</th><th>Técnica e Instrumentos</th></tr>
<tr>
<td>

Problema general

¿A raíz de la pandemia, por qué es necesario incluir el tipo básico de estafa en la ley de delitos informáticos N° 30096 para reducir la impunidad?

Problemas específicos:

1. ¿Qué problemas afrontan los operadores punitivos para subsumir la conducta de los estafadores informáticos en la Ley Especial N° 30096?

2. ¿Qué dificultades afrontan los operadores punitivos de Lima Norte para acreditar el ciberdelito?
3. ¿De qué manera se pueden solucionar los concursos reales o aparentes ante la ausencia del tipo básico de estafa en la Ley N° 30096?

</td>
<td>

Objetivo general

Sustentar los fundamentos socio-jurídicos para que se tipifique de *lege data* la estafa básica en el capítulo de delitos contra el patrimonio de la LDI, con lo cual se sancionaría a los agentes delictivos que usan el Internet y las TIC para engañar e inducir a error a sus víctimas apoderándose de su patrimonio.

Objetivos específicos

1. Reducir la impunidad
2. Determinar los problemas que afrontan policías y fiscales en la investigación del ciberdelito.
3. Esbozar la necesidad de incrementar la pena cuando interviene pluralidad de agentes en la comisión de delitos contra el patrimonio de la LDI.

</td>
<td>

Categorías y subcategorías

<table>
<tr><th>Categorías</th><th>Subcategorías</th></tr>
<tr><td rowspan="2">La estafa básica en la Ley de Delitos Informáticos</td><td>Ciberestafa y su relación con el ciberdelito</td></tr>
<tr><td>Delitos informáticos en la legislación nacional</td></tr>
<tr><td rowspan="3">Impunidad por falta de tipicidad</td><td>Rol de los operadores jurídicos</td></tr>
<tr><td>Vacíos de punibilidad o lagunas del derecho</td></tr>
<tr><td></td></tr>
</table>

</td>
<td>

Técnica

La técnica empleada en el estudio es la Entrevista

Instrumentos

El instrumento empleado es la guía de entrevista

</td>
</tr>
</table>

Paradigma, tipo y diseño de investigación	Población y muestra		
El estudio se realiza desde un paradigma interpretativo, el tipo de investigación es Básica. El diseño que se asume corresponde a la teoría fundamentada. **Escenario:** Distrito Judicial de Lima Norte	**Población** Se ha tomado un subgrupo de la población de Lima Norte, constituido por jueces, fiscales, policías y abogados que laboran en el **DJLN.** **Muestra** La muestra de acuerdo al acápite anterior es no probabilística, pues los participantes deben tener conocimientos jurídicos o pragmáticos del tema de estudio.		

Anexo 3: CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO

Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORIA 1: Política criminal de los delitos informáticos	Pertinencia [1]		Relevancia [2]		Claridad[3]		Sugerencias
	SUBCATEGORÍA 1 : La estafa cibernética	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
	¿Cuál es la característica principal de la estafa cibernética como delito contra el patrimonio?							
	¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta.							
	¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión qué se puede hacer al respecto?							
	SUBCATEGORÍA 2: El delito informático							
	¿Según su criterio, cuál es la característica principal del delito informático? Explique su respuesta.							
	¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta.							
	¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?							

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]
Apellidos y nombres del juez validador: Dr: …… **DNI: .....**
Especialidad del validador: ……

Lima,… De …. del 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

_____

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Anexo 4: CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO
Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORÍA 2: Fundamentos socio-jurídicos para la tipificación de la estafa cibernética	**Pertinencia**[1]		**Relevancia**[2]		**Claridad**[3]		**Sugerencias**
N°	**SUBCATEGORÍA 1:** Estafa cibernética	Sí	No	Sí	No	Sí	No	
1	¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?							
2	¿Considera usted que es necesario incluir el tipo de estafa cibernética en la ley de delitos informáticos? Explique su respuesta.							
3	¿Considera usted necesario que se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta							
N°	**SUBCATEGORÍA 2:** Problemas que afrontan los miembros del Ministerio Público en la investigación de la estafa cibernética							
4	¿Considera usted que el Ministerio Público hace uso adecuado de las TIC en las investigaciones? Explique su respuesta							
5	¿Cómo evalúa la utilidad de las TIC en las investigaciones que realiza el Ministerio Público?							
6	¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta							
N°	SUBCATEGORÍA 3: Problemas que afrontan los miembros de la Policía Nacional en la investigación de la estafa cibernética							
7	¿Según su criterio cuáles son las principales dificultades que enfrenta la PNP en la persecución de la estafa cibernética?							
	¿Considera usted que es necesario capacitar en forma permanente a policías para combatir con mayor eficacia el ciberdelito? Explique su respuesta							

¿Qué tipo de mejoras logísticas deben tener policías que se dedican a la persecución de estos delitos?

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr: …… **DNI: .....**

Especialidad del validador: ……

Lima,… De …. del 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

_____

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

ANEXO 5

Matriz de datos cualitativos
Título: Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad en el Perú

GUIA DE ENTREVISTA - JUECES **CATEGORIA 1: Tipo básico de estafa en la Ley de Delitos Informáticos**

PREGUNTAS	**J1** **JUEZ**	**J2**	**J3**	Categorías emergentes	Semejanzas	Diferencias	Interpretación
1. ¿Cuál es la característica principal dela estafa como delito contra el patrimonio?	El engaño o cualquier conducta con fraude para embaucar al agraviado	Que el sujeto activo consiga una disposición patrimonial de la víctima por inducción a error mediante el engaño	La afectación directa al patrimonio ajeno a través del engaño y maniobras fraudulentas	Engaño, patrimonio ajeno	Plantean el engaño como hecho central de este delito	No existen mayores diferencias	Los jueces entrevistados señalan que en este tipo de delito se afecta el bien jurídico del patrimonio el cual debe ser resguardado por el Estado
2. ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta?	Si ha aumentado por que las personas compran por internet	Si, por que las personasrequieren ser atendidas en bancos y empresas y recibir servicios por delivery	Considero que el índice de estafas se ha incrementado durante la pandemia por la gran cantidad de personas estafadas al comprar o contratar servicios y por el aumento de las transacciones virtuales	Internet, transacciones virtuales, estafas - -	Este tipo de delitos utiliza medios informáticos para llevarlos a cabo	No existen mayores diferencias	Los jueces señalan que este tipo de delitos ha aumentado considerablemente, por lo que el Estado debe asumir atención en ello

3. ¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opiniónque se puede hacer al respecto?	La suplantaciónde identidad,pero antes se apoderan de las claves de los agraviados. Se tiene quehacer labor educativa.	El engaño con plataformasfalsas con mensajes falsos y ofrecimientode serviciosfalsos	Lo más comúnes enviar links desde supuestos bancos ofreciendo prestamos, la gente entra a estos links, llena sus datosy el estafador se apodera del dinero de las	Suplantación de identidad - -	Esta modalidad engaña a través de plataformas, webs falsas	No existen mayores diferencias	En este delito, el ciberdelincuente engaña con plataformas falsas con mensajes falsos y ofrecimiento de servicios falsos
			víctimas, asimismo llaman por teléfono ofreciendo incrementar líneas de crédito, tambiénes usual la estafa de vendedores que nunca entregan el producto y luego desaparecen	Líneas de crédito, cuentas de los agraviados	El uso de una plataforma informática con accesos a páginas web		
4. ¿Según su criterio cuál es la característica principal del delito informático? Explique su respuesta.	El uso de programas para acceder indebidamentete a los correos y cuentas de los agraviados	El uso de una plataforma informática con accesosa páginas web de los bancos o de entidades públicas queofrecen servicios simulados	Son delitos nuevos difíciles de demostrar, se llevan a cabo en forma rápiday sin dejar huella, por lo que el Estado debe encontrar mecanismos para proteger a la población	Programas informáticos, entidades públicas	Coinciden en señalar que son delitos sofisticados y cada vez van en aumento	No existen mayores diferencias	Los jueces señalan que se trata de delitos nuevos difíciles de demostrar, se llevan a cabo en forma rápida y sin dejar huella, por lo que el Estado debe encontrar mecanismos para proteger a la población

5. ¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta	Si hay deficiencias pues coexiste el art. 183 A del C.P. referente a la Pornografía de menores y el art. 5 deLDI para obtener material pornográficola pena es diferente pese a que en ambos casos se puede usar tecnología o internet	Si, en el aspecto típico hay deficienciaspara comprender nuevas figuras delictivas como la estafa y en el aspecto punitivo	Si hay deficiencias porque la norma no identifica concretamente el bien jurídico protegido, la tipificación resulta redundante, desproporciona da y carente de idoneidad	Pornografía de menores	Hay deficiencias porque la norma no identifica concretamente el bien jurídico protegido	No existen mayores diferencias	Hay deficiencias porque la norma no identifica concretamente el bien jurídico protegido, la tipificación resulta redundante, desproporciona da y carente de idoneidad
6. ¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?	Para estafarno se requiere estudios avanzados de computaciónpero para hackear una cuenta sí	Si se requiere capacidad especial delautor, conocimientoo de informática para acceder a las cuentas de las PCs	Actualmente no, considero que el internet es una fuente gratuita de información, lo cual permite aprender todo tipo de cosas incluso las ilícitas	Hacker, informática	Si se requiere capacidad especial del autor	Hay quienes señalan que el problema sí es la internet, otros creen que es el uso que se le da	Los entrevistados señalan que el problema no es la internet, sino el uso que se le da. El internet es una fuente gratuita de información, lo cual permite aprender todo tipo de cosas incluso las ilícitas

GUIA DE ENTREVISTA - FISCALES CATEGORIA 1: Tipo básico de estafa en la Ley de Delitos Informáticos

PREGUNTAS	F1 FISCAL	F2	F3	Categorías emergentes	Semejanzas	Diferencias	Interpretación
1. ¿Cuál es la característica principalde la estafa como delito contra el patrimonio?	El engaño, elardid y otras formas fraudulentas para inducir aerror a la víctima y menoscabar su patrimonio	El desprendimiento patrimonial que realiza el sujeto pasivo producto del engaño	La característica principal es el engaño, el ardid para sorprender a la víctima y lograr que se desprende desu patrimonio	EngañoArdid Error	El ardid es el engaño como estrategia principal	No existen diferencias	El uso del engaño es el ardid más usado para sorprender a la víctima y lograr que se desprende de su patrimonio
2. ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta?	Si se ha incrementado por el covid a través de las redes socialeso paginas donde el estafador se gana la confianza de la víctima, haciéndose pasar por alguien de confianza paraconseguir que revele información o haga clic en un enlace peligroso	Sí toda vez que a raíz de la pandemia la población seha visto obligada a utilizar medios tecnológicos para comprar sus productos	Si, se ha incrementado,lo vemos a diario en los medios de comunicación.	Redes sociales, un enlace peligroso	Aumento de este tipo de delito	No existen diferencias	A raíz de la pandemia la población se ha visto obligada a utilizar medios tecnológicos para comprar sus productos

3. ¿Cuál es la modalidad más usualutilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión que se puede hacer al respecto?	Usar herramientas tecnológicas para hacerse de los pagos que se tramitan por internet, estafando y manipulando a sus victimas	Las modalidadesmás usualesson las que se realizan para efectuar transacciones por internet	Los avisos que ponen enlas redes sociales y en el open market, las cuales en la mayoría son falsos	transacciones por internet, open market	Las operaciones por internet son cada vez más frecuentes	No existen diferencias	
4. ¿Según su criterio cuál es la característica principal del delito informático? Explique su respuesta.	Son conductas criminógenasde cuello banco de carácter ocupacional pues muchasse realizan cuando el sujeto se encuentra trabajando, violando la confidencialidad, integridady disponibilidadde los datos y sistemas	El acceso ilícito por que el sujetoactivo accede sin autorización a un sistema informático vulnerando medidas de seguridad	La característica más importante es el uso de tecnología informática para acceder a las cuentas de los usuarios desprendidos	Usuarios desprendidos, confidencialidad, integridad y disponibilidad	Los sistemas informáticos son cada vez más vulnerables	No existen diferencias	La característica más importante es el uso de tecnología informática para acceder a las cuentas de los usuarios desprendidos

	informáticos						

5. ¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta	Hay problemas defalta de seguimiento, control e improvisaciónen la Ley 30096 y deficientes técnicas de redacción legislativa, lo que facilita lafalta de protección de losdatos personales	Sí hay deficiencias,las penas que se imponen son mínimas	Si hay deficiencias no se ha regulado la propiedad intelectual y el espionaje industrial en esa ley especial	espionaje industrial, protección de los datos personales	Existen deficiencias pues no se ha regulado la propiedad intelectual y el espionaje industrial en esa ley especial	No existen diferencias	Existen problemas de falta de seguimiento, control e improvisación en la Ley 30096 y deficientes técnicas de redacción legislativa, lo que facilita la falta de protección de los datos personales
6. ¿Considera usted que se requieren conocimientos avanzadosde informática para causar estafas a través del internet?	Claro que sí, los expertos señalan que los cibernautas tienen conocimientos avanzados deredes y usan canales digitales que afectan a los sistemas y datos informáticos	Si por que elperfil del ciber- delincuente requiere tener conocimientos importantes de informática para ingresar sin autorización a un sistemade datos	En algunos casos se requiere pero para engañara través de las redes no se requiere.	Cibernautas, redes y canales digitales	En ciertos casos se requiere pero para engañar a través de las redes no se requiere	No existen diferencias	Los entrevistados señalan que los cibernautas tienen conocimientos avanzados de redes y usan canales digitales que afectan a los sistemas y datos informáticos

GUIA DE ENTREVISTA - POLICIAS CATEGORIA 1: Tipo básico de estafa en la Ley de Delitos Informáticos

PREGUNTAS	P1 Policía	P2	P3	CONCEPTOS IDENTIFICADOS	CATEGORIAS O CONCEPTOS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACION
1. ¿Cuál es la característica principal de la estafa como delito contra el patrimonio?	La principal característica es el engaño que utilizan los delincuentes para sorprender a los incautos.	De acuerdo a las estadísticas el engaño y la mentira que utilizan los delincuentes	Siempre es el engaño, es lo que dicen todos los agraviados que vienen a denunciar.	engaño- - -	Estadística - - -	Conducta fraudulenta del agente- - -	El medio empleado- - -	Todos los entrevistados coinciden que el elemento central es el engaño- - -
2. ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta?	Si han aumentado estos delitos porque la gente bajo la guardia por los altos índices de la pandemia, debido a que tienen que comprar sus cosas por internet	La pandemia ha generado nuevas oportunidades para la delincuencia, los engaños se han multiplicado por el distanciamiento social	Pienso que si se ha incrementado porque la gente no puede salir libremente de su casa por la pandemia y por los impedimentos de transito que ha decretado el gobierno	índice de crecimiento - - -	Distanciamiento social - - -	Crecimiento sostenido - - -	No hay diferencias - - -	Los participantes opinan que las estafas se han incrementado por la pandemia - -
3. ¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión que se puede hacer al respecto?	Lo más usual es que ponen avisos y ofertas falsas en las redes para que le hagan depósitos o para que hagan clic en links fraudulentos y una vez conseguido eso le vacían sus cuentas	Hacen ofertas falsas a través del internet, ofrecen mercadería a bajo costo precio y también ofrecen préstamos. Una vez que hacen los depósitos se hacen humo.	Lo más usual son las estafas por internet la venta de medicamentos para el covid cuando estaban escasos y los avisos falsos para cobrar el bono, previa entrega de datos.	Ofertas falsas - - -	Redes sociales - - -	Uso del internet - - -	No hay diferencias - - -	Los participantes señalaron que lo mas usual son las ofertas falsas - - -

4. ¿Según su criterio cuál es la característica principal del delito informático? Explique su respuesta.	Lo principal es el uso de la tecnología que hace el hacker para apoderarse de datos del usuario básicamente sus cuentas o claves para poder hacer transferencias no autorizadas a favor de sus cómplices	El uso de programas maliciosos para infiltrarse en otras computadoras y robar información o claves de cuentas bancarias	El envió de enlaces fraudulentos que hacen los hackers usando las redes y también el uso de programas maliciosos.	Tecnología - - -	Programas maliciosos - - -	Uso de la tecnología - - -	No hay diferencias - - -	Los entrevistados coinciden en el uso de la tecnología - - -
5. ¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta	Me parece que si porque mucho demoran las autorizaciones judiciales cuando queremos identificar al delincuente, la ley debe dar facilidades a la fiscalía obligando a las empresas a entregar la información solicitada de inmediato	Es muy difícil dar con el paradero de los delincuentes la ley pone muchas trabas para acceder al secreto bancario y para levantar el secreto de las comunicaciones	Lo que yo aprecio es que existen muchas dificultades para identificar a los delincuentes, para todo se le tiene que pedir permiso al juez y además los fiscales demoran mucho para adoptar medidas drásticas.	ninguno - - -	Autorización judicial Dificultad para identificar - - -	ninguna - - -	ninguna - - -	Los entrevistados coinciden en que hay deficiencias en la ley de delitos informáticos - - -
6. ¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?	No creo que se requiera conocimientos avanzados para engañar a los incautos basta poner avisos en las redes y mucho caen tentados por los bajos precios de los productos que ofrecen	Solo se requieren conocimientos básicos para engañar a través de las redes sociales	Por la experiencia que tengo en las investigaciones no se requiere ser experto en informática para engañar con ofertas falsas, aunque si se requiere más conocimiento para hackear cuentas de manera remota.	ninguno - - -	Experto en informática Hacker - - -	Conocimientos básicos - - -	Ninguna - - -	Los entrevistados coinciden en que no se requiere conocimientos avanzados de informática - - -

GUIA DE ENTREVISTA - ABOGADOS <u>CATEGORIA 1</u>: Tipo básico de estafa en la Ley de Delitos Informáticos

PREGUNTAS	A1 Abogado	A2	A3	CONCEPTOS IDENTIFICADOS	CATEGORIAS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACION
1. ¿Cuál es la característica principal de la estafa como delito contra el patrimonio?	Me parece que es el engaño en todas sus formas y por todos los medios.	La característica es el engaño y el fraude en todas sus variantes.	Es evidente que el engaño y toda conducta fraudulenta.	- engaño- -	- Conducta fraudulenta- -	- Toda conducta fraudulenta - -	- ninguna- -	Los participantes coinciden en el engaño - -
2. ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta?	Si ha crecido por la pandemia debido a que la gente tiene que usar las redes para comprar muchas cosas, antes del covid-19 las estafas eran presenciales pero ahora el contacto físico no es necesario.	Si considero que debido a la pandemia las estafas por las redes se han multiplicado de manera alarmante.	Es natural que se incrementen los fraudes a través de la red, ya que tanto los delincuentes como la ciudadanía en general, estuvieron en aislamiento obligatorio.	pandemia- - -	Ninguna - - -	Uso de las redes para comprar bienes- - -	ninguna- - -	Los entrevistados que si se ha incrementado el índice - - -
3. ¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión que se puede hacer al respecto?	Las modalidades mas frecuentes son las ofertas fraudulentas a través de las redes sociales y los fake news que generan dudas en las personas desprevenidas.	Lo más usual es el envío de links fraudulentos a través de páginas web falsas para obtener datos de las víctimas.	La proliferación de ofertas engañosas para adquirir bienes a bajo costo y para cobrar los bonos que autorizo el gobierno	La estafa - - -	Link fraudulento- - -	Proliferación de ofertas- - -	Ninguna - - -	Los participantes coinciden que lo más usual es la oferta engañosa - - -
4. ¿Según su criterio cuál es la característica principal del delito informático? Explique su respuesta.	El uso de tecnologías y programas piratas que hackear cuentas para acceder indebidamente a cuentas de terceros. Otra característica es usar software para apoderarse de información valiosa de las empresas.	Lo principal es el empleo de software fraudulento para ingresar a las cuentas de los usuarios, siempre a través de servidores difíciles de rastrear.	Lo que caracteriza el delito informático es el uso de programas creados exprofeso para acceder y extraer información, principalmente claves, para acceder a cuentas y tecnología de punta para piratearlo.	Tecnología - - -	Software fraudulento- - -	Uso de la tecnología - - -	- ninguna- -	El uso de la tecnología - - -
5. ¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta	Si me parece que hay deficiencias pues no se ha registrado como debe de ser el acceso a claves secretas de	Se debe unificar el tratamiento de delitos contra el patrimonio	Considero que hay deficiencias en el tratamiento de la propiedad intelectual que se piratea en forma	ninguno- - -	Tratamiento de la propiedad intelectual- -	Si hay deficiencias- - -	- Ninguna - -	Todos los participantes coinciden en que si hay deficiencias-

	tarjetas de crédito cuando hay empleados de instituciones financieras que actúan como cómplices.	cuando el medio empleado es el internet o el software especializado.	inescrupulosa y la ley no la contempla		-			- -
6. ¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?	Para estafar a través de las redes no se requiere de conocimientos avanzados de telemática, pero si para acceder a una base de datos de las empresas.	Solo se requiere de medianos conocimientos para embaucar, salvo cuando se trate de hackear páginas de los bancos.	Para estafar usando el engaño en las redes no se requiere ser un experto basta colocar avisos que sirven como señuelo.	ninguno- - -	Hackear - Conocimientos básicos- -	Medianos conocimientos- - -	Ninguna - - -	Los participantes coinciden en que no se requieren conocimientos avanzados en informática- - -

MATRIZ DE DATOS CUALITATIVOS

GUIA DE ENTREVISTA - JUECES CATEGORIA 2: Impunidad por falta de la tipicidad propuesta

PREGUNTAS	J1 JUEZ	J2	J3	CONCEPTOS IDENTIFICADOS	CATEGORIAS O CONCEPTOS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACION
7. ¿Considera usted que existen vacíos en la ley de delitos informáticos para sancionar ciertas conductas en el espacio virtual? ¿Podría preciar cuáles?	El principal vacío es el escaso castigo para los que se aprovechan de menores para obtener material pornográfico	Estafas con el cuento de pagos de pensiones, con el cuento del proveedor de servicios, hackeo de cuentas de usuarios, mensaje para obtener premios	Si existen vacíos para sancionar ciertas conductas delictivas cometidas en espacios virtuales como la clonación de tarjetas de crédito, debito o el phishing de datos	Phishing - - -	Clonación - - -	La existencia de vacíos en la ley- - -	Ninguna - - -	Los participantes coinciden en que si existen vacíos en la ley - - -
8. ¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta	Si, me parece que es necesario para dar respuesta adecuada a los delincuentes que usan el internet	Sí, mejorando su redacción típica y los medios comisivos empleados	Si, lo considero importante para lograr un marco normativo que se ajuste a la realidad	Ninguno - - -	Medios comisivos empleados- - -	Nuevo marco normativo- - -	Ninguna - - -	Los participantes coinciden en que es necesario incluir la estafa básica en la ley- - -

9. ¿Considera usted necesario ue se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	Si, se debe incrementar como en el caso del hurto y robo que también son delitos contra el patrimonio	Si, puede ser tanto en la autoría como en banda criminal	Sí considero importante que se incremente la pena en la estafa informática cuando hay pluralidad de agente por que nos encontramos ante una organización criminal	Ninguna - - -	Pluralidad de agentes- - -	Incremento de pena - - -	Ninguna - - -	Los entrevistados coinciden en que es necesario incrementar la pena cuando hay pluralidad de agentes- - -
10. ¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio?	Si, se ha incrementado por que la gente debe hacer compras sin salir de su casa debido a la pandemia	Si, tanto por la necesidad de no contagiarse, como por el hecho de que las transacciones electrónicas se han incrementado	Considero que sí y en gran porcentaje por que la mayor parte de la población comenzó a comprar de manera virtual desde alimentos básicos hasta terrenos o palizas de seguro	Transacción electrónica - - -	Compras virtuales - - -	Crecimiento del comercio electrónico - - -	Ninguna - - -	Todos coinciden que si se ha incrementado el comercio electrónico - - -
11. ¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	Las TIC son necesarias y cuando se usan bien permiten el desarrollo del comercio electrónico los pagos desde casa y el delivery	Las TICs han incrementado su potencial en todas las áreas del ámbito económico, por la necesidad de hacer transacciones	Los avances tecnológicos permiten sostener plataformas de compra capaces de concretar múltiples ventas al mismo tiempo. Asimismo, de no tener canales de comunicación eficaces las transacciones en los bancos serían lentas	Ninguna - - -	Avance tecnológico - - -	Influencia de las Tecnologías de la información y comunicación - - -	Ninguna - - -	Todos coinciden que las TIC han influido en el desarrollo del comercio electrónico - - -

12.¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.	Si, por que las personas tienen que adquirir sus productos desde su casa usando el internet y como no saben usarlo bien caen en	Sí, ha cesado la estafa presencial y clásica por estas nuevas modalidades que se ve en los medios de	Considero que sí, al usar más el internet se han encontrado mayores mecanismos para la comisión de delitos como estafas	Ninguna - - -	Ninguna - - -	Uso del internet - - -	Ninguna - - -	Los entrevistados coinciden que la pandemia ha generalizado el uso del internet para cometer fraudes- - -
	lasa redes de los estafadores	comunicació nn	cibernéticas					
13. ¿Según su criterio cuales son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático?	Identificar a los sujetos activos pues estos nunca usan su verdadero nombre, para identificarlos hay que pedir el levantamient o del secreto de las comunicacio nes	Que solo cuenta con una unidad especializad a y se requieren mas unidades de atención, así como capacitación e incremento de fiscales	La principal desventaja es la forma tan rápida en que los delitos cibernéticos van evolucionando y cada vez es más difícil descubrir sus huellas	Ninguna - - -	Levantamiento del secreto de las comunicaciones - - -	Dificultad para identificar al agente- - -	Ninguna - - -	Se dividen las opiniones, un juez dice que la principal dificultad es la identificación, otro dice es la evolución del delito informático- - -
14. ¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito?	Por supuesto la capacitación debe ser permanente por que el refinamiento delictivo también crece	Sí, es básico para detectar, prevenir, perseguir y lograr su sanción en sede judicial	Considero que la capacitación es fundamental para enfrentar este tipo de delitos. Asimismo, considero indispensables que policías y fiscales cuenten con herramientas necesarias para combatir estos delitos	- - -	- - -	- - -	- - -	- - -

15. ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	Deben contar con equipos modernos y si es posible con asesores técnicos.	Se le debe proporcionar sistemas de internet capaces de cubrir las necesidades de la investigación y proveerlos de mejores	Indiscutiblemente, se necesitan mejoras en la infraestructura cibernética, software mas avanzados y actualizados	Equipos modernos - - -	Infraestructura cibernética - - -	-mejor infraestructura - -	Ninguna- - -	Todos coinciden en las mejoras logísticas - - -
		herramientas tecnológicas						

MATRIZ DE DATOS CUALITATIVOS

GUIA DE ENTREVISTA -FISCALES CATEGORIA 2: Impunidad por falta de la tipicidad propuesta

PREGUNTAS	F1 FISCAL	F2	F3	CONCEPTOS IDENTIFICADOS	CATEGORIAS O CONCEPTOS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACION
7. ¿Considera usted que existen vacíos en la ley de delitos informáticos para sancionar ciertas conductas en el espacio virtual? ¿Precise cuáles?	Si, tales como el fraude, la penetración en redes informáticas, el envío de correos basura, la pesca de datos a través del phishing y la piratería digital	Si la falta de tipificación penal de ciertas conductas como la estafa	No se sancionan las estafas simples cometidos en el espacio virtual, tampoco los delitos contra la propiedad intelectual básicamente piratería de software	Correos basura- - -	Espacio virtual- - -	Falta de tipificación - - -	Ninguna - - -	Los entrevistados coinciden en que no se sanciona la estafa simple- - -
8. ¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta	Si es necesario incluir en la LDI el delito de estafa por que tiene las características del engaño y el ardid, lo que va contra el patrimonio de las victimas	Si porque es una modalidad de cometer un acto ilícito mediante engaño y en perjuicio de terceros	Si sería necesario que se incluya la modalidad de estafa básica, con esa medida se combatiría la impunidad, para favorecer a los agraviados	Ninguno - - -	Ninguna - - -	Necesidad de tipificar - - -	Ninguna - - -	Los entrevistados coindicen en que se debe tipificar la estafa básica en la ley especial - - -

9. ¿Considera usted necesario ue se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	Si es necesario incrementar la pena debido a su semejanza con una organización criminal según sus roles, donde uno manipula el sistema, otro maneja las redes y la transferencia de datos que se consiguen en el mercado negro	Si por que realizar maniobras para ingresar sin autorización del titular es cuestionable más si participan varias personas	Si se debería incrementar la pena para disuadir a los delincuentes, esto es parte de la prevención general negativa propia de la política criminal que debe implementar el estado.	Ninguna - - -	Organización criminal - - -	Incremento de pena - - -	Ninguna - - -	Los entrevistados coinciden en que si se debe incrementar la pena en estos casos - - -
10. ¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio?	Se ha incrementado debido a las restricciones del gobierno por la emergencia sanitaria. Los usuarios por necesidades personales o empresariales usan este medio para hacer compras	Sí por que las empresas han tenido que realizar transacciones por internet para continuar con sus actividades	Si se ha incrementado porque toda la ciudadanía ha tenido que adquirir lo que consume o los servicios que necesita usando el internet	Emergencia sanitaria - - -	ninguna- - -	Desarrollo del comercio electrónico - - -	- Ninguna - -	Todos los entrevistados señalan que el comercio electrónico si se ha incrementado- - -
11. ¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	Es importante para el desarrollo del comercio, pero también lo es para el sistema financiero y empresarial, lo cual es usual en los países desarrollados	Permiten el acceso de información a fin de seleccionar y tomar una adecuada decisión	Esas tecnologias son muy necesarias de eso no cabe duda, de lo contratrio las empresas colapsarian, por las restricciones que ha impuesto el gobierno	Ninguno - - -	Acceso a la información - - -	Influencia directa - - -	Ninguna - - -	Todos los entrevistados coinciden en que el papel de las TIC es importante para el comercio electrónico - -

12.¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.	No estoy seguro, por que hay otros factores como la crisis económica, el sistema de salud , la falta de hospitales y suministros para la salud y las deficiencias para contener la pandemia	Si debido al mayor uso de la tecnología	Si el uso de internet se ha generalizado en esta era del covid-19, muchos se han visto obligados a aprender sobre la marcha para sobrevivir	Ninguna - - -	Ninguna - - -	No hay semejanzas - - -	Si hay diferencia de opiniones - - -	Uno de los entrevistados opino que la crisis económica ha sido el principal factor, los otros lo atribuyen a la pandemia- - -
13. ¿Según su criterio cuales son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático?	La principal dificultad es la falta de capacitación y la falta de especialización por que también actúan delincuentes informáticos extranjeros	La falta de capacitación permanente y la no entrega por parte del Estado de equipo tecnológico avanzado	Las principales dificultades son la falta de capacitación y la falta de equipos adecuados para identificar a los delincuentes informáticos, eso pasa por un problema presupuestal	Ninguna - - -	Falta de especialización - - -	Falta de capacitación - - -	Ninguna - - -	Los entrevistados coinciden en la falta de capacitación y especialización -

14. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el ciberdelito?	Si es necesario capacitarlos por que los delincuentes informáticos son cibernautas que conocen todos los medios tecnológicos y las modalidades para romper las barreras de seguridad	Si	Es lógico, tanto policías como fiscales deben recibir capacitación permanente mente, incluso de ponentes extranjeros a través del espacio virtual o por medio de convenios con instituciones especializadas	Ninguna - - -	Ninguna - - -	Si hay semejanzas - - -	No hay diferencias- - -	Los entrevistados coinciden en que es necesaria la capacitación permanente para policías y fiscales - - -
15. ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	Equipos y sistemas de última generación con todas las herramientas de búsqueda que usan los cibernautas con fines delictivos	Realizar adecuadas coordinaciones con instituciones nacionales e internacionales	El estado debe suministrar equipos modernos y software moderno y original a la fiscalía y a la policía para que persigan con eficacia a los ciber delincuentes	Ninguna - - -	Ninguna - -	Si hay semejanzas - - -	No hay diferencias- - -	Todos los entrevistados coinciden en que tanto policías como fiscales deben tener mejoras logísticas - - -

MATRIZ DE DATOS CUALITATIVOS

GUIA DE ENTREVISTA -POLICÍAS <u>CATEGORIA 2</u>: Impunidad por falta de la tipicidad propuesta

PREGUNTAS	P1 Policía	P2	P3	CONCEPTOS IDENTIFICADOS	CATEGORIAS O CONCEPTOS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACION
7. ¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?	Si hay vacíos por que no sancionan como debe ser a los estafadores de las redes, tampoco sancionan a los que piratean los programas informáticos.	Uno de los vacíos es la falta de sanción para la estafa de los que usan las redes, de eso me he percatado como abogado.	Lo que yo veo es que existe impunidad porque es difícil identificar y ubicar a los delincuentes, porque maniobran lejos de la víctima y como no hay flagrancia para capturarlo hay que pedir autorización al juez.	Ninguno - - -	Ninguna - - -	- Relativa - -	Ninguna - - -	Los entrevistados dividen sus opiniones en lo referente a las consecuencias de los vacíos legales - - -
8. ¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta	Si deben incluir toda clase de estafas que se comenten en las redes sociales porque hay muchas denuncias de ese tipo	Si me parece que sería necesario para darle más herramientas al fiscal y a la policía y poder sanción en forma más severa a estos delincuentes evitando la impunidad	Si me parece que sería útil, porque mucho han proliferado las estafas a través del internet y con la ley de delitos informáticos se podría incautar con más facilidad los CPU que usan los delincuentes.	Ninguno - - -	Herramientas legales - - -	Relativa - - -	Ninguna - - -	Los entrevistados coinciden en que se debe incluir la estafa básica, pero difieren en las consecuencias legales - - -

9. ¿Considera usted necesario que seincremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	Por su puesto, para sancionar a las bandas de estos delincuentes porque nunca actúan solos siempre utilizan a otros para recibir los depósitos de los agraviados	Las penas no deberían aumentarse, pero se debe eliminar los beneficios penitenciarios para que los delincuentes no salgan sin cumplir su pena	Si creo que debe aumentar la pena en estos casos porque el delincuente nunca actúa solo.	Ninguno - - -	Ninguna - - -	Ninguna - - -	Relativa - - -	La mayoría de entrevistados coincide en que se debe aumentar la pena, pero uno de ellos dice que se debe eliminar los beneficios penitenciarios- - -
10. ¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio?	Las ventas a través del internet han crecido por el covid-19, la gente vulnerable tiene que hacer sus pedidos de lo que necesitan de forma virtual	Si se ha incrementado porque las empresas hacen campañas publicitarias por internet y además porque no se puede salir mucho a cualquier hora lo la pandemia	Si ha aumentado el comercio a través de las redes porque la gente al principio de la pandemia no podía salir de su casa.	- Ninguno - -	- Ninguna - -	- Hay coincidencia - -	- Ninguna - -	Todos los entrevistados coinciden en que el comercio electrónico se ha incrementado por el aislamiento social obligatorio- - -
11. ¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	Las tecnologías son necesarias, el problema es el mal uso que hacen de ellas los delincuentes para engañar a sus victimas	No se soy técnico en informática, pero la tecnología permite mejorar los servicios que ofrecen las empresas a traves del comercio electrónico	La tecnología es importante y necesaria para cualquier negocio y en el caso del comercio electrónico mucho más.	Ninguna - - -	Ninguna- - -	Hay coincidencia- - -	Ninguna - - -	Los entrevistados coinciden que el papel de las TIC ha sido positivo para el desarrollo del comercio electrónico - - -

12.¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.	Si, porque la gente se ha visto obligada a comprar sus cosas por las redes y de eso se han aprovechado los delincuentes para sorprender a los incautos usando muchas artimañas	El covid 19 ha hecho que casi todo el mundo utilice el internet incluso los escolares, por lo tanto los delincuentes también están acechando a sus víctimas gracias al internet	Si porque hasta la gente de tercera edad tienen que aprender a ingresar al internet	- -ninguno -	- Ninguna - -	- Hay coincidencia - -	- Ninguna - -	Todos coinciden en que la pandemia ha generalizado el uso de internet para defraudar- - -
13. ¿Según su criterio cuales son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático?	La principal dificultad, es identificar al delincuente porque no es un delito cometido en flagrancia, mejor dicho nunca se sorprende al delincuente en flagrancia porque hacen sus cosas a través de una computadora	la principal dificultad es identificar y ubicar a estos delincuentes escurridizos y la otra dificultad es sostener las dificultades legales para continuar con éxito la investigación	Falta capacitación permanente no solo para las unidades especializadas sino también en provincias donde no hay estas unidades. Lo mismo debe ocurrir en el ministerio público.	Ninguna - - -	Ninguna - - -	- Hay coincidencia - -	- Relativa - -	La mayoría coinciden en la falta de capacitación, uno de ellos opino que la principal dificultad es la no identificación del agente - - -
14. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el ciberdelito?	Si me parece que es muy necesario, lo que ocurre que el ministerio del interior no siempre tiene el presupuesto adecuado, además se tiene que dar permiso al personal para que reciba capacitación. En el caso de la fiscalía no sé cómo es la capacitación	Si creo que tanto la policía como el ministerio Publico deben ser capacitados con seminarios y cursos periódicos a cargo de especialistas.	Si, por lo menos en forma trimestral con seminarios virtuales debido a la pandemia.	- - -	- - -	- - -	- - -	- - -

15. ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	Debemos contar con modernos equipos y con programas adecuados para hacer el seguimiento de la delincuencia en la red. La fiscalía también debe contar con estos equipos para sus investigaciones	el ministerio del interior y el estado deben dotar de mejores equipos logísticos a ambas instituciones.	Deben contar con mejores equipos de cómputo y mejores locales. Y con peritos en forma descentralizada	Ninguna - - -	Ninguno - - -	Hay coincidencia- - -	Ninguna - - -	Todos los entrevistados coinciden en que debe haber mejoras logísticas - - -

MATRIZ DE DATOS CUALITATIVOS

GUIA DE ENTREVISTA -ABOGADOS **CATEGORIA 2: Impunidad por falta de la tipicidad propuesta**

PREGUNTAS	A1 Abogado	A2	A3	CONCEPTOS IDENTIFICADOS	CATEGORÍAS O CONCEPTOS EMERGENTES	SEMEJANZAS	DIFERENCIAS	INTERPRETACIÓN
7. ¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?	Si me parece que existen vacíos pero no se ha unificado el hurto de claves de tarjetas de crédito y la estafa informática para obtener estas claves.	En esa ley se debe unificar todos los delitos, cuando se privilegia el uso del internet, a mi criterio no deberían estar dispersos.	Si hay vacíos uno de ellos es la falta de protección a la propiedad intelectual en esa ley.	- Ninguno - -	- Ninguna - -	- Relativa - -	- Relativa - -	- Los entrevistados difieren en la falta de tipificación y en el objeto de protección de la ley - -
8. ¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta	No se debe incluir porque es un simple engaño a través de las redes, pero no hay empleo de habilidades informáticas como suelen usar las hackers, por lo tanto esos engaños deben quedar como estafa simple	Si se debe incluir la estafa en la ley especial, cuando se privilegie el uso de internet o cualquier tecnología informática.	Pienso que si es necesario ya que la estafa a través de las redes se ha incrementado debido al covid 19, pero se le debe diferenciar de la estafa común.	- Redes sociales - -	Ninguna - - -	- No hay semejanzas- -	Si hay diferencias - - -	Dos entrevistados coinciden en que se debe tipificar la – estafa básica en la ley especial, pero uno de ellos no está de acuerdo. - -
9. ¿Considera usted necesario ue se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	No se deben incrementar las penas porque estas ya son muy altas	A mi criterio no se deben incrementar las penas, pues eso no soluciona el problema. La prioridad es la prevención.	No me parece que la solución este en aumentar las penas, eso no disuade a los delincuentes se debería hacer campañas para alertar a la población evitando que sean presa fácil de los delincuentes.	Ninguna - - -	Ninguna - - -	Relativa - - -	Ninguna - - -	Todos los entrevistados coinciden en que no se debe incrementar la pena ante el concurso de agentes, solo difieren en la causa. - - -

10. ¿Considera usted que el comercio electrónico se incrementó a raíz del Aislamiento social obligatorio?	El comercio a través de las redes si ha crecido pero por necesidad, no porque la mayoría de la gente lo haya buscado. Muchas personas tienen miedo al contagio por eso compran por internet.	El comercio electrónico al igual que todas las actividades que antes eran presenciales se han incrementado por la pandemia, incluso los niños debido al aislamiento social tienen que recibir sus clases por internet	Si se ha incrementado porque debido a la pandemia las compras tiene que hacerse usando el internet.	- - Ninguna -	- Ninguna - -	- Hay coincidencia - -	- Relativa - -	Todos los entrevistados coinciden en que el comercio electrónico ha crecido, solo difieren en la causa de este fenómeno. - - -
11. ¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	Las tecnologías permiten que se dinamicen las ventas y las empresas aprovechan esas tecnologías para ofrecer sus productos al público reduciendo sus costos.	La tecnología es vital para el desarrollo de cualquier actividad económica, más aun tratándose de la informática aplicada a los negocios.	La tecnología va de la mano con el crecimiento de los negocios y el comercio electrónico, este usa muchas herramientas novedosas para captar a más clientes	Ninguno - - -	Ninguna - - -	Relativa - - -	Relativa - - -	Los entrevistados coinciden en que la tecnología influye en el crecimiento del comercio electrónico, empero difieren en forma relativa en las causas- - -
12.¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.	En cierta forma sí, porque los delincuentes aprovechan cualquier oportunidad para hacer su fechorías ya que no pueden tener contacto directo con sus víctimas por el covid y el temor al contagio	Los delincuentes al ver que no pueden embaucar a sus víctimas de manera presencial han tenido que usar las redes para perpetrar sus fraudes.	Es natural que se haya generalizado el uso de internet, incluso en las escuelas, por lo tanto los delincuentes cada vez usan más el internet para cometer sus delitos.	- Ninguno - -	- Ninguna - -	- Relativa - -	- Relativa - -	Los entrevistados coinciden en que la pandemia ha generalizado el uso del Internet y los fraudes, solo difieren en los motivos de los delincuentes - - -

13. ¿Según su criterio cuales son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático?	La falta de preparación tanto de policías como de fiscales, demoran mucho casi y casi nunca se encuentran al culpable.	No hay personal capacitado suficiente en los distritos y conos, se debería descentralizar y crear unidades especializadas en todos los conos porque la población aumenta.	La dificultad para investigar en el plazo que fija la ley, la falta preparación tanto a la policía como a los fiscales para reducir la impunidad	- - Ninguno -	- - Ninguna -	- - Relativa -	- - Relativa -	Los entrevistados coinciden en la falta de preparación de policías y fiscales, uno de ellos señala la falta de descentralización de las unidades especializadas- - -
14. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el ciberdelito?	Si me parece que es necesario para que hagan rápido sus investigaciones y no tengan pretextos para tanta demora.	Si considero que es necesario, pero también es necesario que ese personal rote, para que se capacite al mayor número de efectivos policiales y fiscales.	Si es obvio que deben recibir capacitación de técnicas en informática para estar al día con las nuevas modalidades que usan los hackers	- Ninguna - -	- Ninguna - -	- Hay coincidencia - -	- Ninguna - -	Todos los entrevistados señalan que es necesaria la capacitación permanente - - -
15. ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se Dedican a la persecución de estosdelitos?	Deben tener buenos equipos y reemplazar esas máquinas viejas que se ven en las comisarías y en algunas fiscalías.	Deben tener mejores equipos y tecnología de última generación para hacer el seguimiento a las organizaciones criminales que se dedican a estos delitos.	El estado debe dotarlos de equipos de cómputo modernos, especialmente a la policía que utiliza maquinas obsoletas.	Ninguna - - -	Ninguna - - -	Hay coincidencia - - -	Ninguna - - -	Todos los entrevistados señalan que tanto policías como fiscales deben contar con mejores equipos proporcionados por el Estado - - -

ANEXO 6

CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO
Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORIA 1: Tipo básico de estafa en la ley de delitos informáticos	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	SUBCATEGORÍA 1 : La estafa básica	Sí	No	Sí	No	Sí	No	
1	¿Cuál es la característica principal de la estafa como delito contra el patrimonio?	X		X		X		
2	¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta.	X		X		X		
3	¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión qué se puede hacer al respecto?	X		X		X		
N°	SUBCATEGORÍA 2:El delito informático	X		X		X		
4	¿Según su criterio, cuál es la característica principal del delito informático? Explique su respuesta.	X		X		X		
5	¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
6	¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?	X		X		X		

Observaciones (precisar si hay suficiencia): Si hay suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Orrasco Campos Marco Antonio DNI: 09964761

Especialidad del validador: Dr. en Educación

Lima, 06 De agosto de 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO
Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORÍA 2: Impunidad por falta de la tipicidad propuesta	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	SUBCATEGORÍA 1: Vacíos de punibilidad en la ley	Sí	No	Sí	No	Sí	No	
1	¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?	X		X		X		
2	¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
3	¿Considera usted necesario que se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	X		X		X		
N°	SUBCATEGORÍA 2: Desarrollo del comercio electrónico por la pandemia	X		X		X		
4	¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio?	X		X		X		
5	¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	X		X		X		
6	¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta	X		X		X		
N°	SUBCATEGORÍA 3: Rol de los operadores de justicia	X		X		X		

7	¿Según su criterio cuáles son las principales dificultades que enfrenta la PNP y el Ministerio Público en la persecución del delito informático?	X		X		X		
8	¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito?	X		X		X		
9	¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	X		X		X		

Observaciones (precisar si hay suficiencia): SI

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr: MARCO ANTONIO CALDERON CAMPOS **DNI:** 09964961

Especialidad del validador: Doctor Abogado Magister Derecho Constitucional

Lima, 27 De julio de 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO

Guía de entrevistas en profundidad a jueces

	CATEGORIA 1: Tipo básico de estafa en la ley de delitos informáticos	**Pertinencia[1]**		**Relevancia[2]**		**Claridad[3]**		**Sugerencias**
N°	**SUBCATEGORÍA 1 :** La estafa básica	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	¿Cuál es la característica principal de la estafa como delito contra el patrimonio?	X		X		X		
2	¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia por covid 19? Explique su respuesta.	X		X		X		
3	¿Cuáles son las modalidades más usuales utilizadas por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión que se puede hacer al respecto?	X		X		X		
N°	**SUBCATEGORÍA 2:** El delito informático							
4	¿Según su criterio, cuál es la característica principal del delito informático? Explique su respuesta.	X		X		X		
5	¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
6	¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través de internet?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA.

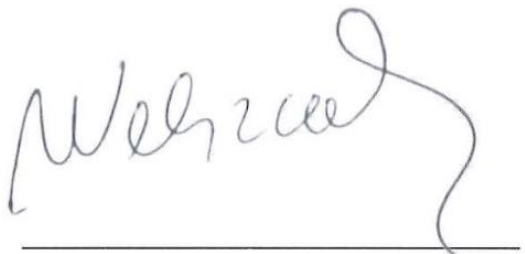
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Nilton César VELAZCO LEVANO **DNI:** 09927657

Especialidad del validador: Doctor en Derecho y Ciencias Políticas CAL N°30620

Lima, 25 de julio del 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.



Firma del Experto Informante

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Guía de entrevistas en profundidad a jueces, fiscales, abogados y policías

	CATEGORÍA 2: Impunidad por falta de la tipicidad propuesta	**Pertinencia**[1]		**Relevancia**[2]		**Claridad**[3]		**Sugerencias**
N°	**SUBCATEGORÍA 1:** Vacíos de punibilidad en la ley	Sí	No	Sí	No	Sí	No	
1	¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?	X		X		X		
2	¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
3	¿Considera usted necesario que se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta.	X		X		X		
N°	**SUBCATEGORÍA 2:** Desarrollo del comercio electrónico a raíz de la pandemia							
4	¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio? Explique su respuesta.	X		X		X		
5	¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	X		X		X		
6	¿Cree usted que la pandemia por el covid 19 ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta.	X		X		X		
N°	**SUBCATEGORÍA 3:** Rol de los operadores de justicia							
7	¿Según su criterio cuáles son las principales dificultades que enfrenta la Policía Nacional y el Ministerio Público en la persecución de los delitos informáticos?	X		X		X		

8	¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito?	X		X		X		
9	¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA**.**

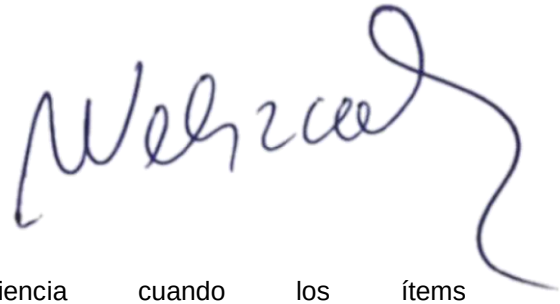
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr**.** Nilton César VELAZCO LEVANO **DNI:** 09927657

Especialidad del validador: Doctor en Derecho y Ciencias Políticas CAL N°30620

Lima, 25 de julio del 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.



_____

Firma del Experto Informante

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO
Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORIA 1: Tipo básico de estafa en la ley de delitos informáticos	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**SUBCATEGORÍA 1 :** La estafa básica	Sí	No	Sí	No	Sí	No	
1	¿Cuál es la característica principal de la estafa como delito contra el patrimonio?	X		X		X		
2	¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia? Explique su respuesta.	X		X		X		
3	¿Cuál es la modalidad más usual utilizada por los agentes delictivos para embaucar a sus víctimas según los medios de comunicación y en su opinión qué se puede hacer al respecto?	X		X		X		
N°	**SUBCATEGORÍA 2:**El delito informático							
4	¿Según su criterio, cuál es la característica principal del delito informático? Explique su respuesta.	X		X		X		
5	¿Considera usted que existen deficiencias en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
6	¿Considera usted que se requieren conocimientos avanzados de informática para causar estafas a través del internet?	X		X		X		

Observaciones (precisar si hay suficiencia): Si

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr: Miguel Angel Gonzales Barbadillo **DNI:** 16654997

Especialidad del validador: Doctor en Derecho y Ciencia Política y Magister en Derecho Constitucional y DD.HH.

Lima, 16 De Agosto de 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

CERTIFICADO DE VALIDACIÓN DE CONTENIDO DE INSTRUMENTO
Guía de entrevista a participantes: Jueces, Fiscales, Policías

	CATEGORÍA 2: Impunidad por falta de la tipicidad propuesta	**Pertinencia**[1]		**Relevancia**[2]		**Claridad**[3]		**Sugerencias**
N°	**SUBCATEGORÍA 1:** Vacíos de punibilidad en la ley	Sí	No	Sí	No	Sí	No	
1	¿Considera usted que existen vacíos en la ley de delitos informáticos? ¿Precise cuáles?	X		X		X		
2	¿Considera usted que es necesario incluir el tipo básico de estafa en la ley de delitos informáticos? Explique su respuesta.	X		X		X		
3	¿Considera usted necesario que se incremente la pena en la estafa informática cuando interviene pluralidad de agentes u organizaciones delictivas? Explique su respuesta	X		X		X		
N°	**SUBCATEGORÍA 2:** Desarrollo del comercio electrónico por la pandemia	X						
4	¿Considera usted que el comercio electrónico se incrementó a raíz del aislamiento social obligatorio?	X		X		X		
5	¿Cómo evalúa el papel de las TIC en el desarrollo del comercio electrónico?	X		X		X		
6	¿Cree usted que la pandemia ha contribuido en generalizar el uso del internet para cometer defraudaciones? Explique su respuesta	X		X		X		
N°	**SUBCATEGORÍA 3:** Rol de los operadores de justicia							

7	¿Según su criterio cuáles son las principales dificultades que enfrenta la PNP y el Ministerio Público en la persecución del delito informático?	X		X		X		
8	¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito?	X		X		X		
9	¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?	X		X		X		

Observaciones (precisar si hay suficiencia): Si

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr: Miguel Angel Gonzales Barbadillo **DNI:** 16654994

Especialidad del validador: Doctor en Derecho y Ciencia Política y Magister en Derecho Constitucional y DD. HH.

Lima, 16 De Agosto de 2021

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El Ítem es apropiado al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem es conciso, claro y directo.

Nota: Suficiencia, se considera tal cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Anexo 7

Tabla 2

Matriz de caracterización de los sujetos de estudio

Tipo de labor que realiza	Código asignado	Cargo
Jueces	JI, J2, J3	Juez de la Corte Superior de Justicia de Lima Norte Juez de la Corte Superior de Justicia de Lima Norte Juez de Corte Superior de Justicia de Lima Norte
Fiscales	F1, F2, F3,	Fiscal Provincial del Ministerio Público - Lima Norte Fiscal Provincial de Lima Norte Fiscal Adjunto Provincial de Lima Norte. Dirincri Depincri Comas Depincri Los Olivos
Policías	P1, P2, P3	DEPINCRI Independencia DEPCOO-Departamento de apoyo a las investigaciones del Ministerio Publico
Abogados	A1, A2, A3	Abogado litigante Abogado litigante Abogado litigante

Anexo 8

Tabla 3

Caracterización de informantes

N°	Entrevistado / Código	Descripción
1	Oscar Crisóstomo Salvatierra (J1)	Juez Superior. Primera Sala Penal de Apelaciones. Corte Superior de Lima Norte
2	Rosa Conopuma Genebroso (J2)	Juez del Décimo Juzgado de Instrucción Preparatoria de la Corte Superior de Justicia de Lima Norte
3	Sara Ana Victoria, Muñoz Rivera (J3)	Juez del Décimo Primer Juzgado de Investigación Preparatoria de la Corte Superior del Juzgado de Lima Norte
4	Yandira Zevallos Pinto (F1)	Fiscal Adjunta Provincial del Pool de Fiscales del Distrito Fiscal de Lima Norte
5	Marco Ayrampo Gutiérrez (F2)	Fiscal Adjunto Provincial del Primer Despacho - 2° Fiscalía Penal Corporativa del Distrito Fiscal de Lima Norte
6	Rober Hernández Paredes (F3)	Fiscal Provincial Penal del Primer Despacho 8° Fiscalía Penal Corporativa del Distrito Fiscal de Lima Norte
7	Gibson Peña-Herrera Tuesta (P1)	Mayor de la Policía Nacional DEPINCRI Los Olivos Distrito Lima Norte
8	Marlon L. Díaz Chávez (P2)	Sub Oficial Brigadier de la Policía Nacional del Perú – DEPCOO PNP – División de apoyo a las investigaciones del Ministerio Publico
9	Eliseo Mejía Díaz (P3)	Sub Oficial de Primera-PNP DEPINCRI Independencia Distrito Lima Norte
10	Edwin Quichua Pérez (A1)	Abogado litigante
11	Jorge Carlos Campos Tapia (A2)	Abogado litigante
12	Hugo Alejandro Villanueva Areche (A3)	Abogado litigante

Anexo 9

INSTRUMENTO
GUIA DE ENTREVISTA

- TÍTULO: **Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad**

……

CARGO
:……

INSTITUCION :
……

OBJETIVO GENERAL: El desarrollo de esta tesis, pretende demostrar la necesidad de incluir de lege data el tipo básico de estafa en la Ley de Delitos Informáticos para reducir la impunidad.

---

1. Según su criterio ¿Cuál es la característica principal de la estafa como delito contra el patrimonio? Explique su respuesta
   _____
   _____
   _____
   _____
   _____
   _____
   _____

2. ¿Considera usted que se ha incrementado esta modalidad delictiva a raíz de la pandemia por COVID 19? Explique su respuesta
   _____
   _____
   _____
   _____
   _____
   _____
   _____

3. ¿Cuáles son las modalidades más usuales utilizadas por los delincuentes para embaucar a sus víctimas a través del Internet, según los medios de comunicación, y en su opinión que se puede hacer al respecto?
   _____
   _____
   _____
   _____
   _____

_____
_____

4. En su opinión ¿Cuál es la característica principal del delito informático? Explique su respuesta.

_____
_____
_____
_____
_____
_____
_____

5. ¿Considera usted que existen deficiencias en la actual Ley Especial de Delitos Informáticos N° 30096? Explique su respuesta.

_____
_____
_____
_____
_____
_____
_____

6. ¿Considera usted que se requieren conocimientos avanzados de informática para estafar a través del Internet? Explique su respuesta.

_____
_____
_____
_____
_____
_____
_____

OBJETIVOS ESPECIFICOS: Copar los vacíos de punibilidad en la Ley de Delitos Informáticos, lograr que se capacite en forma permanente a policías y fiscales y que se les dote de la logística adecuada para combatir con eficacia a la ciberdelincuencia.

7. En su opinión ¿Existen vacíos en la Ley de Delitos Informáticos para sancionar ciertas conductas delictivas cometidas en el espacio virtual? ¿Podría precisar cuáles?

_____
_____
_____
_____
_____
_____

8. ¿Considera usted que es necesario incluir el tipo básico de estafa en la Ley de Delitos Informáticos, cuando el engaño se produce a través del Internet? Explique su respuesta.

   _____
   _____
   _____
   _____
   _____
   _____
   _____

9. ¿Considera usted necesario que se incremente la pena en el fraude o estafa informática cuando interviene pluralidad de agentes? Explique su respuesta.

   _____
   _____
   _____
   _____
   _____
   _____
   _____

10. En su experiencia ¿Considera usted que el comercio electrónico se ha incrementado a raíz del aislamiento social obligatorio impuesto por el gobierno central? Explique su respuesta.

    _____
    _____
    _____
    _____
    _____
    _____
    _____

11. ¿Cómo evalúa usted el papel de las tecnologías de la información y la comunicación en el desarrollo del comercio electrónico? Explique su respuesta.

    _____
    _____
    _____
    _____
    _____
    _____
    _____

12. ¿Cree usted que la pandemia por el COVID 19 ha contribuido a generalizar el uso del Internet para cometer defraudaciones? Explique su respuesta.

    _____
    _____
    _____

_____
_____
_____
_____

13. En su opinión ¿Cuáles son las principales dificultades que enfrenta la PNP y el Ministerio Publico en la persecución del delito informático?

_____
_____
_____
_____
_____
_____
_____

14. ¿Considera usted que es necesario capacitar en forma permanente a policías y fiscales para combatir con mayor eficacia el ciberdelito?

_____
_____
_____
_____
_____
_____
_____

15. En su opinión ¿Qué tipo de mejoras logísticas deben tener policías y fiscales que se dedican a la persecución de estos delitos?

_____
_____
_____
_____
_____
_____

……
FIRMA

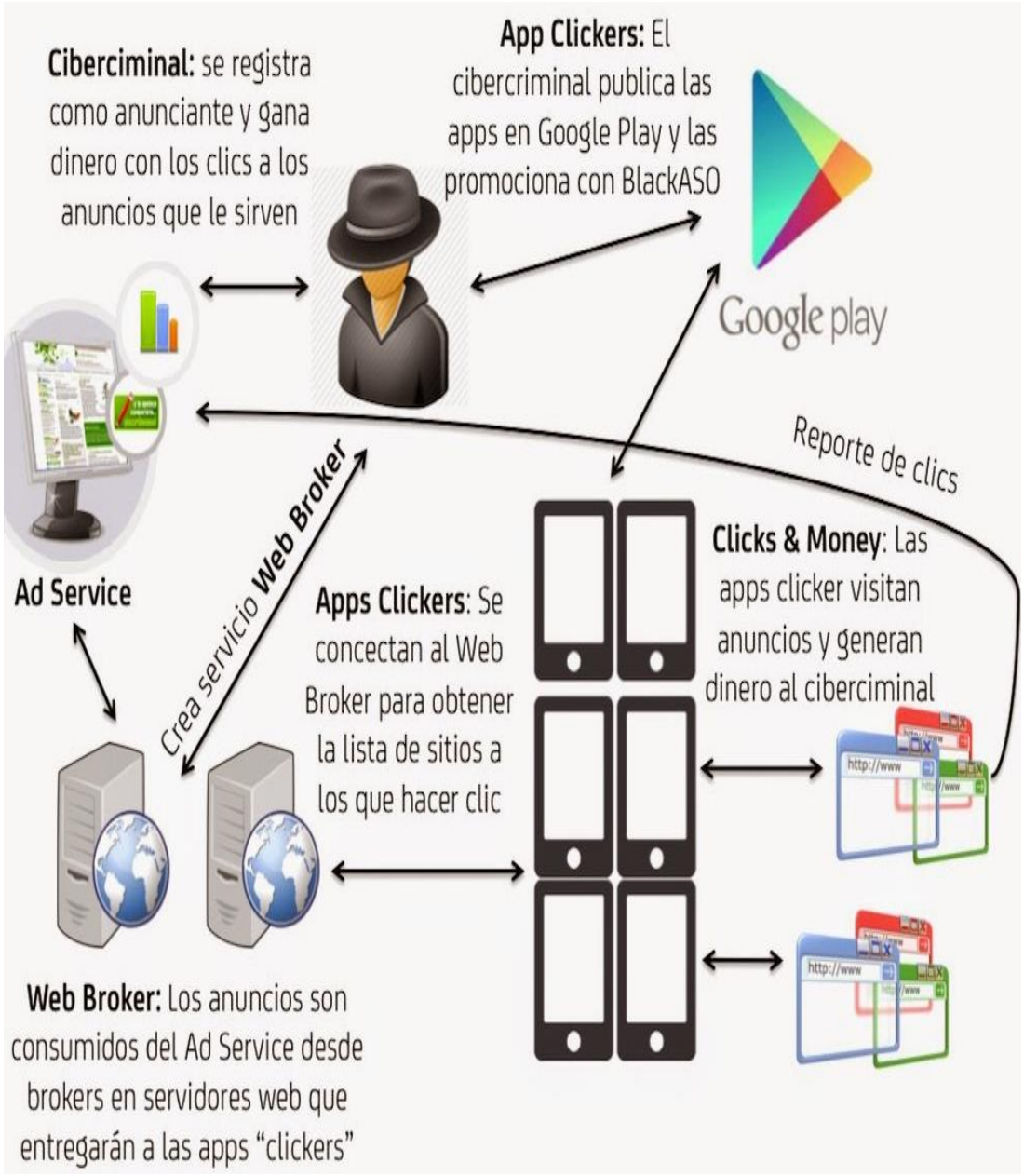
Anexo 10

Figura 1: Delitos cibernéticos: concepto y tipología

Fuente: Sain, 2018

Anexo 11

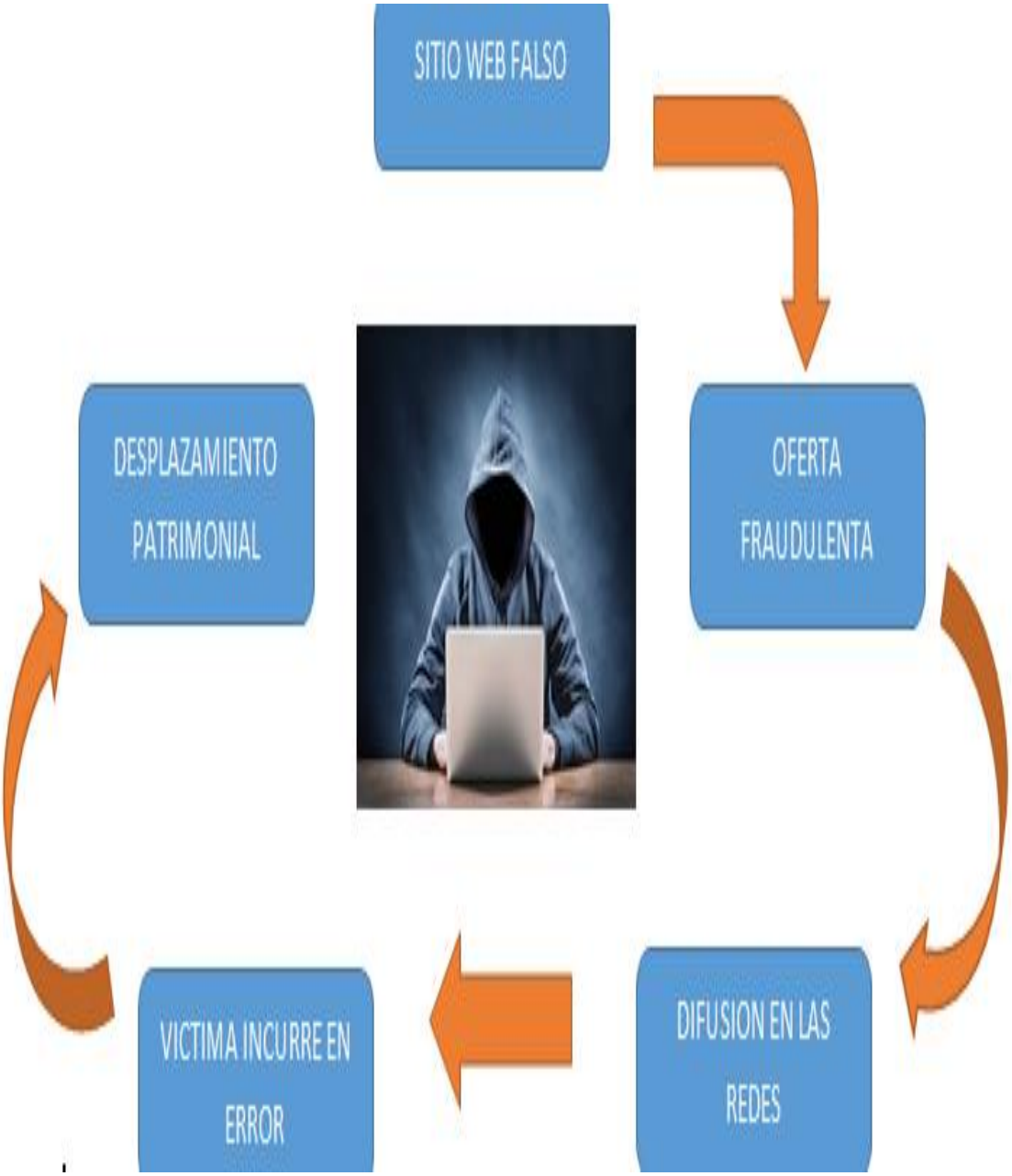
Figura 2: Ruta de la cibercriminalidad



Fuente: Sain, 2018

Anexo 12

Figura 3: *Esquema de la estafa informática*



Fuente: Sain, 2018

Anexo 13

Figura 4: *Ciberconsejos para evitar los delitos informáticos*

Fuente: Ministerio del Interior y Seguridad Pública, 2018. Equipo de respuesta ante incidentes de seguridad informática. Chile.

Anexo 14

Figura 5: Consejos para enfrentar los delitos cibernéticos

Fuente: Sain, 2018

Anexo 15

Figura 6: Tipos de fraude y estafas cibernéticas

Fuente: Ministerio del interior y Seguridad Pública, 2018. Equipo de respuesta ante incidentes de seguridad informática. Chile.

Anexo 16

Tabla 4: Denuncias por delitos informáticos registrados en Fiscalías Penales Comunes y Mixtas, de octubre 2013 a julio 2020

	2013		2014	2015	2016	2017	2018	2019	2020	TOTAL	%
LIMA	67		325	550	708	1495	2366	3713	1116	10340	47.68%
LIMA NORTE	3		24	24	99	174	357	717	220	1618	7.46%
AREQUIPA	1		18	47	155	255	291	506	115	1388	6.40%
LIMA ESTE	3		17	26	53	147	251	603	183	1283	5.92%
LA LIBERTAD	3		20	35	36	94	213	487	232	1120	5.16%
LAMBAYEQUE	1		11	31	82	119	182	326	124	876	4.04%
CALLAO	3		15	16	52	57	130	322	101	696	3.21%
LIMA SUR	1		4	9	27	52	120	355	119	687	3.17%
CUSCO	4		33	42	41	79	81	176	81	537	2.48%
ICA			3	10	22	24	91	195	57	402	1.85%
PIURA	3		10	33	15	34	68	134	40	337	1.55%
LORETO	1		7	15	24	48	93	100	32	320	1.48%
MOQUECUA	1		2	1	5	19	46	141	47	262	1.21%
SANTA			3	3	6	36	20	90	27	185	0.85%
HUANUCO			3	2	3	30	25	61	36	160	0.74%
JUNIN			5	7	5	16	44	52	27	156	0.72%
UCAYALI			4	6	9	18	43	44	15	139	0.64%
SAN MARTIN			3	4	6	32	31	49	13	138	0.64%
AMAZONAS	2		1	2	6	30	18	51	20	130	0.60%
CAJAMARCA	1		3	2	4	5	21	59	31	126	0.58%
AYACUCHO	2		3	2	9	9	24	50	15	114	0.53%
TACNA			6		5	4	20	50	15	100	0.46%
SU LLANA			3	12	9	12	15	25	15	91	0.42%
HUAURA			4	6	8	11	20	32	10	91	0.42%
ANCASH			2	4	5	12	20	35	8	86	0.40%
LIMA NOROESTE				2	6	3	15	31	15	72	0.33%
PUNO	1			3	3	12	8	15	6	48	0.22%
APURIMAC			3	1	1	2	18	13	4	42	0.19%
MADRE DE DIOS			2	3		3	1	23		32	0.15%
TUMBES			4	3	2	5	6	8	1	29	0.13%
HUANCAVELICA	1		1	2	3		4	17	1	29	0.13%
CAÑETE			1	1	1	1	1	15	3	23	0.11%
SELVA CENTRAL				3		1	1	5	8	18	0.08%
PASCO	1					2	4	4	1	12	0.06%
TOTAL	**99**		**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21687**	**100.00%**

Fuente: Reporte de la Oficina de Racionalización y Estadística del Ministerio Publico, remitido a la Oficina de Análisis Estratégico Contra la Criminalidad– Informe N° 4.

Anexo 17

Proyecto de ley que modifica el articulo 8° de la Ley N° 30096

En ejercicio del derecho a la iniciativa legislativa que confiere el articulo 107 de la Constitución Política del Perú en concordancia con lo dispuesto en el inciso c) del artículo 22 y los artículos 67, 75 y 76 del Reglamento del Congreso de la República, se presenta el siguiente proyecto de ley.

Articulo 1.- Objeto de la norma

La presente ley tiene por objeto modificar el artículo 8° de la Ley N° 30096 con el objeto de incluir en forma genérica los verbos rectores de la estafa básica en la Ley de Delitos Informáticos a efectos de sancionar conductas fraudulentas que se han incrementado en el espacio virtual a raíz de la pandemia originada por el Covid 19.

Articulo 2.- Alcance de la norma

La presente ley se aplica a cualquier persona natural o jurídica, cuyo accionar se subsuma en la ley, el sujeto activo no necesita cualificación especial.

EXPOSICIÓN DE MOTIVOS

La presente propuesta legislativa propende cerrar vacíos de punibilidad, en la Ley de Delitos Informáticos, habida cuenta que a raíz de la pandemia los fraudes se han incrementado en el espacio virtual, por lo que resulta necesario incluir cualquier conducta fraudulenta, propio de la estafa básica, en el capitulo de delitos contra el patrimonio de la Ley N° 30096, siempre y cuando el medio preponderante donde se despliega el engaño es el espacio virtual.

I. Fundamentos teóricos

El presente proyecto de ley tiene como fundamento jurídico la legislación comparada de otros países, sin embargo el factor preponderante para proponer la modificación ha sido un asunto de salud pública surgido por la pandemia, que obligo a miles de ciudadanos a volcarse al espacio virtual para adquirir bienes y servicios difíciles de adquirir en la forma tradicional, debido al aislamiento social obligatorio y las restricciones de tránsito impuestas o por el gobierno.

En ese sentido, consideramos que se deben tener en cuenta los aportes teóricos de Bustos y Zúñiga (2013) cuando en sus estudios enfatizan las deficiencias de la ley penal chilena para sancionar las nuevas conductas nocivas que afectando a sistemas informáticos no están reguladas en forma expresa, situación que generaba impunidad ante la dificultad de identificar a los agentes que se escudan en el anonimato u operan desde el extranjero, por lo que concluyeron que era necesario modificar la Ley 19.223 para recoger el enfoque europeo en la lucha contra la

ciberdelincuencia a la luz del convenio de Budapest. Su investigación fue útil porque permitió advertir las deficiencias de la Ley N° 30096, la misma que a pesar de contemplar la posibilidad de celebrar convenios multilaterales para perseguir el ciberdelito, éstos aún no se hacen efectivos.

Por otra parte García (2018) en su trabajo sobre el *Phishing* como modalidad de estafa informática, comentando una Sentencia de la Audiencia de Valencia, señala que el agente utiliza el engaño para clonar datos logrando que la víctima acceda a un *link* fraudulento, consiguiendo las claves de sus cuentas bancarias para luego realizar transferencias ilícitas. Utiliza la investigación descriptiva, siendo uno de sus propósitos que se establezca la responsabilidad cuasi objetiva de la institución financiera que provee estos servicios para proteger a los usuarios de la falta de diligencia de estas entidades que suelen protegerse con contratos lesivos que los exime de responsabilidad. Concluye que la protección a los usuarios es indispensable para que las entidades bancarias mejoren sus sistemas de seguridad y coadyuven a la policía para detectar estas conductas. El estudio es importante pues nos permite advertir que en España la estafa informática es el género y el *phishing* la especie, mientras en nuestro país el fraude informático es el género y la estafa informática que se pretende incluir vendría a ser la especie.

Por otro lado, Balmaceda (2011) en su estudio sobre la estafa informática en Europa Continental, explica que el fraude y la estafa comparten el uso de artimañas para lograr un beneficio personal en perjuicio ajeno; sin embargo, el fraude informático es una categoría criminológica más amplia pues involucra intereses económicos heterogéneos no solo patrimoniales, en cambio, la estafa informática alude solo a defraudaciones patrimoniales realizadas por medios informáticos. Su objetivo es que a ambas figuras se le brinde un tratamiento homogéneo pese a la existencia de posiciones doctrinarias dispares en lo referente a los límites de esa proximidad. El autor utiliza el estudio de casos emblemáticos acontecidos en Europa Continental para arribar a la conclusión de que el legislador chileno debería tipificar al delito de estafa informática para otorgar mayor seguridad jurídica a los usuarios de la red. Esta investigación nos brinda una aproximación somera del tratamiento que le dispensan a la criminalidad informática los diferentes sistemas legislativos en Europa.

Jain y Shrivastava (2014), en su artículo sobre el ciberdelito señalan que si bien el internet es una herramienta maravillosa que nos ha cambiado la vida, también ha traído consigo riesgos y amenazas para los que navegan y hacen transacciones por la red, debido al crecimiento exponencial de los fraudes, las extorsiones, los acosos y la pornografía infantil, por lo que proponen la adopción de convenios, estrategias preventivas globales y campañas de divulgación para alertar sobre los riesgos del cibercrimen, lo cual nos permite colegir que esas estrategias pueden ser de aplicación en el contexto nacional.

Quevedo (2017) en su tesis doctoral sobre la investigación y la prueba del delito informático, utilizando el estudio de casos formula recomendaciones para evitar que se frustre la recolección de medios probatorios cuando colisionan con derechos fundamentales. Detalla cómo ha de practicarse la investigación preliminar para superar los juicios de licitud y fiabilidad y luego analiza la valoración judicial de la prueba informática en base a profusa jurisprudencia europea sobre la materia. Sus conclusiones son útiles para nuestro estudio porque permite avizorar las dificultades prácticas a las que han de enfrentarse los operadores de justicia en la recolección de evidencia digital en la estafa informática.

Elías (2014) en su informe sobre la lucha contra la delincuencia informática en el país, hace un recuento cronológico de la evolución del delito informático hasta convertirse en una ley especial bajo los parámetros del Convenio de Budapest, empero, señala los defectos de técnica legislativa del legislador al promulgar la Ley 30171 que modifica a la LDI, al incorporar la frase “deliberada e ilegítimamente” en diversos artículos incluyendo el fraude informático, toda vez que resulta innecesario emplear el término “deliberadamente” en la tipificación de estos delitos ya que el artículo 12 del C.P. prevé que las penas establecidas en el código se aplican siempre al agente que obra con dolo, en cambio la infracción culposa solo es punible en los casos regulados en forma expresa.

Por su parte, Sánchez (2016) en su Manual Auto Instructivo sobre delitos informáticos alerta sobre los riesgos de *cyber* seguridad y el peligro del uso de las TIC en la actual sociedad de la información, debido a que los ciudadanos ponen en manos de terceros (proveedores de servicios) gran cantidad de

información que tiene que ver con su identidad, su patrimonio y su vida privada, por lo cual propugna que debe mantenerse incólume el Derecho al Secreto de las Comunicaciones y el uso restrictivo de esa información digitalizada en base de datos privadas, por lo que la información no relevante con contenido personalísimo debe ser tratada mediante protocolos debidamente establecidos y con límites claros en lo referente a la información a ser desclasificada en un proceso penal.

II. Antecedentes normativos

Ley N° 27309 publicada el 17 de julio 2000, incorporo el capítulo X sobre Delitos informáticos, incorporando el artículo 207 A, Interferencia, acceso o copia ilícita contenida en base de datos; artículo 207 B, Alteración, daño o destrucción de base de datos; articulo 207 C, Circunstancias agravadas.

Ley N° 30076 del 19 de agosto de 2013, incorporó el articulo 207 D, referente al tráfico ilegal de datos, en el capítulo de delitos informáticos del C.P.

Ley N° 30096 Ley de Delitos Informáticos promulgada el 22-10- 2013.

Ley N° 30171 del 10 de marzo de 2014, su finalidad fue adecuar la Ley 30096 a los estándares del convenio de cibercriminalidad o convenio de Budapest.

Ley N° 30838 modifico el articulo 5 de la Ley N° 30096 referente a los delitos contra la indemnidad y libertad sexual.

III. Análisis costo beneficio

En lo referente al impacto socioeconómico del presente proyecto de ley, debemos destacar que la modificación permitirá englobar en una sola norma las fronteras difusas del phishing, el vishing y el smishing de la estafa básica y la estafa agravada que solo se ocupa de tarjetas de débito o de crédito. Habida cuenta la diversidad de productos financieros que ofrece la banca y las empresas de seguros, siendo que en todas estas figuras el elemento central es el engaño que despliega el agente, (independientemente del soporte, plataforma o sistema al que pretende acceder) para hacerse del patrimonio de la víctima. Al final de cuentas lo que los diferencia es el know how del agente, el instrumento y/o la TIC empleada.

El primer beneficio que se identifica con la modificación legislativa es la reducción de la impunidad, lo que a su vez permitirá reducir la sensación de inseguridad ciudadana, habida cuenta el crecimiento exponencial de estos delitos a raíz de la pandemia, pues el operador punitivo podrá subsumir toda conducta fraudulenta empleada en el espacio virtual dentro del capítulo de delitos contra el patrimonio de la LDI. Además permitirá reducir la cifra negra de la criminalidad, toda vez que al incorporar la estafa básica en la LDI, el titular de la percusión penal podrá utilizar las herramientas y los plazos de la Ley N° 30077, Ley contra el crimen organizado dentro de los parámetros del convenio de Budapest.

En cuanto al costo de la implementación de la propuesta normativa, resulta pertinente que los operadores punitivos especializados (Fiscalía y PNP) articulen sus acciones a nivel nacional y cuenten con laboratorios de Análisis Digital Forense para tratar la evidencia digital y culminar con éxito sus investigaciones, por lo que el Ministerio del Interior y la Fiscalía de la Nación como titulares del pliego, deberán dotar del presupuesto necesario a sus unidades especializadas para el mantenimiento de estos laboratorios.

Empero, se concluye que los beneficios de la modificación legislativa superan con creces los costos de implementación al estar involucrada de por medio la seguridad ciudadana.

Texto sustitutorio del Artículo 8° de la Ley N° 30096 Fraude informático

El que deliberada e ilegítimamente, empleando cualquier medio fraudulento procura para si 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 o soporte informático de cualquier índole, 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 intervengan dos o más personas o se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

Anexo 18

Tabla 5: Denuncias por delitos informáticos investigados por la DIVINDAT 2013-2020

Delito	2013	2014	2015	2016	2017	2018	2019	2020	Total	%
Abuso de Mecanismos informáticos	14	3	6	4	5	1	2	19	54	0.4
Suplantación De identidad	10	101	114	134	132	227	247	572	1537	12.6
Proposiciones A niños fines sexuales	9	9			29	94	49	100	290	2.4
Contra datos y sistemas Informáticos	38	62	47	47	104	126	159	177	760	6.2
Contra intimidad Y secreto de las comunicaciones						3	2	8	13	0.1
Fraude Informático	298	334	414	610	1219	1928	2097	2615	9515	78.2
Total	369	509	581	795	1489	2379	2556	3491	12169	100%

Fuente: Informe Nº 237-2020-DIRINCRI-DIVINDAT-SEC, remitido a la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Publico.

Anexo 19

INSTITUTO PACÍFICO
Actualidad Penal
Al día con el Derecho
PENAL • PROCESAL PENAL • PENITENCIARIO • CRIMINOLOGÍA

CONSTANCIA DE PUBLICACIÓN

Por medio de la presente, se hace constar que el artículo: "La necesidad de cambios en la ley de delitos informáticos a raíz de la pandemia de Covid 19", elaborado por el abogado Wilson Vargas Miñan, fue publicado en el n.° 83 de la revista ***Actualidad Penal*** del Instituto Pacífico, correspondiente al mes de mayo del 2021. La Revista en mención es una publicación de naturaleza mensual ubicada en los datos de Latindex en el Folio n.° 25380 y Folio único n.° 22616.

Constancia que se expide a petición de la parte interesada,

Breña, 2 de diciembre del 2021

Lynda Josefina Fernández Olivas

Editora de ***Actualidad Penal***

editorpenal1@institutopacifico.pe

Instituto Pacífico SAC

Jr. Castrovirreyna 224 – Breña, Lima-Perú

Anexo 20

DOCTRINA PRÁCTICA

La necesidad de cambios en la Ley de Delitos Informáticos a raíz de la pandemia de COVID-19

Wilson Vargas Miñan*
Universidad de San Martín de Porres

SUMARIO

RESUMEN:

El autor analiza la importancia de incluir los verbos rectores del delito de estafa básica en la Ley N.° 30096, Ley de Delitos Informáticos, para combatir y sancionar con mayor eficacia el crecimiento exponencial de los delitos que se cometen a través del internet, por el incremento del comercio electrónico a raíz de la pandemia de COVID-19.

Palabras clave: Ciberdelito / Fraude informático / Delitos contra el patrimonio / Estafa básica / Medios fraudulentos / Ley N.° 30096 / Convenio de Budapest.

Recibido: 13-2-21
Aprobado: 1-3-21
Publicado en línea: 1-6-21

ABSTRACT

In this article the author analyzes the importance of including the guiding verbs of the crime of basic fraud inside the Law N.° 30096, Law of Computer Crimes, to combat and punish more effectively the exponential growt of crimes that are committed through the internet, due to increase in electronic commerce as a result of the pandemic caused by coronavirus infection.

Keywords: *Cybercrime / Computer fraud / Crimes against property / Basic fraud / Fraudulent means / Law N.° 30096 / Budapest Convention*

Title: *Necessity for changes in the Law on Computer Crimes as a result of pandemic caused by coronavirus infection*

* Abogado por la Universidad de San Martín de Porres. Maestro en Derecho Penal y Procesal Penal por la Universidad César Vallejo.

1. Introducción[1]

La trascendencia del fenómeno informático, según indica Pérez López[2], 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.

¿SABÍA USTED QUE?

Para apoderarse del 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, lanzan ofertas irreales de bienes y servicios que registran gran demanda por la pandemia.

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 merca-

1 El presente artículo es la base de un proyecto de tesis del suscrito en el programa académico de doctorado en Derecho por la Universidad César Vallejo.

2 Pérez López, Jorge, *Delitos regulados en leyes especiales*, Lima: Gaceta Jurídica, 2019.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

dería 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[3]. 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,

3 El art. 8 de la Ley N.° 30096 señala: "El que deliberada e ilegítimamente procura para sí o para otro un perjuicio 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 pena privativa de libertad no menor de tres ni mayor de ocho años [...]".

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.

2. Antecedentes

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.

¿SABÍA USTED QUE?

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.

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

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2413-2285 (en línea)

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.

3. Concepto y características 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[4]. 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 Díaz, al principio el ilícito informático se limitaba al ámbito patrimonial[5], 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

4 Hernández Díaz, Leyre, "El delito informático", en *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, n.° 23, San Sebastián: diciembre del 2009, pp. 228 y 230. Recuperado de <https://bit.ly/2RYsTBn>.

5 Hernández Díaz, "El delito informático", art. cit., p. 230. Sobre los delitos informáticos de carácter patrimonial, véase Romeo Casabona, Carlos M., "Delitos informáticos de carácter patrimonial", en *Informática y Derecho*, n.° 10, 1.ª época, Madrid: 1996.

fraudes informáticos, entendidos estos como manipulación o interferencia en el funcionamiento de sistemas informáticos que causen perjuicios patrimoniales.

Salinas Siccha 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"[6]. 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"[7]. 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 Díaz[8], 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 Fernández 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.

6 Salinas Siccha, Ramiro, *Derecho penal. Parte especial*, 5.ª ed., Lima: Grijley, 2013, pp. 1300 y 1301.

7 Villavicencio Terreros, Felipe, "Delitos informáticos", en *Ius et Veritas*, n.° 49, Lima: diciembre del 2014, p. 286. Recuperado de <https://bit.ly/3hA565v>.

8 Hernández Díaz, Leyre, "El delito informático", en *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, n.° 23, San Sebastián: diciembre del 2009. Recuperado de <https://bit.ly/2RYsTBn>.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

Las características de los delitos informáticos, según apunta MORILLAS FERNÁNDEZ[9], son los siguientes:

— 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.

— La falta de regulación en la red dificulta la verificación de la información que circula en el ciberespacio.

— El anonimato prima en la mayoría de transacciones de bienes y servicios. Existe gran facilidad para borrar las huellas perceptibles del delito.

— 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.

— Existe indeterminación en las víctimas, pues los destinatarios de las ofertas fraudulentas son el colectivo social, cuyos miembros ni siquiera son conocidos por el agente.

— 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.

¿SABÍA USTED QUE?

El bien jurídico en los delitos informáticos 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. En cambio, en sentido amplio la cibercriminalidad engloba también a ciertos delitos tradicionales cometidos a través de computadoras y/o el internet.

3.1. 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 sabo-

9 MORILLAS FERNÁNDEZ, David, "Delitos informáticos", en *Material de la maestría en derecho penal económico internacional*, Granada: Universidad de Granada, 2017, p. 32.

taje 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"[10].

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[11].

Por su parte, Palomino Ramírez 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[12].

10 Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", en *Revista Chilena de Derecho*, vol. 44, n.º 1, Santiago: 2017, p. 255. Recuperado de <https://bit.ly/3eUyFgr>.

11 Gutiérrez Francés, María, "Atentados contra la información como valor económico de empresa", citada por Villavicencio Terreros, "Delitos informáticos", art. cit., pp. 288 y 289.

12 Palomino Ramírez, Walter, "El intrusismo y otros delitos informáticos regulados en la Ley

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

4. El delito de fraude informático en la Ley N.° 30096

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 nom-

N.° 30096", en *Gaceta Penal & Procesal Penal*, n.° 56, Lima: 2014, p. 145.

bres de terceros, aunque estos terceros sean personas con incapacidad relativa (farmacodependientes) o personas jurídicas dadas de baja por el registro.

Según García Cavero, 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"[13].

5. Incremento del comercio electrónico en la red de redes

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.° 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.

IMPORTANTE

La redacción del art. 8 de la LID 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.

Otra de estas normas es la Ley N.° 27269, Ley de Firmas y Certificados Digitales, y el D. S. N.° 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

13 García Cavero, Percy, *Derecho penal económico*, 2.ª ed., t. I, Lima: Instituto Pacífico, 2015, pp. 312 y 315.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

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[14].

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 %[15].

Respecto a las regulaciones y control del *e-commerce*, Arocena Alonso y Esparza Leibar[16] 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.

¿SABÍA USTED QUE?

Para diferenciar entre el fraude informático y el atentado contra la integridad de datos informáticos 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.

6. 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

14 Noticias de Business Empresarial, sobre la empresa Pagos Digitales Peruanos, que administra la billetera móvil BIM, publicada en su página web el 26 de enero del 2021.

15 BlackSip, *Reporte de industria: el e-commerce en Perú 2020*, Lima: BlackSip, 2020.

16 Arocena Alonso, Lorena e Iñaki Esparza Leibar, "Los retos procesales de la criminalidad informática desde una perspectiva española", en *Novum Jus*, vol. 11, n.º 1, Bogotá: enero-junio del 2017. Recuperado de <https://bit.ly/3u8stWt>.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

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 prestamos o realizar los servicios ofrecidos[17]. En fin, los ciberdelincuentes tienen una creatividad monumental.

17 Superintendencia de Banca, Seguros y AFP, "Advertencia sobre préstamos fraudulentos por internet", en *Superintendencia de Banca, Seguros y AFP*, Lima: 8 de julio del 2018. Recuperado de <https://bit.ly/3oyG1cJ>; Superintendencia de Banca, Seguros y AFP, "Advertencia sobre casos de informalidad financiera", en *Superintendencia de Banca, Seguros y AFP*, Lima: 20 de agosto del 2019.

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.

Recuperado de <https://bit.ly/3fxRULZ>; Superintendencia de Banca, Seguros y AFP, "SBS advierte a la ciudadanía no dejarse sorprender por entidades informales que ofrecen grandes ganancias por su dinero", en *Superintendencia de Banca, Seguros y AFP*, Lima: 9 de junio del 2020. Recuperado de <https://bit.ly/3bJxDSp>; Superintendencia de Banca, Seguros y AFP, "SBS advierte al público sobre aparición de nuevos esquemas de captación de dinero sin contar con la autorización respectiva", en *Superintendencia de Banca, Seguros y AFP*, Lima: 14 de abril del 2021. Recuperado de <https://bit.ly/3fumsy2>.

7. 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

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

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 Hoyos[18] 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,

18 Balmaceda Hoyos, Gustavo, "El delito de estafa informática en el derecho europeo continental", en *Revista de Derecho y Ciencias Penales*, n.° 17, Santiago: 2011. Recuperado de <https://bit.ly/3otEnc4>.

ESPINOSA SÁNCHEZ[19] 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.

CONCLUSIÓN MÁS IMPORTANTE

La inclusión de la frase "cualquier medio o conducta fraudulenta" en el primer párrafo del art. 8 de la LDI facilitará el trabajo de los operadores punitivos para perseguir y sancionar conductas típicas en donde, empleando el internet o las TIC, prima el ardid o engaño para apoderarse del patrimonio de víctimas incautas

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). 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.

19 ESPINOSA SÁNCHEZ, Jesús F., "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", en *La Razón Histórica*, n.° 44, Murcia: septiembre-diciembre del 2019. Recuperado de <https://bit.ly/3tYjR4z>.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)

8. Conclusiones

La inclusión de la frase "cualquier medio o conducta fraudulenta" en el primer párrafo del art. 8 de la LDI facilitará el trabajo de los operadores punitivos para perseguir y sancionar conductas típicas en donde, empleando el internet o las TIC, prima el ardid o engaño para apoderarse del patrimonio de víctimas incautas.

Al tratarse de un delito de dominio en donde intervienen verdaderas organizaciones criminales, se debe contemplar en el art. 8 de la LDI la agravante de pluralidad de agentes para sancionar con mayor severidad estas conductas.

La capacitación de la policía especializada (Divindat) y los fiscales penales especializados debe tener carácter permanente, de lo contario la persecución de estas actividades delincuenciales se tornaría ilusoria.

La tipificación de la estafa básica en la forma propuesta permitirá a los operadores punitivos la obtención en tiempo real de datos relativos al tráfico de información en la red y hacer uso de los principios generales relativos a la asistencia mutua que contempla el Convenio de Budapest.

9. Referencias bibliográficas

Arocena Alonso, Lorena e Iñaki Esparza Leibar, "Los retos procesales de la criminalidad informática desde una perspectiva española", en *Novum Jus*, vol. 11, n.º 1, Bogotá: enero-junio del 2017. Recuperado de <https://bit.ly/3u8stWt>.

Balmaceda Hoyos, Gustavo, "El delito de estafa informática en el derecho europeo continental", en *Revista de Derecho y Ciencias Penales*, n.º 17, Santiago: 2011. Recuperado de <https://bit.ly/3otEnc4>.

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

Elías Puelles, Ricardo, *Luces y sombras en la lucha contra la delincuencia informática en el Perú*, Lima: Hiperderecho, 2014. Recuperado de <https://bit.ly/3eVew9W>.

Espinosa Sánchez, Jesús F., "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", en *La Razón Histórica*, n.º 44, Murcia: septiembre-diciembre del 2019. Recuperado de <https://bit.ly/3tYjR4z>.

García Cavero, Percy, *Derecho penal económico*, 2.ª ed., t. I, Lima: Instituto Pacífico, 2015.

Hernández Díaz, Leyre, "El delito informático", en *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, n.º 23, San Sebastián: diciembre del 2009. Recuperado de <https://bit.ly/2RYsTBn>.

Jiménez Herrera, Juan Carlos, *Manual de derecho penal informático*, Lima: Jurista Editores, 2017.

Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", en *Revista Chilena de Derecho*, vol. 44, n.º 1, Santiago: 2017. Recuperado de <https://bit.ly/3eUyFgr>.

Mazuelos Coello, Julio F., "Los delitos informáticos: una aproximación a la regulación del código penal peruano", en *Revista Peruana de Doctrina y Jurisprudencia Penales*, n.º 2, Lima: 2001.

Morillas Fernández, David L., "Delitos informáticos", en *Material de la maestría en derecho penal económico internacional*, Granada: Universidad de Granada, 2017.

Observatorio Ecommerce, *Reporte oficial de la industria ecommerce en Perú. Crecimiento de Perú y Latinoamérica 2009-2019*, Lima: Cámara Peruana de Comercio Electrónico, s/f. Recuperado de <https://bit.ly/3tZzyZt>.

Palomino Ramírez, Walter, "El intrusismo y otros delitos informáticos regulados en la Ley N.º 30096", en *Gaceta Penal & Procesal Penal*, n.º 56, Lima: 2014.

Pardo Vargas, Alejo, *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*, tesis para optar el grado académico de maestro en Derecho Penal y Procesal Penal por la Universidad César Vallejo, Lima: 2018.

Pérez López, Jorge, *Delitos regulados en leyes especiales*, Lima: Gaceta Jurídica, 2019.

Romeo Casabona, Carlos M., "Delitos informáticos de carácter patrimonial", en *Informática y Derecho*, 1.ª época, n.° 10, Madrid: 1996.

Rico Carrillo, Mariliana, "Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos", en *Revista IUS*, vol. 7, n.° 31, Puebla: 2013. Recuperado de <https://bit.ly/2Rwuu1g>.

Salinas Siccha, Ramiro, *Derecho penal. Parte especial*, 5.ª ed., Lima: Grijley, 2013.

Villavicencio Terreros, Felipe, "Delitos informáticos", en *Ius et Veritas*, n.° 49, Lima: diciembre del 2014. Recuperado de <https://bit.ly/3hA565v>.

Zevallos Prado, Óscar, "Delitos informáticos: ¿cuáles son los principales fraudes informáticos que se pueden cometer a través del e-commerce?", en *Ius 360*, Lima: 22 de mayo del 2020. Recuperado de <https://bit.ly/3hBlylS>.

Número 83 • Mayo 2021 • pp. 83-100
ISSN 2313-268X (impresa) • ISSN 2415-2285 (en línea)