FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE

ABOGADO

AUTOR:

Lujan Ccorahua Zakir Temir (ORCID: 0000-0001-7552-3082)

ASESOR:

Mg. Lázaro Ortiz Yanira (ORCID: 0000-0002-5628-4086)

LÍNEA DE INVESTIGACIÓN

Derecho Penal - Procesal Penal - Sistema de Penas, Causas y Formas del Fenómeno Criminal

LIMA – PERÚ

2022

DEDICATORIA

Dedico el presente trabajo académico a la memoria de mi padre quien en vida fue el Gran escultor *Víctor Humberto LUJÁN RODRÍGUEZ.*

AGRADECIMIENTO

En primer lugar, quiero agradecer a mi esposa e hija gracias a ellas porque en todo momento fueron un apoyo incondicional en mi vida, por siempre estar ahí aun cuando mis ánimos decaían. Ellas demuestran mi felicidad, son mi todo reflejado a quienes amo demasiado por quienes estoy dispuesto a enfrentar todo y en todo momento.

En especial, quiero hacer mención de mis padres, que siempre estuvieron ahí para darme palabras de aliento y un abrazo reconfortante.

También quiero agradecer a Universidad Cesar Vallejo por brindarme todos los recursos y herramientas que fueron necesarios para llevar a cabo el proceso de investigación.

A todos mis profesores que con sus conocimientos y experiencias vertidos en las aulas universitarias, ayudaron a forjar mi carrera profesional.

Por último, quiero agradecer a mi asesora, quien con sus conocimientos y apoyo me guio a través de cada una de las etapas de este proyecto para alcanzar los resultados que buscaba.

Índice de Contenido

RESUMEN

La presente investigación tuvo como objetivo, analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, en el año 2022; se realizó bajo el tipo de investigación básica, bajo el enfoque cualitativo y teniendo como diseño el fenomenológico. El instrumento utilizado fue la guía de entrevista, la cual fue aplicada a los operadores de justicia del distrito Judicial de Lima; abogados, fiscales, policías y jueces.

Los resultados obtenidos permiten advertir que los órganos especializados en delitos informáticos no se encuentran capacitados ni cuentan con las herramientas para realizar sus funciones de manera eficaz; toda vez que estos delitos tienen peculiaridades y son cambiantes de acuerdo a la innovación tecnológica. Asimismo, es necesario la actualización de la ley de delitos informáticos para poder precisar el tratamiento jurídico a aquellos tipos de delitos informáticos como la de suplantación de identidad y las diferentes formas de accionar delictivas derivadas de este delito.

Se concluyó que a pesar de la existencia de una norma legal que establece el tratamiento jurídico penal para estos delitos informáticos, aún existe ambigüedad en la tipología y penas muy leves, lo que conlleva a sentencias no efectivas.

Palabras claves: Delitos informáticos, Suplantación de identidad, fraude informático, ciberataque

ABSTRACT

The objective of this research was to analyze the criminal legal treatment of computer crimes against property and public faith in the Judicial District of Lima, in the year 2022; It was carried out under the type of basic research, under the qualitative approach and having the phenomenological design. The instrument used was the interview guide, which was applied to the justice operators of the Judicial District of Lima; lawyers, prosecutors, police and judges.

The results obtained allow us to notice that the specialized agencies in computer crimes are not trained or have the tools to perform their functions effectively; since these crimes have peculiarities and are changing according to technological innovation. Likewise, it is necessary to update the computer crime law in order to specify the legal treatment for those types of computer crimes such as identity theft and the different forms of criminal actions derived from this crime.

It was concluded that despite the existence of a legal norm that establishes the criminal legal treatment for these computer crimes, there is still ambiguity in the typology and very light penalties, which leads to ineffective sentences.

Keywords: Computer crimes, identity theft, computer fraud, cyber attack

I. INTRODUCCIÓN

La situación en pandemia que se vive desde enero 2020 a causa del SARS-CoV2, ha generado que los países implementen diversas medidas que permitan el restablecimiento de la salud en la población; una de ellas fue el aislamiento social obligatorio, la cual trajo como consecuencia el trabajo remoto y el aumento del e commerce, ya sea desde las empresas como de la población. Este nuevo escenario fue pretexto para el aumento de fraudes digitales y ciberataques; delitos que vulneran los estándares de seguridad. La expansión del uso de sistemas informáticos y de telemática en los ámbitos público y privado puede favorecer la práctica delictiva de cualquier tipo de delito, constituyéndose en un nuevo canal que facilita su operación. Es por ello que los Estados mundiales tienen la gran responsabilidad de regular las políticas instauradas en la época de pandemia. Bokovnya, et al. (2020)

La variedad y complejidad de los delitos informáticos, han llevado a muchos países a implementar nuevas figuras penales de acciones relacionadas al uso de medios informáticos. De un análisis del derecho comparado sobre delitos informáticos en América Latina al 2014, se puedo evidenciar que, respecto al tipo penal, delito de violación de datos personales, implementaron normativa los países de Argentina, Brasil, Colombia, Costa Rica, Ecuador, Guatemala y Puerto Rico. Respecto al delito Suplantación de identidad digital, solo tres países de América implementaron normativa, República Dominicana, Puerto Rico y Costa Rica. Asimismo, se identificó que Puerto Rico fue el país con niveles de sanción penal altos respecto a delitos informáticos (91%). Estos datos estadísticos sugieren la urgencia de homogenizar en el ámbito sustantivo de la normativa penal aplicable a delitos informáticos en América Latina en general. Temperini (2014).

De acuerdo al reporte de ciberseguridad en Latinoamérica y el Caribe emitido por BID y OEA en el 2020, sostiene que el cibercrimen representa, un aproximado del 50% de los delitos en el mundo contra la propiedad. También afirman que los perjuicios económicos por estos delitos podrían representar el 1% del PBI en algunos países; aumentando esta cifra cuando se exponen los daños a la

infraestructura crítica representando el 6% del PBI. A su vez, el crecimiento en el uso de herramientas digitales en la región, la coloca en la mira para diversas modalidades de fraude en la creación de cuentas. Este panorama llevó a implementar nuevamente el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones, el cual permite medir el crecimiento y desarrollo de las capacidades de los Estados miembros en su defensa ante amenazas cibernéticas. Es importante considerar que los delitos informáticos no solo amenazan las economías, sino también la democracia, libertades y valores.

El informe del Foro Económico Mundial respecto a los Riesgos Globales en el 2020, ubicó entre los 10 principales riesgos con mayor probabilidad de ataques cibernéticos a la infraestructura crítica y el fraude o robo de datos.
Las cifras de registros de datos robados durante el año 2019, alcanzan los 8500 millones de registros de datos personales, los cuales son comercializados y utilizados en red para ataques de ingeniería social. Los delitos informáticos seguirán evolucionando al ritmo que lo hacen los contextos sociales, económicos y tecnológicos. IBM (2020).

El Perú, en el primer trimestre del 2021, registró 1 188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (DIVIDANT) de la Policía Nacional del Perú. Los casos frecuentes se relacionaron al fraude informático y a la suplantación de identidad. De las denuncias realizadas, 600 son sobre fraudes informáticos, relacionados a hechos como compras fraudulentas por internet, retiros y transferencias de fondos no autorizados y clonación de tarjetas. Respecto a suplantación de identidad se han atendido 296 denuncias, las cuales se duplicaron en relación al 2020. En los últimos cinco años la Policía desarticuló 40 bandas criminales por delitos informáticos y en el 2020 detuvieron a 225 implicados por estos delitos. Andina (2021), El Peruano (2021).
Este contexto llevó a formular el siguiente problema de investigación: ¿De qué manera se da el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021?; a partir de este problema general de investigación se formularon los siguientes problemas específicos: ¿De qué manera se da el tratamiento jurídico penal del delito fraude informático en el

Distrito Judicial Lima,2021?, ¿De qué manera se da el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021?

La investigación se justifica teóricamente, en el uso y análisis de teorías modernas vinculadas a la sanción penal de los delitos informáticos recurrentes en los años 2020-2021, años de inicio y auge de la pandemia por COVID 19 y la obligada transformación a la digitalización. La justificación práctica recae en que los resultados de la investigación permiten servir de sustento para la actualización de legislación en el campo de delitos informáticos.

Por otro lado, la justificación metodológica, recae en la sistematización y análisis de jurisprudencia, dispositivos legales y entrevistas a los actores claves de la investigación; adecuando los procedimientos al método científico.

La investigación adquiere relevancia jurídica, académica y doctrinaria, toda vez que el tema es vigente y cambiante ante los diversos escenarios sociales, económicos y tecnológicos.

Por lo tanto, se planteó el siguiente objetivo general del estudio: Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021. Así como los objetivos específicos: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021. Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021

II. MARCO TEORICO

Los antecedentes teóricos relacionados con la investigación están determinados por los trabajos previos, los cuales se presentan a continuación:

Bokovnya, et al. (2020); en su investigación titulada *Computer crimes on the COVID-19 scene: Analysis of social, legal, and criminal threats.* cuyo objetivo fue analizar las consecuencias sociales y legales de los delitos informáticos durante la pandémica COVID-19l. La metodología utilizada en base a un enfoque de revisión sistemática, utilizando para ello métodos como la dialéctica, la lógica, generalizaciones científicas, el análisis de contenido, el análisis comparativo, la síntesis, entre otros. Los resultados mostraron que todos los países en el mundo adoptaron medidas sociales y económicas para frenar los efectos de la pandemia, siendo algunos de ellos, la provisión de servicios diferenciados y asignaciones y beneficios para grupos vulnerables; de igual manera la preservación de incentivos al trabajo, la asistencia para encontrar trabajo, obtener servicios de salud y aprobar programas educativos y de capacitación. También se identificó los grupos de ataques criminales que adquirieron el carácter de tendencia estable: ciberataques masivos en la infraestructura de acceso remoto, crecimiento de ataques de phishing y la propagación de malware en relación con el crecimiento de la audiencia digital, adaptación de esquemas de fraude “clásicos”, ataques y hackeos a plataformas de comunicación digital, crecimiento de fenómenos delictivos en el juego online, mayor demanda y distribución de material pornográfico a través de redes sociales.

Se concluye que, ante las prioridades de preservar la salud y economía, los países vieron deteriorados los estándares de seguridad en el contexto de cuarentana social, exponiendo las limitaciones para un adecuado trabajo remoto en empresas tanto público como privadas; de este modo quedan expuestas a ser víctimas de delitos cibernéticos , los cuales seguirán creciendo en el futuro cercano.

Según Cherniavskyi, et al. (2021), en su artículo científico Measures to combat cybercrime: analysis of international and Ukrainian experience. Buscó analizar las medidas utilizadas por diversos países para combatir el cibercrimen y el caso ucraniano en particular. La investigación tuvo un diseño de revisión sistemática a partir de legislación e informes de la comunidad internacional. Se concluyó que

Ucrania debe mejorar el uso de la base de información de la nación, el desarrollo de la producción de información y los sistemas de comunicación de información social, lo cual le permitirá una mejor posición en la cooperación internacional. Los problemas de seguridad cibernética son muy importantes para el estado ucraniano lo que se debe a la necesidad de resistir la invasión ilegal del espacio de información del país, la preservación de los recursos de información, la protección de la población contra la influencia negativa de la información y más. Es preciso mencionar que es prioridad estratégica para Ucrania la integración europea, por lo que requiere mejorar el marco regulatorio para la seguridad cibernética. Por último, La guerra cibernética puede provocar crisis en países que pueden llevar a la desintegración de estos; por lo que los riesgos potenciales están dados por las vulnerabilidades a la intrusión exterior.

Alanezi, (2016), en su tesis con el título Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions. Tuvo como objetivo examinar la percepción de fraude en línea y las contramedidas diseñadas y utilizadas por las instituciones financieras en Arabia Saudita para el control y prevención del fraude en línea en su contexto ambiental, examinar la efectividad/impacto de las contramedidas. Se realizó bajo en enfoque de investigación cualitativa. Los resultados encontrados demuestran los esfuerzos de las instituciones para implementar medidas utilizando medios tecnológicos junto a controles y controles de procedimientos. A pesar de ello los usuarios consideran que estas medidas son engorrosas. Se identificó dos tipos de regulaciones, por un aldo reglas gubernamentales y organizacionales, que en su mayoría se centran en el monitoreo de las operaciones de internet y lineamientos operativos. La La persecución de los infractores ha sido mínima y pasiva.

Mayer (2018), en su artículo científico titulado, Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Cuyo objetivo fue examinar los elementos criminológicos que contribuyen al análisis jurídico-penal de los delitos informáticos, utilizó como metodología la revisión de literatura de estudios nacionales y extranjeros, sentencias chilenas sobre conductas incorporadas en la Ley 19223. Las conclusiones a las que arriba están relacionadas con que algunos

usuarios de internet expresan miedo desmedido ante la posibilidad de ser víctimas de cibercrímenes, también sostiene que las víctimas potenciales perciben de manera limitada el riesgo por lo que no toman mayores medidas de autoprotección, esto se agrava por el conocimiento limitado ante los riesgos o conocimiento errado de los mismos. Por ello recomienda la sensibilización oportuna a la sociedad respecto a los riesgos que conlleva el uso de tecnología moderna.

Según Mayer (2017) en su estudio intitulado: *El bien jurídico protegido en los delitos informáticos*. cuyo objetivo fue reflexionar sobre los roles que cumplen los sistemas informáticos en un Estado democrático de derecho, teniendo en cuenta la libertad de desarrollo de la persona y las instituciones a su servicio. La metodología utilizada tiene un diseño de revisión de literatura. Concluye que, en un Estado democrático de derecho la funcionalidad informática es un presupuesto para la operatividad en diversos ámbitos y actividades relevantes de personas e instituciones, por lo que se debe garantizar el adecuado funcionamiento de las operaciones de almacenamiento, transferencia de datos y tratamientos de los sistemas informáticos en un marco de riesgo tolerable. El reconocer la funcionalidad informática como bien jurídico, se justifica si los ciberdelitos, a la vez repercuten en el soporte lógico del sistema informático, implica el uso de redes computacionales. Además, de reconocerlo como bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particulares.

Temperini (2014), en su artículo científico titulado *Delitos informáticos en Latinoamérica: un estudio de derecho comparado.* Planteo como objetivo, analizar el estado situacional de los delitos informáticos en América Latina a partir del estudio comparado del derecho en su aspecto material sustantivo. La investigación tiene un diseño de revisión de literatura reflejada en la recolección de legislación aplicable en países como: Argentina, Brasil, Bolivia, Colombia, Chile, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela. A partir del análisis comparativo se identificó a los países que poseen sanción penal para determinados delitos informáticos, así pues, el 81% de los países en estudio plantean sanciones penales para menos del 40% de los delitos

incluidos en la investigación. Precisa también que falta homogenizar en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos de manera general en América Latina.

Según Pons (2017), en su artículo científico de revisión de literatura titulado : *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad*. Cuyo objetivo planteado fue analizar la visión de varios autores respecto a los ciberdelitos y la respuesta de las naciones para defenderse. Los resultados mostrados están relacionados a los delitos establecidos como ciberdelincuencia: chantaje, robo, fraude, malversación de fondos públicos, la falsificación; introduciendo además en la legislación española el descubrimiento y revelación de los secretos, el acoso electrónico contra la libertad de personas, , la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otro medio de comunicación a menores. Concluye que las leyes deben ir adaptándose a los constantes cambios y amenazas; para ello las naciones necesitan un conjunto de sistemas de defensa interconectado que traspase países.

Según Cortés, et al (2015), en su artículo científico intitulado: *La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio.* Su objetivo fue describir la efectividad judicial de la persecución penal de los delitos informáticos en el Distrito Judicial de Villavicencio, trabajo de enfoque cualitativo y que entrevistó a funcionarios públicos, así como la revisión de información pública. Los resultados confirman la tesis que sustenta la criminología crítica, considerando insuficiente la determinación de un tipo penal para la materialización de la persecución penal que es selectiva. Se concluye que los delitos informáticos no son conocidos por el sistema penal colombiano, siendo las principales causas la ausencia de denuncias, así como de adecuados mecanismos de investigación oficiosa en la etapa de indagación penal. También se concluye que de las denuncias interpuestas solo 9 terminaron en condena, por lo que se evidencia una gran brecha en el proceso desde la denuncia hasta su terminación. Asimismo, los juzgados penales sobre delitos informáticos son solo 4 de categoría municipal. La carencia de Talento humano suficiente que permita iniciar una adecuada

investigación de delitos informáticos en la totalidad del Distrito Judicial. La carencia de formación técnica de los fiscales asignados a delitos informáticos.

Según Velásquez y Garrido (2016), en su artículo científico titulado, *El ciberilícito en Colombia: ¿ante cuál juez acudir?,* busca indagar sobre la interpretación en Colombia del criterio tradicional del escenario físico donde sucede el ciberilícito; para ello los autores utilizan el método dogmático, revisando soluciones dadas en el derecho extranjero pudiendo ser ejemplo al derecho colombiano y para los regímenes que aplican el criterio *loci delicti commissi.* De acuerdo a l estudio se identifica el domicilio de la víctima como el lugar en donde se sucedió el hecho. El legislador colombiano no ha tenido en cuenta que para determinar la jurisdicción en un ciberilícito , requiere una mejor concreción; el intérprete del derecho debe ejercer la hermenéutica y llevados a cabo en el ciberespacio. Las dificultades manifiestas pueden generar alta probabilidad de impunidad que tendría el agente dañoso ante los daños causados a una persona en o por medio de internet.

Según Aguilar (2019) en su investigación titulada *Suplantación de la identidad digital con fines de trata de personas en facebook"* cuyo objetivo fue diseñar una propuesta de intervención para prevenir la suplantación de identidad en medios digitales con fines de trata de personas, el método utilizado fue el inductivo-deductivo, para lo cual se elaboró una infografía digital que contine un mensaje de prevención y difusión de trata de personas a través de Facebook. Se evidenció que existe poca información sobre la definición de este delito; la suplantación de identidad digital se da con fines principalmente para perpetrar fraudes y extraer dinero de las víctimas de quienes obtuvieron datos financieros y bancarios. En México las leyes sobre suplantación de la identidad en medios digitales aún no están definidas como un ilícito.

Para Borghello y Temperini (2012) en su investigación que lleva por título, *Suplantación de Identidad Digital como delito informático en Argentina.*que buscó establecer las raíces de este tipo de delito informático, indagaron sobre el impacto, modos de ejecución y consecuencias en las víctimas, de igual manera se analizó la legislación vigente en la materia. Concluyen en que la identidad digital está estrechamente relacionada con la identidad personal de cada sujeto en los

aspectos psico social y moral; una de las raíces de este delito es lo sencillo que resulta la captación ilegitima de datos de identificación personal, también la carente legislación en la materia; limitada acciones de control en las entidades, los escasos niveles de educación en los usuarios de internet a pesar de que el manejo de redes sociales y telefonía móvil es alto. Recomienda que se unan esfuerzos para que la identidad digital sea un bien jurídico protegido y se tipifique penalmente, en Argentina, el delito de suplantación de identidad digital y la tenencia y trasferencia ilegitima de datos de identificación personal.

Fernandez y Vargas (2018) en su investigación que tuvo como título, *¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías;* cuyo objetivo fue determinar la relación existente entre el manejo de las TIC´S en el personal de una comisaría y si esto puede disuadir a los criminales en la acción de ciberdelitos. Para ello realizó una revisión sistemática teniendo como base de datos información del censo nacional de comisarías y Registro nacional de Delitos en las dependencias policiales; la unidad de análisis fueron las comisarías peruanas, que suman 1471 ; información de los años 2015 y 2016. Concluyeron que el uso de las TIC´s en las comisarías si cumple como señal significativa en la persuasión a los delincuentes de cometer delitos informáticos; las comisarías peruanas deben implementar más horas de uso de la computadora, registro digital de denuncias, entre otros. Es costos la implementación de la DIVIDANT en todo el Perú por lo que se sugiere potenciar el uso de tic´s en comisarías con mobiliarios adecuado y capacitación correcta al personal. Se comprobó la capacidad de las comisarías para luchar contra los ciberdelitos. Recomienda esbozar un perfil de los criminales cibernéticos o de las víctimas permitiendo que la policía tenga mayor probabilidad de captura.

Para Mori (2019), en su tesis *Los Delitos Informáticos y La Protección Penal de la intimidad en el Distrito Judicial De Lima, Periodo 2008 al 2012*, que tuvo como objetivo explicar las causas que influyen en el desacierto de los operadores de justicia (Policías, Fiscales y Jueces) en dicho distrito judicial. La investigación fue de tipo descriptiva explicativa. Los resultados alcanzados demuestran que los jueces, reconocen la carencia de formación tecnológica en delitos informáticos; sin

embargo, los policías y fiscales contradicen esa afirmación. Los jueces están de acuerdo con la impropia determinación del tipo penal, mientras que los policías y fiscales no están de acuerdo con ello. Concluye que la deontología tecnológica afecta la competitividad de los operadores de justicia que intervinieron en la investigación e influye en la impropia determinación del tipo penal.

Según Zambrano (2020), en su tesis *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020;* que tuvo como objetivo determinar si los delitos informáticos contra el patrimonio se promueven por el uso de banca móvil. Utilizó un tipo de investigación básica de enfoque cualitativo, la entrevista fue la técnica de recolección de datos utilizada. Las conclusiones de la investigación son que el uso de la banca móvil promueve los Delitos Informáticos Contra el Patrimonio, el Fraude Informático y la clonación de datos informáticos, toda vez que los datos informáticos de los clientes son clonados y con ellos se comete el fraude Informático y Delitos Informáticos que atentan contra el patrimonio.

Según Pardo (2018) en su tesis *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*; cuyo objetivo fue analizar los delitos informáticos contra el patrimonio y su tratamiento jurídico penal en dicho distrito judicial. Respecto a la metodología utilizada, tuvo un enfoque cualitativo de nivel descriptivo explicativo; la técnica utilizada fue la entrevista, aplicada a expertos sobre el tema tanto nacionales como extranjeros. Los resultados encontrados llevan a plantear la deficiencia en el manejo jurídico penal de delitos informáticos contra el patrimonio, ya que no es lógico que se incorpore dentro de fraude informático todos los tipos o modalidades de delitos informáticos contra el patrimonio; lo cual genera confusión en la interpretación de dicha norma, impidiendo la efectividad de la sanción contra estos delitos.

Las teorías relacionadas con la investigación están delimitadas por la teoría del delito, que de acuerdo a Muñoz (citado en Peña y Almanza, 2010), se entiende como aquel sistema de hipótesis, que teniendo en cuenta una determinada tendencia dogmática exponen los elementos que posibilitan o no la aplicación de

una consecuencia jurídico penal a una acción humana. Esto se sustenta en que es una estructura ordenada de conocimientos, utilizando para ello enunciados susceptibles de ser probados o confirmados por sus consecuencias. Al referirse a que posee una tendencia dogmática es porque no existe criterio único para su abordaje por lo que existen más de un sistema que trata de explicarlo en su naturaleza de ciencia social. Esta teoría tiene como objeto de estudio todo aquello que ocasiona la instauración de una pena o medida de seguridad.
Las teorías que intentan explicar el delito son diversas, pero para la presente investigación se consideran a la teoría del causalismo naturalista, propuesto por Liszt; esta teoría concibe al accionar delictivo desde una perspectiva física o naturalística, que va desde el movimiento corporal que da como resultado la alteración del mundo externo, unidos por un nexo causal. Peña (2010)

La “teoría de las normas”, planteada por Binding, quien sustenta que el ladrón no viola la ley sino el principio que prohíbe robar, en otras palabras el delincuente confirma la ley, no la contradice. Plasencia (1998)

La teoría del funcionalismo moderado, reconoce los elementos del delito : tipicidad, antijuridicidad, culpabilidad; orientándose a lo político-criminal ya que sus presupuestos de la punibilidad estarán orientados por los fines del Derecho penal

De acuerdo a lo sostiene Peña y Almanza (2010); el delito se define como el comportamiento humano con oposición al mandato o prohibición de la ley, bajo amenaza de una pena, en conclusión, la ley es la que precisa que hechos serán considerados delitos, así como también es la que fija caracteres delictivos a un hecho, por lo tanto, si la ley desaparece, también desaparece el delito. La concepción sociológica del delito, sostiene que el delito está determinado por las acciones antisociales e individuales que alteran las condiciones de coexistencia y lesionan la moralidad de una sociedad en un tiempo determinado. El concepto jurídico del delito está sostenido por diversos autores las cuales podría describirse de la siguiente manera:

- Según Beling, es una acción atípica contraria al derecho culpable, con

sanción de una pena adecuada y suficiente a la objetividad de la punibilidad.

- Carrara, define como la infracción a la ley de un Estado como producto del actuar externo del hombre en el sentido positivo o negativo, considerándose moralmente imputable y políticamente dañosos.
- Carmignani, acción humana castigada por la ley.
- Mezger, Acción pasible referida al conjunto de los presupuestos de la pena.
- Florián, acción inherente al hombre, contraria a la ley la cual es sancionada con pena.
- Mayer, Acontecimiento típico, antijurídico, imputable.

El concepto de delito desde lo legal, está amparado al código penal de 1991: “Lesión o puesta en peligro de un bien jurídico protegido legalmente con una sanción penal”.

La evolución de la sociedad conlleva también a la presencia de nuevos delitos que deben ir tipificados en los sistemas legales, el desarrollo tecnológico, la informatización, la interdependencia económica; han demandado la moderna Ciencia Penal, incorporando conductas criminales inmersas con la informática. Piña (2014)

El uso del término delito informático hace su aparición a fines de los años noventa, en paralelo con la expansión del internet, en Francia. Inicialmente este término se utilizó para describir delitos realizados en la red o redes de telecomunicaciones Azaola (2010)

Según Ramirez y Aguilera (2009) el delito informático lo constituye las conductas ilícitas expresadas en actividades criminales a través de medios informáticos, que son susceptibles de ser sancionadas por el derecho penal.

Según Levin y Ilkina (2013), el ciberdelito o delito informático es aquel crimen donde

se hace uso de las herramientas de la tecnología de la información y la comunicación o un dispositivo de almacenamiento en la comisión de un delito.

Para Villavicencio (2014) el crimen informático son las conductas que se dirigen a burlar los sistemas de dispositivos de seguridad, ya sea invasión a computadoras, correo electrónico o sistema de datos, mediante clave de accesos; conductas que solo pueden ser realizadas con el uso de tecnología; lo que no es lo mismo que sea solo por el hecho de usarlo.

Hance (1996) sostiene tres categorías para los delitos informáticos: Acceso no autorizado, actos dañinos o circulación de material dañino e interceptación no autorizada.

De acuerdo al convenio sobre la Ciberdelincuencia (2001), establece las medidas que los países firmantes deben adoptar a nivel nacional, determinando delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (título 1):

- Art 2 Acceso ilícito; establece como delito el acceso intencionado e ilegítimo ya sea este a todo o parte de algún sistema informático
- Art3 Interceptación ilícita: Uso deliberado e ilegitimo en la interceptación de datos informáticos por medios técnicos de datos informáticos en trasmisiones no públicas.
- Art 4 Ataques a la integridad de los datos; acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. Pueden constituirse daños graves.
- Art 5 Ataques a la integridad del sistema; obstaculizando gravemente el funcionamiento de un sistema; siendo el acto deliberado e ilegítimo de un sistema
- Arty 6 Abuso de los dispositivos: vinculados con la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de; cualquier dispositivo, programa informático concebido para algún ilícito precedente.

Delitos informáticos (Título 2):

- Art7, la falsificación informática; generación de datos no auténticos debido a la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos, independientemente de la legibilidad e inteligibilidad de los datos.
- Art 8 Fraude informático; actos ilegítimos y deliberados causantes de prejuicio patrimonial a otro individuo, mediante, la introducción, alteración, borrado o supresión de datos informáticos, además de cualquier interferencia con intención dolosa o delictiva en la obtención ilegítima de un beneficio económico para uno mismo o para otros sujetos usando algún sistema informático.

  Estos artículos constituyen la base para el diseño de la política nacional para combatir los delitos informáticos, permitiendo de este modo la definición estricta de estos delitos.

En el Perú el delito informático fue tipificado en el código procesal de 1991, constituyéndose solo un agravante al delito de hurto. Luego se incluyó y se reguló los delitos informáticos; estableciéndose como el uso e ingreso indebido de datos, sistema o red, alteración, daño o destrucción de base de datos, circunstancias cualificantes graves y tráfico ilegal de datos.

De acuerdo a la Ley de Delitos informáticos en el Perú Ley 30096; identifica los delitos informáticos contra el patrimonio en el capítulo V. El artículo 8 define a fraude informático como el que a través de uso de tecnología de información o comunicación hace uso para sí u otra persona de un aprovechamiento ilícito en perjuicio de terceros ya sea en el diseño, introducción, borrado, alteración, clonación, supresión de datos informáticos o cualquier manipulación o interferencia en la ejecución de un sistema informático, estableciendo la pena privativa de libertad no menor de tres ni mayor de 8 años y con sesenta a ciento veinte días de multa. La modificación a esta ley recae en la Ley 30171, modificando el articulo 8 en el extremo referido a que la pena no privativa de la libertad debe ser no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días de multa cuando

se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

El capítulo VI delitos contra la fe pública en su artículo 9 identifica a la suplantación de identidad, siendo el que mediante el uso de TIC´s suplantan la identidad de una persona ya sea esta natural o jurídica, siempre que se evidencie el daño material o moral, siendo castigado con pena privativa de libertad no menor de tres ni mayor de cinco años.

De acuerdo al informe de análisis N° 04, emitido por la Fiscalía de la Nación en febrero del 2021, menciona los instrumentos internacionales emitidos para la protección de derechos y libertades básicas que podrían verse afectadas por la ciberdelincuencia en sus diversas formas; es por ello que a través de resoluciones aprobadas por la Asamblea General de la Naciones Unidas, los países miembros tienen al alcance las siguientes resoluciones: 56/121 , sobre la lucha contra la utilización de la tecnología de la información con fines delictivos; de fecha 19 de diciembre del 2001. 64/211 sobre la creación de una Cultura Mundial de Seguridad cibernética y Balance de medidas nacionales para la protección de infraestructuras de información esenciales; aprobada el 21 de diciembre de 2009.

La legislación nacional también ha venido siendo actualizada, por ello tenemos la Ley 30999, ley de Ciberdefensa, aprobada el 26 de agosto de 2019. La Ley de Protección de Datos personales de julio de 2011. Ley 28493, ley que regula el uso del correo electrónico comercial no solicitado (SPAM) de abril 2005. Ley 27291, ley que modifica el código civil para permitir la utilización de medios electrónicos para la manifestación de la voluntad y la utilización de la firma electrónica, en junio 2000. Ley 27697, que otorga facultades al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional; de fecha abril 2002, a través de la Ley 300096 del 2013, se modifica agregando los delitos informáticos a la lista de delitos en que los jueces tienen facultad constitucional para tomar conocimiento y controlar las comunicaciones de las personas investigadas ya sea esta preliminar o jurisdiccional.

III. METODOLOGIA

3.1. Tipo y diseño de investigación

La investigación fue de tipo básica, ya que de acuerdo a lo que establece el reglamento RENACYT, este tipo de investigación está dirigida a un conocimiento más completo a través de la comprensión de los aspectos fundamentales de los fenómenos, de los hechos observables o de las relaciones que establecen los entes. (Concytec 2018). Para el caso de la presente investigación se analizaron hechos vinculados a los delitos informáticos y se conoció las percepciones de los especialistas en temas de estos delitos.

El diseño de investigación se enmarca en el enfoque cualitativo por lo que se usó el diseño fenomenológico. Estos diseños se enfocan en las experiencias individuales subjetivas de los participantes (Salgado 2007, p.73).

3.2. Categorías, Subcategorías y matriz de categorización

Herrera, Guevara y Munster (2015) consideran a las categorías como tópicos de investigación que surgen dentro de la investigación o a partir de la formulación de los objetivos generales, considerando a las subcategorías como tópicos que detallan los tópicos de investigación de manera específica, siendo el investigador quien proporciona el significado a las mismas (p. 6).

Al respecto, la presente investigación propuso como categoría de investigación:

- Delitos informáticos: “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas” Hernández (2009)

De esta categoría y alineados con los objetivos de la investigación se plantearon las siguientes subcategorías: Fraude informático y suplantación de identidad. La matriz de categorización apriorística se muestra en **anexo 1**

3.3. Escenario de estudio

Para Hernández y Mendoza (2018) en el proceso cualitativo los escenarios pueden estar delimitados por personas, eventos, sucesos, comunidades, entre otros. siendo en estos espacios donde se llevará a cabo el proceso de aplicación de instrumentos de recolección de datos validados previamente. El escenario de estudio estuvo definido por la jurisdicción del Distrito Judicial de Lima.

3.4. Participantes

La caracterización de los participantes fueron aquellos sujetos que tienen la expertís, conocimiento de informática y de delitos informáticos, siendo estos: 2 jueces, 2 abogados, 2 fiscales, 2 policías especializados en delitos informáticos dentro del distrito judicial de Lima.

3.5. Técnicas e instrumentos de recolección de datos

Se hizo uso de la técnica de la entrevista, para ello la guía de entrevista fue el instrumento de recolección de información, la misma que contenía 12 preguntas pertinentes y alineadas a las subcategorías, categorías y unidad temática de la investigación. Según Canales (2006) como se citó en Díaz et al. (2013), la entrevista es aquella comunicación establecida de manera personalizada entre el investigador y el participante del estudio con la finalidad de dar respuesta a las interrogantes establecidas sobre el problema de investigación. Anexo3: instrumento de recolección de información.

3.6. Procedimiento

Para dar inicio a la investigación se realizó la búsqueda de información previa del tema para plasmarlo en los antecedentes de la investigación, esta información servirá para el diseño de la matriz de categorización apriorística y el desarrollo del marco teórico, posterior a ello se diseñará el marco metodológico incluyendo el diseño del instrumento de recolección de información ; también se diseñará el marco administrativo de la investigación lo permitirá desarrollar de manera ordenada el proyecto. La aplicación del instrumento se realizará teniendo en cuenta la disponibilidad de los participantes, pudiendo ser de manera virtual o presencial. Después de la aplicación del instrumento se procederá a analizar la información a través del método de análisis de contenido lo que implica luego la presentación y discusión de resultados; posteriormente se redactan las conclusiones y recomendaciones de la tesis plasmado en el informe final.

3.7. Rigor científico

Dependencia o consistencia lógica

Según Varela y Vives (2016) la dependencia se manifiesta en el análisis comparativo de diversos estudios y autores con la finalidad de generar resultados lógicos de la investigación. Por lo que la presente investigación buscó cumplir con este rigor ya que se está indagando en estudios previos y normativa vigente en el derecho penal.

La credibilidad

Para Rada (2006) se relaciona a como los resultados del estudio resultan verdaderos a aquellos sujetos que participaron de la investigación o estado en contacto con el fenómeno estudiado. Es por ello que la investigación resguardó y transcribió textualmente la información recolectada de los informantes. Asimismo, solicitó la identificación de los informantes cumpliendo con las capacidades

solicitadas para la presente investigación.

La confirmabilidad

Castillo y Vásquez (2003), consideran necesario un manejo adecuado de los registros de la información, así como la documentación utilizada en todo el proceso de la investigación siendo esta información en su totalidad y adecuada, incluyendo ideas y decisiones del investigador, permitiendo el uso de otros investigadores, pudiendo llegar a similares conclusiones siempre que tengan perspectivas semejantes. Es por ello que la presente investigación consolidó en anexos la transcripción veraz de las entrevistas aplicadas, así como los links de las entrevistas virtuales, si fuera el caso.

Transferibilidad

Castillo y Vásquez (2003), refieren que este criterio considera la probabilidad de que los resultados de un estudio puedan extenderse a otros grupos poblacionales. Por lo que la investigación puede extenderse a otras jurisdicciones judiciales en el país.

El instrumento de recolección de información se validó por el juicio de expertos, para ello se procede a presentar los datos de los expertos en Derecho quienes hicieron la revisión del instrumento

Tabla 1

Validación de Expertos

N°	Apellidos y nombres del experto	Grado Académico	Promedio de valoración
1	Lázaro Ortiz Yanira	Magister	85%
2	Vilela Apón Rolando Javier	Magister	85%
3	Velásquez Saldaña Wilberto	Magister	85%

Nota. Elaboración propia

3.8. Método de análisis de datos

Se utilizó el método de análisis de contenido, toda vez que la investigación es de enfoque cualitativo, este método permitirá la interpretación de los datos recogidos por la entrevista, ya sean estos grabados, filmados, escritos, etc; permitiendo de ese modo la comprensión de fenómenos de la vida social. (López, 2002)

3.9. Aspectos éticos

La investigación respetó el correcto citado de acuerdo a normas APA 7ma edición; así como se realizó el consentimiento informado a los participantes de la investigación, solicitando su autorización en el uso de la información que brindaron. Asimismo, el informe de la investigación fue sometido al software TURNITIN para conocer el índice de similitud, respetando de este modo los porcentajes permitidos por la universidad

Se respetó el código de ética de la universidad en la práctica investigativa.

IV. RESULTADOS Y DISCUSIÓN

Resultados:

El presente capítulo contiene los resultados obtenidos de la aplicación del instrumento de recolección de la información, la guía de entrevista; para ello se presentan el análisis de los resultados teniendo en cuenta los objetivos de la investigación.

Respecto al objetivo general: Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública, en el Distrito Judicial de Lima, 2022. Desde la opinión de los miembros de la policía nacional del Perú, el tratamiento jurídico penal de los delitos contra el patrimonio y la fe pública en el Distrito judicial de Lima, inicia con el acopio de la evidencia del delito para luego ser elevado al ministerio público a través de la fiscalía especializada en delitos informáticos; coinciden que el tratamiento de estos delitos tiene peculiaridades que van desde la obtención de evidencias digitales las cuales son difíciles de conseguir; la PNP especializada en delitos informáticos tiene la responsabilidad de, en el menor tiempo, pueda aportar evidencias digitales concretas que ayude a la construcción de un caso bien fundamentado en esta etapa investigativa. Algunas de estas evidencias son actas de visualización y análisis forense. Cabe resaltar que la mayor incidencia son los delitos contra el patrimonio, principalmente fraude informático, pornografía infantil y seducción a menores.

El código procesal penal, determina que para el levantamiento del secreto de comunicaciones debe existir primero una orden del juez, de lo contrario esto no estaría en el marco legal. Esta situación procesal dificulta el trabajo de la policía especializada en estos delitos, toda vez que sin esa información no podría ser posible construir el caso. Esta peculiaridad en el tratamiento de estos delitos se aprecia en el anonimato de los autores del delito, así como la posibilidad que esté en cualquier parte del país perpetrando el ataque. Es por ello que los policías entrevistados coinciden en que para el proceso de investigación

policial deben contar con acceso a información tanto pública como privada de manera oportuna.

"Lo que se ve ahora con mayor incidencia son los delitos contra el patrimonio lo que es fraude informático, así mismo, pornografía infantil mucho caso de seducción a menores. Lo que es el tratamiento legal se reúne la evidencia y se eleva al ministerio público para su tratamiento, pero existen ciertas dificultades de este tipo de casos que manejamos, la información la evidencia digital es un poco complicada para conseguir y montar buen caso (…). En ese trayecto lo que hacemos nosotros es reunir la cantidad de evidencias con actas de visualización y analisis forenses y poder reunir evidencias que requiere la fiscalía para sus casos" *Sub oficial de primera Hegel Covarrubias Maihua. Departamento de patrullaje virtual de la* DIVINDAT

"Nosotros lo que hacemos , en la premura , necesitamos acceso a la información, que tienen los bancos, entidades públicas, privadas, que normalmente exige el código procesal penal que un juez autorice el levantamiento del secreto de comunicaciones o levantamiento de ciertas medidas de derecho , pero esa información es importante es indispensable para construir el caso y poder reunir mayor información, recuerda que ese tipo de casos tiene varias dificultades por ejemplo el anonimato del actor, la distancia, la persona puede estar en cualquier parte del país y ejecutar el ataque (…)" *Sub oficial de primera Hegel Covarrubias Maihua. Departamento de patrullaje virtual de la* DIVINDAT

"Al recibir la denuncia por algún delito informático ya sea de fraude o suplantación de identidad intentamos por todos los medios legales agilizar el proceso de investigación que permita la formalización de la denuncia; en algunos casos las evidencias digitales no están al alcance debiendo hasta pedir al denunciante que haga las gestiones ante su banco para solicitar más pruebas; esta lentitud en el proceso de intercomunicación entre nosotros como policía nacional y la banca a veces no es rápida *(…)" Oficial de primera Marco Antonio Pahuacho Cajahuaman – Investigador de la DEPINCRI Villa María del Triunfo*

Los fiscales por su parte coinciden en catalogar como ley especial y específica a la ley de delitos informáticos; pero resaltan que, a pesar de ello, el tratamiento jurídico penal de estos delitos no se da de manera idónea, lo cual se debe, principalmente a las limitadas herramientas tecnológicas al alcance de los magistrados para desarrollar una efectiva indagación del proceso; otro motivo también recae en las escasas dependencias especializadas en estos delitos. Asimismo, consideran que se debe prever otros tipos penales contra el patrimonio ya que por la actualización de la tecnología surgen en corto tiempo nuevas modalidades, impidiendo de ese modo el tratamiento jurídico penal.

Consideran que la investigación de este tipo de delitos debe actuar con celeridad y oportunidad debido a lo cambiante y complejo de las evidencias digitales, puesto que si se siguen criterios de investigación como los delitos comunes es muy probable que no se alcance la verdad sobre el hecho delictivo; resaltan también la necesidad de fortalecer las unidades especiales encargadas de combatir estos delitos contando para ello con profesionales altamente capacitados tanto en la policía, fiscalía como judicial.

Respecto a que si los delitos informáticos contra la fe pública se dan en el momento que aparece el dolo; sostienen que a pesar que el tipo penal en estudio, amerita haber causado daño económico o moral, el daño moral es muy amplio y poco objetivo de acuerdo a los contextos socio culturales; es por ello que consideran necesario para este tipo de delitos la intención de ocasionar daño a terceros, desde los actos preparatorios antes de cometer el delito usando la tecnología para el accionar.

> “Los delitos informáticos, tienen la característica de ser delitos especiales y se encuentran sancionadas con una ley especial, el tratamiento jurídico penal en lo referente a dichos delitos no se viene realizando de manera idónea por falta de una plataforma especial y del apoyo tecnológico que ello conlleva, siendo escasas las dependencias especializadas en los referidos delitos” *Jerson Josip Campó Díaz- Fiscal Adjunto Provincial de VMT.*

"Se debería desde un principio al tomar conocimiento de estos delitos realizar una investigación célere puesto que en este tipo de delitos la evidencia digital es esencial para la obtención de resultados siendo la misma muy volátil en su permanencia en el tiempo, siendo así si se aplica un método de investigación a los delitos comunes o antiguos, es factible que muchas veces no se alcance la verdad sobre el hecho delictivo". *Wilfredo Vegas López- Fiscal adjunto Provincial Penal Corporativa de Villa María del Triunfo*

"Los delitos informáticos muchas veces son confundidos con los delitos de hurto agravado, estafa y apropiación ilícita, sin embargo debe tenerse presente que los delitos informáticos son delitos especiales y cada tipo penal está descrito en la ley, el uso de las herramientas tecnológicas en evolución permiten la creación de nuevas formas delictivas y nuevos tipos penales, el dolo como conocimiento y voluntad se manifiesta desde antes de cometerse el delito, existen actos preparatorios y es justamente el uso de las tecnologías acompañadas de la conducta ilícita para suplantar, engañar o defraudar para conseguir el resultado final". *Jerson Josip Campó Díaz- Fiscal Adjunto Provincial de VMT.*

Desde la perspectiva de los abogados litigantes reconocen la ambigüedad del tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública, esto conlleva a sentencias no efectivas e injustas. A su vez, indicaron que la normativa nacional respecto a estos delitos debe ser más específica en lo referido a la tipología de estos delitos informáticos y estar en constante actualización; estas mejoras permitirían a los jueces un juzgamiento que garantice el debido proceso. Manifestaron que el dolo si se da en el momento que se cometen los delitos informáticos puesto que existe la intención de realizar el hecho delictivo.

"Podremos afirmar, que en la actualidad el tratamiento jurídico penal de los delitos informáticos contra el patrimonio no es tan efectivo, puesto que el ordenamiento jurídico es muy ambiguo al momento de calidad cada tipo de delitos informáticos contra el patrimonio y la fe pública, siendo así al momento de juzgar no puede obtenerse sentencias efectivas y justas". *José Luis Oré Huamani. CAL 76187*

"La Ley de delitos informáticos debe permitir la inclusión de tipologías de delitos de manera continua toda vez que con los procesos de innovación tecnológica tan constantes estos delitos van adaptándose y los perpetradores se aprovechan de la lentitud y vacíos legales para sus actos delictivos". Abogado. *Carlos Alberto Burgos Cuellar. CAL 600036*

Desde la opinión de los jueces entrevistados, afirman que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial Lima, como en todo el territorio peruano, se aplica en base a lo dispuesto en la Ley 30096 y su reglamento. A pesar de existir esta ley es necesario la creación de una dirección especial más fortalecida en la investigación de delitos informáticos puesto que han quedado impunes algunas conductas debido a la investigación deficiente, que involucra a todos los actores que deberían tener conocimiento más técnico de temas informáticos. También afirman que si no existe el dolo para comisión de delitos informáticos entonces no se configuraría el delito informático, lo importante es identificar rápidamente el daño y evidenciarlo.

"Debería crear, el Estado, una dirección especial en la investigación de delitos informáticos, ya que muchas veces se han quedado algunas conductas impunes por la deficiencias en la investigación" *Luis Alberto Dejo Apaestegui. - Juez de la Corte Superior de Justicia de Lima Norte*

"Sería incoherente negar la aplicación de la Ley 30096, creo que debería analizarse por la rapidez del proceso investigativo y los medios probatorios contundentes que deben exponer*" Luis Alberto Dejo Apaestegui. - Juez de la Corte Superior de Justicia de Lima Norte*

"El tipo penal de suplantación de identidad, necesariamente necesitan del dolo para poder ser considerado como delito" *Pedro Wilbert Rojas Arteaga- Juez Corte Superior de Justicia de Lima Norte*

Respecto al objetivo específico: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021. Los resultados obtenidos desde la opinión de los miembros de la Policía

Nacional del Perú reconocen que los avances tecnológicos se relacionan estrechamente con la comisión de delitos informáticos y las nuevas formas de engañar al usuario, resaltan el hecho de que como policías especializados en estos delitos deben estar en constante actualización que les permita estar un paso adelante a los hechos delictivos.

También expresaron que a pesar de que en la ley de delitos informáticos se cumple con el principio de tipicidad para sancionar el fraude informático; la necesidad de que las penas sean más altas ya que la legislación vigente permite que las sentencias sean menores a 4 años de cárcel, lo que conlleva a que no sea efectiva. También mencionaron que, a pesar de existir una fiscalía especializada en estos delitos, los jueces no tienen el conocimiento necesario respecto a informática lo que resulta minimizar la gravedad de los actos.

La pandemia por Covid 19, ha permitido que las transacciones económicas virtuales crezcan de manera exponencial, de esta manera los usuarios han sido víctimas de fraude informático, así como de estafas en compras por plataformas de comercio electrónico.

" (…) hace más de 5 años puede ser 10 años será en el cual era el principal motivo o técnica para hacer fraude informático era la clonación de tarjetas luego apareció los chips en las tarjetas con lo cual la clonación dejó de existir, porque los chip no son clonables. Antes lo que se hacía era leer la banda magnética y transferirlo a una tarjeta en blanco y con esa tarjeta efectuar los retiros, actualmente ya no se da la clonación. Ya que la seguridad fue aumentada con el chip. Pero la tecnología va avanzando y ahora hay nuevas maneras de engañar al usuario como las billeteras móviles como yape plin, luquita, vin , donde las personas crea con su chip, su número de teléfono las cuentas y por medio de una técnica llamada sign wapping, el atacante bloquea la línea y crea un chip con el nombre de la persona y procede con la validación de datos para extraer el dinero. Entonces la tecnología avanza y de igual forma los criminales ven la forma de vulnerar la seguridad que existe y romper esas barreras y obtener el

acceso que le permita obtener el dinero de manera ilícita, nosotros como policías debemos estar un paso adelante para poder neutralizarla" *Sub oficial de primera Hegel Covarrubias Maihua. Departamento de patrullaje virtual de la* DIVINDAT

"La pandemia ha sido una oportunidad para que el uso de tecnología aumente, ya que no hubo entidad bancaria abiertas, las personas tuvieron que usar obligatoriamente la tecnología, se masificó, transferencias bancarias aumentaron. La delincuencia también vio una oportunidad de tener mayor cantidad de víctimas en las compras por internet en linea, se dio bastante el fraude informático asi como estafas por compras en plataformas de comercio. La pandemia en el 2020 y 2021 aumentó. Las personas siguen usando las transacciones por internet" *Oficial de primera Marco Antonio Pahuacho Cajahuaman – Investigador de la DEPINCRI Villa María del Triunfo*

Desde la percepción de los fiscales, existe una relación estrecha entre los avances tecnológicos y la comisión de delitos, ya que se van creando nuevos métodos delictivos y esto conlleva a que también existan tipos penales los cuales tienen características peculiares que no necesariamente sea dado en la misma ubicación geográfica donde se encuentra la víctima. La ley referida a delitos informáticos resulta confusa a aquellos operadores de justicia que no distinguen con claridad el fraude informático con el hurto de dinero, por lo que expone una limitada capacidad técnica en estos temas perjudicando a la víctima y desvirtuando el espíritu de la ley la misma que si cumple con el principio de tipicidad toda vez que si se precisa la conducta, el supuesto de hecho y la consecuencia jurídica. También identificaron que las estrategias para la prevención y sanción de delitos de fraude informático no son claras ni contundentes.

También afirman que la pandemia produjo dependencia en las personas al uso de aparatos electrónicos extendiéndose a transacciones financieras; este escenario también es observado por los

delincuentes que se adaptan rápidamente a estas nuevas tecnologías e identifican los puntos vulnerables.

"Si bien es cierto existe una ley específica para los delitos informáticos, la misma resulta confusa en la medida que no se desarrollen unidades especializadas en esos delitos, toda vez que los operadores de justicia no distinguen muchas veces de un fraude informático con el hurto de dinero". *Jerson Josip Campó Díaz- Fiscal Adjunto Provincial de VMT.*

"El espíritu de la ley si cumple con el principio de tipicidad para los delitos informáticos, ya que está descrita la conducta, el supuesto de hecho y la consecuencia jurídica". *Wilfredo Vegas López- Fiscal adjunto Provincial Penal Corporativa de Villa María del Triunfo*

"Definitivamente la virtualidad produce que las personas dependan de un aparato tecnológico para poder realizar múltiples tareas, desde realizar pagos, hasta recibir salarios, en ese entendido la delincuencia se adapta a ese tipo de tecnologías de manera rápida". *Jerson Josip Campó Díaz- Fiscal Adjunto Provincial de VMT.*

Los abogados penalistas coinciden que los delitos informáticos seguirán en aumento acelerado, constituyendo un reto a nuestro sistema jurídico para que se defina bien los delitos y las tenga de manera expresa. Existe discrepancia en la opinión de los entrevistados ya que para uno de ellos la ley de delitos informáticos no cumple con el principio de tipicidad para sancionar el fraude informático ya que muchas de estas denuncias terminan archivándose debido a que no existe una correspondencia entre lo que el agente ha realizado y aquello que se encuentra descrito en ley. La ambigüedad de la ley de delitos informáticos impide el éxito de los procesos judiciales.

"NO, puesto que como hemos podido conocer, muchos de estos procesos terminan archivándose. Por el simple hecho que no existe una correspondencia exacta entre lo que el agente ha realizado y aquello que se encuentra descrito en la ley". "Dada la experiencia laboral como operador de justicia, he podido advertir

ciertas estrategias de manera incipiente, más no claras ni contundentes” .Abogado. *Carlos Alberto Burgos Cuellar. CAL 600036*

“Se podría decir que, si existe el principio de tipicidad para sancionar este tipo de delito, pero esto se ve afectado cuando los delitos informáticos cambian de proceder lo cual genera un vació al momento de la aplicación de la ley” *José Luis Oré Huamani- ABOGADO - Cal 76187*

Desde la opinión de los jueces, los avances tecnológicos apoyan la investigación de delitos en general, pero el tipo delictivo informático requiere un manejo más avanzado de estas tecnologías y de ese modo realizar efectivamente la investigación; asimismo reconocen que las penas aplicadas por estos delitos son muy benignas sin tomar en cuenta el daño patrimonial a la víctima. Respecto a la tipicidad para sancionar el fraude informático en la ley de delitos informáticos está dado porque si regula las conductas sobre estos delitos, eso no es lo mismo decir que sean efectivas. Las estrategias de prevención y sanción de delitos informáticos por parte del Estado no son claras y solo usan las recomendaciones dadas por otras instituciones expertas en la materia. También se precisa que la pandemia por el Covid 19 ha aumentado las denuncias por delitos informáticos.

“La tecnología de alguna forma va apoyar a la investigación de delitos en general, pero esta clase de delitos informáticos si requiere bastante apoyo para poder realizar una investigación idónea y clara y de esta forma contrarrestar el avance delictivo” *Luis Alberto Dejo Apaestegui. - Juez de la Corte Superior de Justicia de Lima Norte*

“ Si bien es cierto que la tecnología siempre avanzar, más aún al encontrarnos en pandemia, estos delitos aumentaron y trajeron nuevas forma de cometerlos los cuales ayudaron a generar ambientes propicios para la comisión de estos delitos, al ser en su mayoría declarados impunes.” *Pedro Wilbert Rojas Arteaga- Juez Corte Superior de Justicia de Lima Norte*

“ A pesar de la existencia de la Ley y su reglamento en la cual se precisan las tipologías de los delitos enmarcados, es muy poco eficaz la sanción ya que se evidencia en algunos casos que no se logra probar el delito por la lentitud o

desconocimiento de ellos.” *Luis Alberto Dejo Apaestegui. - Juez de la Corte Superior de Justicia de Lima Norte*

Los resultados referidos al objetivo específico 2: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021. La percepción de los entrevistados coincide que la suplantación de identidad no recibe un adecuado tratamiento debido a las pocas unidades tecnológicas avocadas a este tipo de delitos, careciendo muchas veces de herramientas tecnológicas necesarias para individualizar al sujeto activo de delito. Precisan también que la ley para poder ser aplicada y alcanzar el objetivo por la que fue creada debe en la práctica tener un adecuado manejo sumado a ello a que el capital humano sea lo suficientemente capacitado para afrontar de manera eficaz el delito.

“Efectivamente, la limitación vendrá desde el operador de justicia que tenga el adecuado adiestramiento para afrontar la investigación de los delitos informáticos, lo cual conlleva toda una especialización que lamentablemente no es universal”. *Jerson Josip Campó Díaz- Fiscal Adjunto Provincial de VMT.*

“Si, puesto que las fiscalizas especializadas que se han formado para ver este tipo de delitos, no reciben las capaciones necesarias para poder ejercer bien la defensa de los agraviados”. *José Luis Oré Huamani- Abogado - Cal 76187*

“ (…) ya que al no tener las herramientas adecuadas se va a realizar una investigación deficiente(…) La suplantación de identidad digital es uno de los delitos informáticos mas habituales (…) dicha conducta se encuentra regulado en el articulo 401 del código Penal, con una pena de seis meses a tres años.” *Luis Alberto Dejo Apaestegui. - Juez de la Corte Superior de Justicia de Lima Norte*

“Si es una limitante, puesto que si se contara con personal calificado ayudaría realizar mejores investigaciones criminales en torno a estos delitos, lo cual facilitan en gran forma los procesos judiciales” *Pedro Wilbert Rojas Arteaga- Juez Corte Superior de Justicia de Lima Norte*

Discusión:

Respecto al objetivo general; se analiza que el tratamiento jurídico penal de los delitos contra el patrimonio y la fe pública en el Distrito judicial de Lima requiere fortalecer los órganos especializados en este tipo de delitos toda vez que estos tienen peculiaridades en su tratamiento, este fortalecimiento debe estar orientado a la mejora en accesos tecnológicos y capacitación especializada a los actores de justicia. Situación que también afronta Arabia Saudí en los esfuerzos para implementar medidas usando medios tecnológicos y controles en el procedimiento. Alanezi, (2016). En el distrito judicial de Lima se resalta que las mayores incidencias de estos delitos están orientados a fraude informático, pornografía infantil y seducción a menores, estos resultados se apoyan en lo mencionado por Bokovnya, et al. (2020) quienes afirman que en el contexto de la pandemia los países en el mundo han sufrido una tendencia de ciberataques masivos que van desde phishing, propagación de malware, hackeos, juegos en línea, mayor demanda y distribución de material pornográfico a través de redes sociales; lo que evidencia que el Perú no es la excepción.

El tratamiento jurídico penal de los delitos contra el patrimonio y la fe pública son ambiguos lo que conlleva a sentencias no efectivas e injustas; para ello se debe mejorar la normativa nacional siendo más específica en la tipología de estos delitos y las penas establecidas. Así lo sostiene Mayer (2017) en un Estado democrático la funcionalidad informática es un presupuesto para la operatividad en diversos ámbitos y actividades relevantes de personas e instituciones; por lo que al reconocerlo como bien jurídico instrumental de carácter colectivo, la tutela penal debe ser verificada en términos particulares.

Respecto al análisis del tratamiento jurídico penal del fraude informático, se conoce que los delitos informáticos seguirán aumentando en relación a la generación de tecnología, por lo que es un reto al sistema jurídico; que debe generar estrategias claras de prevención y sanción dirigidas a la población.

Respecto al análisis del tratamiento jurídico penal del delito de suplantación de identidad, se conoce que este delito no recibe un adecuado tratamiento debido a la poca capacidad técnica y profesional en este tipo de delito. Estos resultados coinciden con lo establecido por Borghello y Temperini (2012) una de las raíces de este delito es la facilidad de captación ilegítima de datos de identificación personal, asi como la carente legislación en la materia, limitadas acciones de control en las entidades y los escasos niveles de educación en usuarios de internet.

V. CONCLUSIONES

Después del análisis del tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el distrito Judicial de Lima se concluye que, a pesar de la existencia de una norma legal establecida para el tratamiento jurídico penal de estos delitos, aún existe ambigüedad en la tipología y penas muy leves, lo que conlleva sentencias no efectivas e injustas.

Se concluye que el tratamiento jurídico penal del fraude informático debe tener un marco legal que permita actualizar constantemente las diversas modalidades de este delito ya que, por el constante cambio de la tecnología, los hechos delictivos también irán cambiando en las modalidades de ataque. Por ello es necesario que los operadores de justicia desarrollen capacidades en informática que les permita un manejo efectivo.

Respecto al análisis del tratamiento jurídico penal del delito de suplantación de identidad en el Distrito judicial de Lima, se concluye que este delito carece de un tratamiento adecuado debido a la poca capacidad técnica y profesional en este tipo de delito; sumado a las estrategias poco claras por parte de instituciones del Estado para prevenir este tipo de delitos.

VI. RECOMENDACIONES

Se recomienda a los diversos operadores de justicia proponer la modificación de la ley de delitos informáticos, basado desde la experiencia en los hechos delictivos atendidos y la jurisprudencia internacional debido a los contextos cambiantes de la sociedad.

Se sugiere priorizar en el plan anual de capacitaciones de la División de Delitos Informáticos de la Policía Nacional del Perú, de la Fiscalía Especializada en delitos informáticos y Corte Superior de Justicia; temática relacionada al uso de herramientas informáticas que permitan anticiparse y establecer mejor los criterios de juzgamiento ante estos delitos.

Se recomienda la articulación pública- privada para desarrollar campañas de sensibilización constante sobre la prevención de este tipo de delitos, difundiéndolas a través de las redes sociales.

REFERENCIAS

Aguila, E. (2019). *Suplantación de la identidad digital con fines de trata de personas en Facebook.* Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. *[*Propuesta de intervención para obtener el grado de maestro en Derecho de las tecnologías de la información y comunicación]

Azaola, L. (2010). *Delitos informáticos y Derecho Penal*. Editorial UBIJUS. Primera Edición.

Alanezi, F. (2016). Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions. [Tesis para obtener el grado de Doctor en Filosofía de la Universidad de Brunel]
http://bura.brunel.ac.uk/handle/2438/12003

BID-OEA. (2020). Reporte C*iberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe*

Bokovnya, A., Khisamova, Z., Begishev, I., Latypova, E., & Nechaeva, E. (2020). *Computer crimes on the COVID-19 scene: Analysis of social, legal, and criminal threats. Cuestiones Políticas, 38*(66 Especial)

Borghello, C. & Temperini, A. (2012). *Suplantación de Identidad Digital como delito informático en Argentina.* Simposio Argentino de Informática y Derecho. Universidad Nacional de la Plata. 41 JAIIO - SID 2012 - ISSN: 1850-2814 - Página 78-93

Castillo, E. & Vásquez, M. (2003). *El rigor metodológico en la investigación cualitativa.* Colombia Médica, 34 (3),164-167.[fecha de Consulta 20 de Enero de 2022]. ISSN: 0120-8322. https://www.redalyc.org/articulo.oa?id=28334309

Cherniavskyi, S., Babanina, V., Mykytchyk, O., & Mostepaniuk, L. (2021). Measures to combat cybercrime: analysis of international and Ukrainian experience. *Cuestiones Políticas*, *39*(69), 115–132.
https://doi.org/10.46398/cuestpol.3969.06

Cortés, R., Ballén, J. & Duque, J. (2015). *La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio.* Rev. derecho comun. nuevas tecnol.No. 14 http://dx.doi.org/10.15425/redecom.14.2015.05

Díaz, L., Torruco, U., Martínez, M., & Varela, M. (2013). *La entrevista, recurso flexible y dinámico. Investigación en educación médica,* 2(7), 162-167. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572013000300009&lng=es&tlng=es.

FEM (Foro Económico Mundial). (2020). *The Global Risks Report 2020*. Consultado el 11de setiembre de 2021 en https://www.weforum.org/reports/the-

global-risks-report-2020.

Fernández, W; Vargas, C. (2018) *¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías.* **The Law, State and Telecommunications Review**, Brasilia, v. 10, n. 2, p. 37-52, October 2018. [DOI: https://doi.org/10.26512/lstr.v10i2.21492]

Fiscalía de la Nación (2021) informe de análisis n°04. Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada.

Hance, O. (1996). *Leyes y Negocios en internet.* Mcgraw-HILL

Hernández, L. (2009), *El delito informático*. Eguzkilore. Cuaderno del Instituto Vasco de Criminología. nº 23. pp. 227- 243.

Hernández, R. & Mendoza, C (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta, Ciudad de México, México: Editorial Mc Graw Hill Education, ISBN: 978-1-4562-6096-5, 714 p.

Herrera, J., Guevara, G. & Munster , H. (2015). Los diseños y estrategias para los estudios cualitativos. Un acercamiento teórico-metodológico. *Gaceta Médica Espirituana*, *17*(2), 120-134. Recuperado en 22 de enero de 2022, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1608-89212015000200013&lng=es&tlng=es.

IBM Security (2020), *IBM X-Force Threat Intelligence Index*, IBM, Armonk, USA. https://www.ibm.com/security/data-breach/threat-intelligence.

Levin, A., & Ilkina, D. (2013). Comparación internacional del crimen cibernético. Toronto: Ryerson University

López, F. (2002) *El análisis de contenido como método de investigación.* Revista de Educación, 4 (2002): 167-179. Universidad de Huelva

López, J. (2004), *Derecho penal. Parte general: Introducción a la teoría jurídica del delito*, cit., T. I, pp. 51-52.

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. *Revista chilena de derecho*, *44*(1), 261-285. https://dx.doi.org/10.4067/S0718-34372017000100011

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis* , *24* (1), 159-206. https://dx.doi.org/10.4067/S0718-00122018000100159

Mori, J. (2019) Los Delitos Informáticos y La Protección Penal de la intimidad en el Distrito Judicial De Lima, Periodo 2008 al 2012. [Tesis para optar el grado académico de Maestro en Derecho de la Universidad Nacional Federico Villarreal]

Pardo, A. (2018) *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 de la Universidad César Vallejo]

Plascencia, R. (1998) *Teoría del delito* . UNAM, Instituto de Investigaciones Jurídicas

Peña, O. & Almanza, F. (2010) *Teoría del Delito. Manual práctico para su aplicación en la teoría del caso*

Piña, L. (2014). *Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano.* [Consulta 19 enero 2022]. http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

Pons, V. (2017). *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad*. URVIO. Revista Latinoamericana De Estudios De Seguridad, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Ramirez, E. & Aguilera, A. (2009) *Los delitos informáticos. Tratamiento internacional*. en Contribuciones a las Ciencias Sociales. www.eumed.net/rev/cccss/04/rbar2.htm

Rada, D. (2006). *Credibilidad, Transferibilidad y Confirmabilidad en Investigación Cualitativa*. Revista IPASME, Vol. Mayo 2006. MED-IPASME

Temperini, M. (2014) *Delitos informáticos en Latinoamérica: un estudio de derecho comparado.* 2da parte. Sociedad Argentina de Informática e Investigación Operativa. http://sedici.unlp.edu.ar/handle/10915/42145

Varela, M y Vives, T. (2016). *Autenticidad y calidad en la investigación educativa cualitativa: multivocalidad* Investigación en Educación Médica, 5(19), 191-198. https://www.redalyc.org/pdf/3497/349746529008.pdf

Velásquez, O. & Garrido, Y. El ciberilícito en Colombia: ¿ante cuál juez acudir?, 132 Vniversitas, 515-560 (2016). http://dx.doi.org/10.11144/Javeriana.vj132.ccac

Villavicencio, F. (2014). Delitos informáticos. Revista IUS ET VERITAS, N° 49, diciembre 2014 / ISSN 19

Zambrano, A. (2020) *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020.* [tesis para optar el título profesional de abogado de la Universidad César Vallejo]

ANEXOS

ANEXO 1: Matriz de Categorización Apriorística

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública, en el Distrito Judicial de Lima, 2022

Categoría	Definición Conceptual	subcategorías	Técnicas e instrumentos de recolección de datos
Delitos informáticos	"toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas" **Hernández (2009)**	**Fraude informático** **Suplantación de identidad**	**Técnica:** Entrevista Análisis documental **Instrumento:** Guía de entrevista

ANEXO 2: Matriz de consistencia

PROBLEMA DE LAINVESTIGACION	OBJETIVOS	CATEGORIA	SUBCATEGORIAS	INSTRUMENTO
Problema general: ¿De qué manera se da el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima 2022? **Problemas específicos:** a) ¿De qué manera se da el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2022? b) ¿De qué manera se da el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2022?	**Objetivo general:** Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2022 **Objetivos específicos**: a) Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2022 b) Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2022	DELITOS INFORMÁTICOS	FRAUDE INFORMÁTICO SUPLANTACIÓN DE IDENTIDAD	ENTREVISTA: 1.- ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? 2.- ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? 3.- ¿Considera usted que la ley de delitos informáticos cumple con el principio de titpicidad para sancionar el fraude informático? 4.- Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? 5.- ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? 6.- ¿Considera que la pandemia a permitido la práctica delictiva informática? ¿De qué manera? 7.- ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? 8.- ¿Considera que la legislación vigente… 9.- ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad?

ANEXO 3

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Buen día, estoy realizando un trabajo de investigación el cual será útil para elaborar una tesis profesional sobre el Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2021, Es por ello que agradecería responder con la mayor sinceridad

¿Desea participar y otorgar su consentimiento para hacer uso de los datos en la presente investigación? Favor marque con un aspa su respuesta:	SI	NO

Entrevistado/a: …….
Cargo/profesión/grado académico: ……
Normas básicas de la entrevista: ……

Objetivo general: Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2022
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? --- --- --- ---
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? --- --- --- ---
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? --- --- ---

Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? …… ……
5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? …… …… ……
6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? …… ……
7. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? …… …… ……
8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? …… …… ……
9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? …… ……
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? …… ……
11. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? …… ……
12. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? …… ……

Anexo 04
Validación de instrumento

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN
INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

I. DATOS GENERALES:

1.1. **Título de investigación:** TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO Y LA FE PÚBLICA EN EL DISTRITO JUDICIAL LIMA, 2021
1.2. **Apellidos y nombres:** Mg Yanira Guiselia Lázaro Ortiz.
1.3. **Cargo e institución donde labora:** Docente de la UCV
1.4. **Nombre del instrumento motivo de evaluación:** Guía de Entrevista
1.5. **Autor del instrumento:** Bach. Zakir Temir Lujan Coorahua

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			Σ
		40	45	50	55	60	65	70	76	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.										X			
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										X			
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.										X			
4. ORGANIZACIÓN	Existe una organización lógica.										X			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										X			
6. INTENCIONALIDAD	Esta adecuado para valorar o medir las variables.										X			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										X			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, e hipótesis										X			
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar las hipótesis.										X			
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										X			

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los requisitos para su aplicación.
- El Instrumento no cumple con los requisitos para su aplicación

PROMEDIO DE VALORACIÓN

SI

...85 %

Lima, 27 de enero del 2022

Firma del experto
DNI N° 45189824 Cel. 986 593 151

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN
INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

I. DATOS GENERALES:

1.1. **Título de investigación:** TRATAMIENTO JURÍDICO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO Y LA FE PÚBLICA EN EL DISTRITO JUDICIAL LIMA, 2021

1.2. **Apellidos y nombres:** Mgtr. Rolando Javier Vilela Apón

1.3. **Cargo e institución donde labora:** Docente de la UCV

1.4. **Nombre del instrumento motivo de evaluación:** Guía de Entrevista

1.5. **Autor del instrumento:** Bach. Zakir Temir Lujan Ccorahua

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			Σ
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.										X			
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										X			
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.										X			
4. ORGANIZACIÓN	Existe una organización lógica.										X			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										X			
6. INTENCIONALIDAD	Esta adecuado para valorar o medir las variables.										X			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										X			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, e hipótesis										X			
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar las hipótesis.										X			
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										X			

III. OPINIÓN DE APLICABILIDAD

- El instrumento cumple con los requisitos para su aplicación.
- El instrumento no cumple con los requisitos para su aplicación

	SI

PROMEDIO DE VALORACIÓN ...85 %

Lima, 29 de enero del 2022

Firma del experto
DNI N°42301468 Cel. 947119375

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN
INFORME DE OPINIÓN DEL JUICIO DE EXPERTOS

I. DATOS GENERALES

1.1 **Título de la investigación:** Tratamiento Jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima 2022

1.2 **Apellidos y Nombres:** Mgtr. VELÁSQUEZ SALDAÑA WILBERTO

1.3 **Cargo e institución donde labora:** Abogado- GERENTE GENERAL DE COMPAÑÍA TRUJILLO SALEM- SAC.

1.4 **Nombre del instrumento motivo de evaluación:** Guía de entrevista

1.4 Autor de instrumento: Bach. Luján Ccorahua Zakir Temir

II. ASPECTOS DE VALIDACION

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.										X			
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										X			
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.										X			
4. ORGANIZACIÓN	Existe una organización lógica.										X			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										X			
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.										X			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										X			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos										X			
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.										X			
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										X			

III. OPINIÓN DE APLICABILIDAD (SI/NO)

- El Instrumento cumple con los requisitos para su aplicación — SI
- El Instrumento no cumple con los requisitos para su aplicación —

IV. PROMEDIO DE VALORACIÓN — 85%

Lima, 20 de marzo del 2022

FIRMA DEL EXPERTO
DNI: 17890108
TELF: 990315300

ANEXO 05

CONSENTIMIENTO INFORMADO

Estimado participante:

LUIS ALBERTO DEJO APAESTEGUI

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima, 01 de abril del 2022

CONSENTIMIENTO INFORMADO

Estimado participante:

PEDRO WILBERT ROJAS ARTEAGA
JUEZ CORTE SUPERIOR LIMA NORTE.

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima, 19 de abril del 2022

CONSENTIMIENTO INFORMADO

Estimado participante:
CARLOS ALBERTO BURGOS CUELLAR
ABOGADO- CAL 600036

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima, 12 de abril del 2022

.....

CONSENTIMIENTO INFORMADO

Estimado participante:

José Luis Oré Huamani
ABOGADO - Cal 76187

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima,11 de abril del 2022

CONSENTIMIENTO INFORMADO

Estimado participante:

HEGEL COVARRUBIAS MAIHUA
Sub oficial de primera
CIP: 31542918
Departamento de patrullaje virtual – DIVINDAT PNP

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento juridico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima,07 de abril del 2022

.....

SA-31542918
Hegel COVARRUBIAS MAIHUA
S1 PNP

CONSENTIMIENTO INFORMADO

Estimado participante:

Marco Antonio PAHUACHO CAJAHUAMAN
Sub oficial de primera
CIP 31425298
INVESTIGADOR – DEPARTAMENTO DE INVESTIGACION CRIMINAL VILLA MARIA DEL TRIUNFO – POLICIA NACIONAL DEL PERU.

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima, 16 de abril del 2022

31425298
MARCO ANTONIO PAHUACHO CAJAHUAMAN
SI PNP

CONSENTIMIENTO INFORMADO

Estimado participante:

Jerson Josip Campó Díaz, Fiscal Adjunto Provincial de VMT

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima, 12 de abril del 2022

Jerson Josip Campo Díaz
Fiscal Adjunto Provincial (P)
Segunda Fiscalía Provincial Penal
QS Villa María del Triunfo

CONSENTIMIENTO INFORMADO

Estimado participante:
Wilfredo Vegas López
Fiscal adjunto Provincial Penal Cuarto Despacho de la Fiscalía Provincial Penal Corporativa de Villa María del Triunfo.

El Bachiller Zakir Temir LUJAN CCORAHUA, viene realizando la siguiente investigación titulada:

"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021".

Por medio de la presente se hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando en las entrevistas diseñadas para el cumplimiento de los objetivos trazados, los datos e información serán utilizados estrictamente para los fines académicos y del estudio mencionado, así mismo se respetará en todo momento la confidencialidad y en especial su identificación.

La información que usted brinde será de gran ayuda porque sus respuestas nos ayudaran a generar información relevante para analizar y comprender el problema planteado.

Por lo expresado, el participante antes mencionado acepta la voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando en señal de conformidad.

Lima,07 de abril del 2022

ANEXO 06
Transcripción de entrevistas

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: LUIS ALBERTO DEJO APAESTEGUI.
Cargo/profesión/grado académico: Institución: Juez de la Corte Superior de Justicia de Lima Norte
Normas básicas de la entrevista: Agradecería manifestar su consentimiento para el uso de la información brindada.

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Se aplica en base a lo dispuesto en la Ley 30096; regulado con respecto a los delitos informáticos.
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? Deberían crear el estado una dirección especial en la investigación de delitos informáticos, ya que muchas veces se han quedado algunas conductas impunes por las deficiencias en la investigación.
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? Esta clase de conducta sobre delitos informáticos, se requiere el dolo para su comisión, ya que si existiría culpa no se configuraría el delito informático.
Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? La tecnología siempre, de alguna forma va apoyar a la investigación de delitos en general, pero esta clase de delitos informáticos si requiere bastante apoyo para poder realizar una investigación idónea y clara y de esta forma contrarrestar el avance delictivo

5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Las penas que se están tomando para esta clase de delitos son muy benignas, ya que no se toma en cuenta el daño patrimonial que realizan a las empresas que a veces las dejan en bancarrota.
6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? Claro, porque regula las conductas delictivas para la comisión de los delitos informáticos.
7. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? Existe la Ley 30096; regula o sanciona las conductas establecidas como delitos informáticos.
8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? En la actualidad no existen estrategias claras la prevención de los delitos informáticos, solo existen recomendaciones, dadas por aquellas instituciones expertas en la materia.
9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? De acuerdo a la información remitida por el Ministerio Publico, las denuncias por delitos informáticos aumentaron durante la pandemia de COVID 19
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? La suplantación de identidad digital es uno de los delitos informáticos más habituales. Puede obtener toda la información sobre la suplantación o robo de identidad en Internet y cuándo supone un delito penal en este enlace. Y dicha conducta se encuentra reculado en el artículo 401 del Código Penal. Con una pena de seis meses a tres años.
11. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? ..... Si considero.
12. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? Si, ya que al no tener las herramientas adecuadas se va a realizar una investigación deficiente.

PODER JUDICIAL DEL PERU
LUIS ALBERTO DEJO APAESTEGUI
JUEZ
JUZGADO ... INVESTIGACION PREPARATORIA TRANSITORIO DE LOS OLIVOS
CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima Norte, 2021

Entrevistado/a: Pedro Wilbert Rojas Arteaga
Cargo/profesión/grado académico: Corte Superior de Justicia de Lima Norte
Normas básicas de la entrevista: .....

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima Norte,2021
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima Norte? Los delitos informáticos, tienen la caracteristica de ser delitos especiales y se encuentran sancionadas Ley 30096 Ley de Delitos informáticos, el tratamiento jurídico penal no es el adecuado por falta de apoyo tecnológico
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? Se debería de crear una dirección especializada en investigación de delitos informáticos debido a la alta impunidad.
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? El tipo penal de suplantación de identidad, necesariamente necesitan del dolo para poder ser considerado como delito.

Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima Norte,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? Si bien es cierto que la tecnología siempre avanza, más aún al encontramos en pandemia estos delitos aumentaron y trajeron nuevas forma de cometerlos los cuales ayudaron a generan ambientes propicios para la comisión de estos delitos, al ser en su mayoría declarados impunes.
5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Bueno me parecen que las penas son bajas dado que el daño patrimonial no es acorde con las sentencias dejando el sabor de impunidad.

6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático?
En mi opinión se cumple con la tipicidad, pero las penas son bajas para el daño ocasionado en algunos casos.

7. Explique, ¿En la legislación penal, existe regulación especifica del delito fraude informático?
Claro se encuentran enmarcadas dentro de la Ley 30096 Ley de Delitos informáticos.

8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales?
En la actualidad la prevención de estos delitos no se encuentran estrategias o procedimientos claros solo tenemos algunas recomendaciones por parte de Instituciones expertas en la investigación de dichos delitos.

9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera?
De todas maneras, la pandemia por el Covid 19 a permitido un incremento de ciberdelincuencia al tener la obligación de utilizar las herramientas del ciberespacio.

Objetivo Especifico 02:

Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima Norte,2021

10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad?
El delito de suplantación de identidad se encuentra tipificado en el artículo 9 de l ley N° 30096, también en el artículo 401 del Código Penal el cual se sanciona cuando el sujeto activo interactúa por las tecnologías de la comunicación con ur tercera persona haciéndose pasar por el suplantado, con la única finalidad de obtener un provecho de otra persona.

11. ¿Considera que la legislación vigente garantiza el manejo adecuado para est delito?
No, puesto que las penas para este delito son muy bajas, además no se ha considerado realmente el daño moral que se ocasiona a la persona puesto pue percibirse de diferentes formas, al parecer solo han tomado en consideración e daño patrimonial.

12. ¿Considera que la formación tecnológica en delitos informáticos es una limitar para la atención del delito de suplantación de identidad?
Si es una limitante, puesto que si se contara con personal calificado ayudaría realizar mejores investigaciones criminales en torno a estos delitos, lo cual facilitan en gran forma los procesos judiciales.

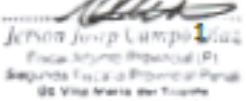
PODER JUDICIAL DEL PERU
PEDRO WILBERT ROJAS ARTEAGA
JUEZ
TERCER JUZGADO PENAL UNIPERSONAL
TRANSITORIO DE LOS OLIVOS
CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTA

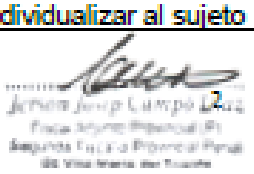
Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: Jerson Josip Campó Díaz
Cargo/profesión/grado académico: Abogado, Fiscal Adjunto Provincial de VMT
Normas básicas de la entrevista: .....

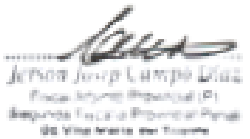
Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Los delitos informáticos, tienen la característica de ser delitos especiales y se encuentran sancionadas con una ley especial, el tratamiento jurídico penal en lo referente a dichos delitos no se viene realizando de manera idónea por falta de una plataforma especial y del apoyo tecnológico que ello conlleva, siendo escasas las dependencias especializadas en los referidos delitos.
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? En principio al tratarse de delitos complejos y con necesidad de apoyo tecnológico, es necesario crear unidades destinadas especiales a combatir esos delitos para lo cual el personal debe estar altamente capacitado tanto a nivel policial, fiscal como judicial.
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? Los delitos informáticos muchas veces son confundidos con los delitos de hurto agravado, estafa y apropiación ilícita, sin embargo debe tenerse presente que los delitos informáticos son delitos especiales y cada tipo penal está descrito en la ley, el uso de las herramientas tecnológicas en evolución permiten la creación de nuevas formas delictivas y nuevos tipos penales, el dolo como conocimiento y voluntad se manifiesta desde antes de cometerse el delito, existen actos preparatorios y es justamente el uso de las tecnologías acompañadas de la conducta ilícita para suplantar, engañar o defraudar para conseguir el resultado final.
Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? La tecnología avanza de manera acelerada y se van creando nuevos



métodos delictivos, ya sea de manera directa o indirecta, a medida que la tecnología continúe avanzando es probable que se manifiesten nuevos delitos y tipos penales, por ejemplo la sustracción de bienes un sujeto lo puede hacer de manera directa por mano propia, con el uso de la tecnología puede apropiarse igualmente desde cualquier punto geográfico y de manera virtual.
5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Si bien es cierto existe una ley específica para los delitos informáticos, la misma resulta confusa en la medida que no se desarrollen unidades especializadas en esos delitos, toda vez que los operadores de justicia no distinguen muchas veces de un fraude informático con una hurto de dinero.
6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? El espíritu de la ley si cumple con el principio de tipicidad para los delitos informáticos, ya que está descrita la conducta, el supuesto de hecho y la consecuencia jurídica.
7. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? En efecto si está regulado el delito de fraude informático, entre otros delitos informáticos.
8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? Dada la experiencia laboral como operador de justicia, he podido advertir ciertas estrategias de manera incipiente, más no claras ni contundentes.
9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? Definitivamente la virtualidad produce que las personas dependan de un aparato tecnológico para poder realizar múltiples tareas, desde realizar pagos, hasta recibir salarios, en ese entendido la delincuencia se adapta a ese tipo de tecnologías de manera rápida.
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? Los delitos informáticos, entre ellos el de suplantación de identidad, desde mi perspectiva no reciben el tratamiento adecuado al no existir unidades tecnológicas avocadas a ver ese tipo de delitos, muchas veces no se cuentan con las herramientas necesarias para lograr individualizar al sujeto



activo del delito.
11. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? La legislación, como toda ley, es un ideal abstracto, la practica hace que el manejo pueda ser adecuado, no obstante no se tienen los recursos tecnológicos ni humanos suficientes para afrontar de manera eficaz dicho delito.
12. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? Efectivamente, la limitación vendrá desde el operador de justicia que tenga el adecuado adiestramiento para afrontar la investigación de los delitos informáticos, lo cual conlleva toda una especialización que lamentablemente no es universal.



INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: Wilfredo Vegas López
Cargo/profesión/grado académico: Fiscal adjunto Provincial Penal Cuarto Despacho de la Fiscalía Provincial Penal Corporativa de Villa María del Triunfo.
Normas básicas de la entrevista: Entrevista

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Estos delitos se encuentran previstos y sancionados en la ley 30096, reglamentada, en ella se detalla las características de los delitos informáticos según los tipos establecidos en la presente ley. Es por ello que si hay un tratamiento jurídico penal de delitos informáticos; lo que considero es que se debe prever otros tipos penales contra el patrimonio, ya que por las características de estos delitos van surgiendo nuevas modalidades que en algunos casos impiden el tratamiento jurídico penal.
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? Se debería desde un principio al tomar conocimiento de estos delitos realizar una investigación célere puesto que en este tipo de delitos la evidencia digital es esencial para la obtención de resultados siendo la misma muy volátil en su permanencia en el tiempo, siendo así si se aplica un método de investigación a los delitos comunes o antiguos, es factible que muchas veces no se alcance la verdad sobre el hecho delictivo.
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? El tipo penal de suplantación de identidad, como bien lo señala el propio texto legal amerita la existencia de un daño económico o moral, esto es una intención del agente de suplantar a la víctima, claro esta que en es fácil demostrar en cuenta existe un perjuicio económico, sin embargo a lo que el tipo penal señala en cuento a un daño moral, es muy amplio puesto que para unas personas o sociedades hay actos propios de ellos que para algunos pueden ser inmorales y para otros pueden ser morales, siendo así es necesario para este tipo de delitos una intención de ocasionar un daño a terceros. ----------

Wilfredo Juan Vegas López
Fiscal Adjunto Provincial
Fiscalia Provincial Penal Corporativa
de Villa María del Triunfo 4° Despacho

1

Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? Así como la tecnología en estos últimos años (de pandemia y post pandemia) ayudaron a las personas a mantener una comunicación y seguir interactuando en sus vidas, este crecimiendo desbordado de la tecnología como era de esperar trajeron nuevos delitos y forma de cometerlos mas aún cuando en el interior de un sistema de redes (o ciberespacio) se generan los ambientes propicios para la comisión de estos delitos, al ser en su mayoría declarados impunes.
5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? La legislación peruana sobre el ciber delito, se encuentra regulada desde la base de la consección del convenio de Budapes el mismo que es el troncal para las legislación que tiene la finalidad de combatir estos delitos, sin embargo al aterrizar este convenio en la legislación peruana, nuestros legisladores trasgredieron diferentes parámetros y paradigmas que volvieron en cierto modo muchos de los delitos informáticos en imposibles jurídicos o redundantes de cumplir un claro ejemplo es los verbos rectores del tipo penal de fraude informático que señala "el que suprime o borra" siendo estos un sinónimo del otro.
6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? En mi opinión no cumple con el principio sancionador, al ser penas muy bajas, puesto conforme se podrá corroborar el hecho de una investigación de un delito informático implica mucho tiempo humano así como requiere análisis digital y tecnología necesaria para la persecución de estos delitos, actos que como estado cuestan y muchas veces existen las carencias de los mismo.
7. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? Si se encuentran tipificados en la Ley 30096 Ley de Delitos informáticos.
8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? En la actualidad la prevención de estos delitos recién se esta dando, como por ejemplo al momento de concientizar a la población común, que cuando poseen un robo de su teléfono celular donde están vinculadas sus cuentas bancarias, antes de producir el bloqueo del teléfono celular es indispensable el bloqueo de cada una de sus tarjetas de crédito o débito.

Wilfredo Juan Vegas López
Fiscal Adjunto Provincial
Fiscalia Provincial Penal Corporativa
de Villa María del Triunfo 4° Despacho

2

9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? Si, como bien lo indique en puntos anteriores, el hecho que existió un aislamiento social, hizo a la sociedad mas pendiente de la tecnológicas, para poder continuar con una vida cotidiana, por lo cual esto fue una gran ventana a la ciberdelincuencia.
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? El delito de suplantación de identidad se encuentra tipificado en el artículo 9 de la ley N° 30096, siendo su tratamiento jurídico de un delito informático, cometiéndose cuando el sujeto activo interactúa por las tecnologías de la comunicación con una tercera persona haciéndose pasar por el suplantado, con la única finalidad de obtener un provecho de una tercera persona o dañar la imagen del suplantado.
11. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? No, puesto como bien lo indique la consumación de este delito en un extremo es cuando se comete un daño patrimonial, hecho que esta claro, y no cabe duda a interpretación, sin embargo la siguiente forma es cuando se refiere a un daño moral, he aquí que no existe un manejo adecuado, puesto que la moral de una persona puede percibirse de diferentes formas.
12. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? No, puesto que las empresas que manejan las redes sociales, tienen políticas claras de ayuda a las investigaciones criminales, lo cual facilitan en gran forma las investigaciones.

Wilfredo Juan Vegas López
Fiscal Adjunto Provincial
Fiscalía Provincial Penal Corporativa
de Villa María del Triunfo 4° Despacho

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: CARLOS ALBERTO BURGOS CUELLAR
Cargo/profesión/grado académico: ABOGADO- CAL 600036
Normas básicas de la entrevista: Agradecería manifestar su consentimiento para el uso de la información brindada

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
1.- En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Considero que al existir una ley y reglamento específicos para estos delitos, si se aplica, es diferente considerar la efectividad de al momento del juzgamiento, ya que en algunos casos las sentencias podrían desvirtuarse
2.- En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? La Ley de delitos informáticos debe permitir la inclusión de tipologías de delitos de manera continua toda vez que con los procesos de innovación tecnológica tan constantes estos delitos van adaptándose y los perpetradores se aprovechan de la lentitud y vacíos legales para sus actos delictivos
3.- ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? Por supuesto, si la ley establece las tipologías de estos delitos y características del hecho delictivo, entonces también existe la intención de realizar el delito.
Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4.- ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? Es una realidad la velocidad que tiene el avance tecnológico, además que esto seguirá acelerándose por lo que los atacantes verán siempre la forma de seguir encontrando artilugios para cometer el hecho delictivo
5.- ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Es urgente que la legislación sobre delitos informáticos se actualice, las nuevas modalidades delictivas que no se consideran agravantes en la ley y que en la realidad si afectan y generan dolo deben ser incorporadas.

6.- ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? NO, puesto que como hemos podido conocer, muchos de estos procesos terminan archivándose. Por el simple hecho que no existe una correspondencia exacta entre lo que el agente ha realizado y aquello que se encuentra descrito en la ley.
7.- Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? Claro que si existe, nuevamente hago énfasis en que este delito cambia en su proceder por lo que exige también a que la ley se adapte
8.- ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? Desde las instituciones públicas no he apreciado alguna campaña para prevenir este delito, más aún no se informa abiertamente de las características del delito y cuál sería el procedimiento que el ciudadano afectado podría realizar
9.- ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? Así es, en este confinamiento, las personas han elegido , por seguridad, realizar los trámites económicos y financieros de manera virtual, sumado a ello la aparición de aplicativos móviles que facilitaron estas transacciones pero que también dieron nuevas opciones a los delincuentes para los hechos delictivos informáticos
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10.- ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? Inicia con la denuncia ante la policía especializada en delistos informáticos, al tener listo la carpeta del caso se presenta al fiscal para la formalización de la demanda e iniciar el proceso de juzgamiento que podría estar en mínimo 3 o máximo 5 años de pena privativa de libertad
11.-¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? Creo que la legislación vigente debe estar en constante actualización, toda vez que al momento de la promulgación de la ley a la fecha han aparecido otros hechos delictivos que en su momento no fueron identificados
12.- ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? Definitivamente, no se puede esperar que el tratamiento jurídico penal procedimental sea eficaz si los agentes que investigan y juzgan estos delitos desconocen las características tan peculiares de los hechos delictivos informáticos

INSTRUMENTO DE RECOLECCIÓN DE DATOS
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: José Luis Oré Huamani
Cargo/profesión/grado académico: ABOGADO - Cal 76187
Normas básicas de la entrevista: Agradecería manifestar su consentimiento para el uso de la información brindada

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
1. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Podremos afirmar, que en la actualidad el tratamiento jurídico penal de los delitos informáticos contra el patrimonio no es tal efectivos, puesto que el ordenamiento jurídico es muy ambiguo al momentos de calidad cada tipo de delitos informáticos contra el patrimonio y la fe pública, siendo así al momento de juzgar no puede obtenerse sentencias efectivas y justas.
2. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? Primero, se debe definir en nuestra Normativa Nacional, cada tipo de Delito Informático y sus requisitos, esto con la finalidad de poder diferenciar cada uno de ellos, puesto que como tenemos conocimientos hay diferentes tipos. Con ello podríamos coadyuvar a que nuestros Jueces al momento de juzgar, puedan garantizar a ambar partes, un debido proceso.
3. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? Si, puesto que para poder cometer este tipo de delitos, es necesario que exista la intención de realizar el hecho delictivo.

Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
4. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos?

Jose Luis Oré Huamani
ABOGADO
CAL, 76187

1

Que conforme, se da el avance tecnológico; la comisión de delitos, van en aumento acelerado. Cada dia sale nuevas formar de delitos informáticos.
5. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Actualmente, nuestro sistema Jurídico, no define bien este tipo de delitos, es decir no los tiene de manera expresa, es por ellos que al momento de juzgar, muchos de estos procesos, terminan archivándose.
6. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? NO, puesto que como hemos podido conocer, muchos de estos procesos terminan archivándose. Por el simple hecho que no existe una correspondencia exacta entre lo que el agente ha realizado y aquello que se encuentra descrito en la ley.
7. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? Si, bien es sabido existe la Ley N° 30096 - LEY DE DELITOS INFORMÁTICOS, esta misma es muy ambigua, y no es suficiente a momento de desarrollarse los procesos judiciales respecto al miso.
8. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? No,
9. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? Si, puesto que con el confinamiento a consecuencia de la pandemia; ha conllevado a usar obligatoriamente los medios tecnológicos, y estos han sido aprovechados por los delincuentes, donde han desarrollado diferente tipo de medios a fin de cometer este tipo de delitos; un medio común utilizado es los mensajes de texto, donde se informan que nuestras cuentas bancarias han sido bloqueadas y nos remiten a un enlace para ingresar.
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
10. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? El agraviado presenta la denuncia y evidencias ante la policía especializada quien debe ejercer las investigaciones para la construcción del caso. Si el delito es comprobado y en la instancia judicial se emite la sentencia; pudiendo ser desde 3 a 5 años de pena privativa de libertad.

Jose Luis Ore Huamani
ABOGADO
CAL. 76187

11. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? No, tenemos una normatividad muy ambigua, que si bien define cada unos de lo delitos, esta no las separa una de otras, conllevando con ello, que al momento de juzgar, el caso pase al archivo.
12. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? Si, puesto que las fiscalizas especializadas que se han formado para ver este tipo de delitos, no reciben las capaciones necesarias para poder ejercer bien la defensa de los agraviados.

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN
GUIA DE ENTREVISTA

Título: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima, 2021

Entrevistado/a: Sub oficial de primera HEGEL COVARRUBIAS MAIHUA

Cargo/profesión/grado académico: *Departamento de patrullaje virtual de la* DIVINDAT

Objetivo general: Determinar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima,2021
10. En base a su experiencia ¿En qué medida se aplica el tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito judicial Lima? Bueno actualmente, como indique en mi presentación lo que se ve ahora con mayor incidencia son los delitos contra el patrimonio lo que es fraude informático, así mismo pornografía infantil mucho caso de seducción a menores. Lo que es el tratamiento legal se reúne la evidencia y se eleva al ministerio público para su tratamiento, pero existen ciertas dificultades de este tipo de casos que manejamos, la información la evidencia digital es un poco complicada para conseguir y montar buen caso, la fiscalía requiere evidencia concreta y poder presentar al juzgado y tener casos que podamos ganar. En ese trayecto lo que hacemos nosotros es reunir la cantidad de evidencias con actas de visualización y análisis forenses y poder reunir evidencias que requiere la fiscalía para sus casos
11. En su opinión ¿Cómo debería de ser el tratamiento jurídico penal adecuado para los delitos informáticos contra el patrimonio, para que sea un buen aporte a la investigación o proceso penal? Nosotros lo que hacemos , es la premura , necesitamos acceso a la información, que tienen los bancos entidades públicas, privadas, que normalmente exige el código procesal penal que un juez autorice el levantamiento del secreto de comunicaciones o levantamiento de ciertas medidas de derecho , pero esa información es importante es indispensable para construir el caso y poder reunir mayor información, recuerda que ese tipo de casos tiene varias dificultades por ejemplo el anonimato del actor, la distancia, la persona puede estar en cualquier parte del país y ejecutar el ataque. Necesitamos acceso a la información publico privada y agilizar la reunión de información del caso eso es vital
12. ¿Considera usted, que los delitos informáticos contra la fe pública, se dan en el momento que aparece el dolo, que se hace de manifiesto con la inducción al error de la víctima a través de la astucia, ardid, engaño u otra forma fraudulenta? Lo que sucede es que la mayor parte de los delitos informaticos requieren la participacion del usuario ya sea por engaño por ardid por ataque de phishing por tecnica de quiza la mas simple en la que el usuario participa del delito sin tener conocimiento. Varias veces hemos vistos casos que hacen tranferencias ilicitas de cuentas bancarias, donde el atacante llama a la víctima haciendose pasar por la entidad bancaria y le pide

SA-31542918
Hegel COVARRUBIAS MAIHUA
S1 PNP

un token de validacion en un supuesto proceso de autenticacion del usuario , y el cliente victima creyendo proporciona el token de validación , que valida la transferencia, esto se da porque la víctima no tiene conocimiento como mantener su seguridad en internet mantener un nivel de seguridad solo se obtiene con el conocimiento adecuado, por ello decimos a las entidades bancarias que eduquen o brinden información a sus usuarios para que no caigan y así reducir el número de víctimas de estos delitos
Objetivo Específico 01: Analizar el tratamiento jurídico penal del delito fraude informático en el Distrito Judicial Lima,2021.
13. ¿Cuál es su opinión respecto a la relación avances tecnológicos y la comisión de delitos? Bueno , eh hace mas de 5 años puede ser 10 años será en el cual era el principal motivo o técnica para hacer fraude informático era la clonación de tarjetas luego apareció los chips en las tarjetas con lo cual la clonación dejó de existir, porque los chip no son clonables. Antes lo que se hacia era leer la banda magnetica y transferirlo a una tarjeta en blanco y con esa tarjeta efectuar los retiros, actualmente ya no se da la clonación. Ya que la seguridad fue aumentada con el chip. Pero la tecnología va avanzando y ahora hay nuevas maneras de engañar al usuario como las billeteras moviles como yape plin, luquita, vin , donde las personas crea con su chip, su numero de telefono las cuentas y por medio de una tecnica llamada sign wapping, el atacante bloquea la linea y crea un chip con el nombre de la persona y procede con la validacion de datos para extraer el dinero. Entonces la tecnología avanza y de igual forma los criminales ven la forma de vulnerar la seguradad que existe y romper esas barreras y obtener el acceso que le permita obtener el dinero de manera ilicita, nosotros como policias debemos estar un paso adelante para poder neutralizarla
14. ¿Cuál es su opinión de la legislación vigente referido a delitos informáticos? Analizando los últimos casos que hemos tenido de delito informático nos hemos dado cuenta que las penas son menores son muy pequeñas y los delicuentes que cometen el delito informático no cumplan una pena efectiva, se les sentencia con menos de 4 años de carcel y eso no es efectiva, yo sugiero que se deben aumentar las penas para que realmente existe una sanción real para estas personas tanto para quienes prestan sus cuentas como quienes son los que reciben el dinero asi como los que captan a las personas por prestar cuentas y sancionar a las cabezas de las bandas u organizaciones criminales en el país porque son varias que no tiene una sanción por sus actos y mayormente se debe a que los jueces y fiscales, aunque hay una fiscalía especializada, principalmente los jueces no tienen conocimiento lo que es informática y la gravedad de estos actos, tomándolo a la ligera y deberían tomar mas empeño en eso.
15. ¿Considera usted que la ley de delitos informáticos cumple con el principio de tipicidad para sancionar el fraude informático? Si está tipificada , es el artpiculo numero 8 de la ley de delitos informáticos está comprendida
16. Explique, ¿En la legislación penal, existe regulación específica del delito fraude informático? Actualmente existe la propia ley de delitos informáticos.

SA-31542918
Hegel COVARRUBIAS MAIHUA
S1 PNP

17. ¿En la actualidad existen estrategias claras para la prevención y sanción de delitos de fraude informático? ¿Cuales? Y como prevención he visto entidades bancarias que existen publicación de campaña de información a sus usuarios, así mismo en la PCM he visto campañas de prevención de ataques informáticos . Para mantener la seguridad de sus usuarios. Ejemplo el banco interbank q te envian mensajes para tener cuidad con mensajes phishing.
18. ¿Considera que la pandemia ha permitido la práctica delictiva informática? ¿De qué manera? La pandemia ha sido una oportunidad para que el uso de tecnología aumente, ya que no hubo entidad bancarias abiertas, las personas tuvieron que usar obligatoriamente la tecnología, se masificó, transferencias bancarias aumentaron. La delincuencia también vio una oportunidad de tener mayor cantidad de victimas en la compras por internet en linea, se dio bastante el fraude informático asi como estafas por compras en plataformas de comercio. La pandemia en el 2020 y 2021 aumentó . Las personas siguen usando las transacciones por internet
Objetivo Específico 02: Analizar el tratamiento jurídico penal del delito suplantación de identidad en el Distrito Judicial Lima,2021
13. ¿Cuál es el tratamiento jurídico penal que se le da al delito suplantación de identidad? Si no me equivoco es el artículo n2 de la ley de delitos informáticos. Si se requiere que exista un daño económico o moral de la persona para configurarse en un delito de suplantación de identidad, estos casos lo e visto cuando suplanta personas por facebook o waap que piden a sus contactos dinero ya que tienen problema, se da un tipo de estafa. También he visto que suplantan la identidad en instagran o facebook para atentar contra su reputación o su honor
14. ¿Considera que la legislación vigente garantiza el manejo adecuado para este delito? Bueno existe una ley que sanciona eso ...se requiere cierto tipo de limitativas de derechos para llegar al atacante pero si existe un proceso de investigación que se puede seguir para sancionarla si fuera el caso
15. ¿Considera que la formación tecnológica en delitos informáticos es una limitante para la atención del delito de suplantación de identidad? Mas que todo yo veo que existe redes sociales en la cual no valida el usuario. Cualquiera puede crear el perfil y hacerse pasar por cualquiera

S1-31542918
Hegel COVARRUBIAS MAIHUA
S1 PNP