FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORA:

Canelo Pacheco, Jery Paola (ORCID: 0000-0002-1613-3209)

ASESOR:

Mtro. Guerra Campos, Jefferson Williams (ORCID: 0000-0003-0158-7248)

LÍNEA DE INVESTIGACIÓN:

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

LIMA – PERÚ

2022

Dedicatoria

Gracias a Dios por darme la oportunidad de estar cumpliendo una de mis metas profesionales, dedico mi trabajo a las personas que me aman, porque verme feliz los hace feliz y sobre todo a mi familia que me motiva a seguir luchando por mis sueños, a mis ángeles que me acompañan en cada paso que doy.

Agradecimiento

Agradezco a la Universidad César Vallejo de Lima por todos los conocimientos brindados.

Así mismo agradezco al Mtro. Guerra Campos, Jefferson Williams, por todas sus enseñanzas.

Agradezco a todos los abogados penalistas que participaron con toda disposición y facilidades del caso para el desarrollo y culminación de la presente investigación.

Índice de Contenidos

Índice de tablas

Resumen

La investigación formuló como objetivo general: Analizar los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público, la metodología empleada es de enfoque cualitativo, de tipo básico, diseño de teoría fundamentada, se tomó como participantes a 6 abogados especialistas en derecho penal, que hayan tratado delitos informáticos. Como técnica se empleó la entrevista y como instrumentos la guía de entrevista validada por un experto. Finalmente concluyo que, los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público es el fraude informático señalado en la Ley 30096, en el Capítulo v, delitos informáticos contra el patrimonio, que implica clonación de tarjeta, compras fraudulentas por internet o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, a consecuencia de la pandemia puesto que se aumentó el comercio electrónico y los niveles de compras por medio de aplicaciones, tiendas virtual y sitios webs.

Palabras clave: Delitos informáticos, redes sociales, tratamiento judicial, Ministerio Público.

Abstract

The research formulated as a general objective: Analyze computer crimes perpetrated through social networks and their judicial treatment in the Public Ministry, the methodology used is a qualitative approach, basic type, grounded theory design, 6 were taken as participants. lawyers specializing in criminal law, one have dealt with computer crimes. The interview was used as a technique and the interview guide validated by two experts as instruments. Finally, it concludes that computer crimes perpetrated through social networks and their judicial treatment in the Public Ministry is the computer fraud indicated in Law 30096, in Chapter V, computer crimes against property, which involves card cloning, purchases fraudulent online, or any interference or manipulation in the operation of a computer system, as a result of the pandemic since electronic commerce and the levels of purchases through applications, virtual stores and websites increased.

***Keywords*:** Computer crimes, social networks, judicial treatment, Public Ministry.

I. INTRODUCCIÓN

Las redes sociales sin duda con el transcurrir del tiempo se han convertido para muchas de las personas en un aspecto esencial para su vida, sin embargo, existen personas inescrupulosas que mediante estas cometen diversos delitos informáticos a fin de vulnerar el derecho de terceros, dañando la integridad, seguridad y bienestar de las personas. Tal es así que en los últimos tiempos estos delitos se han incrementado por el estado de emergencia por covid–19 y la crisis sanitaria que esta genera.

En tanto de acuerdo a la Ley 30096 (2013) en el artículo 1 indica como principal propósito tomar medidas de prevención y lograr sancionar aquellos comportamientos ilícitos afectando data informática de connotación penal, realizadas con herramientas meramente tecnológicas, con el propósito de hacerle frente a la delincuencia, garantizando los derechos de los ciudadanos.

Así mismo en él Código Penal Peruano este se tipifica como delito, especificado en la Ley N° 27309. Según Guerrero (2018) existe un tratado internacional denominado Convenio de Budapest es muy importante pues se trata de un único acuerdo internacional que toma la importancia sobre delitos de la ciberdelincuencia, el objetivo es de proteger a la sociedad, mediante unidades de homologación de normas de derecho penal sustantivo, entro en vigencia tres años después de su redacción aprobada en el 2001, teniendo en América suscrito a: Perú, Argentina, Canadá, y otros.

Según las estadísticas del Ministerio Público de la Oficina de Racionalización, ingresaron de la fecha 22 de octubre de 2013 al 31 de julio de 2020 en las Fiscalías Penales Comunes Especializadas y Fiscalías Mixtas 21 687 denuncias por delitos informáticos (Ministerio Público Fiscalía de la Nación, 2021). Como un ente importante que tiene por función prevenir y sancionar los delitos informáticos es el Ministerio Público, que no actúa solo ni de forma independiente, sino que cuenta con áreas de apoyo para centralizar las ejecuciones de demandas de delitos informáticos.

Por lo tanto, se plantea siguiente problema general ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público?; asimismo se planteó los siguientes problemas específico (a) ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las

redes sociales? (b) ¿Cuáles son las denuncias de delitos informáticos, según artículos específicos de la Ley N°30096? (c) ¿De qué manera afectó a las víctimas los delitos informáticos? (d) ¿Cuál fue el motivo de archivamiento o sobreseimiento de las denuncias por delito informático?

En ese sentido, se presenta la justificación teórica de la investigación que reside en la acumulación del fundamento teórico mediante la recopilación de información, conceptos y demás textos con el fin de fortalecer el conocimiento delitos informáticos perpetrados a través de las redes sociales. De igual manera, la justificación metodológica reside en el aporte de sentar bases como antecedente local para el desarrollo de futuras investigación, puesto que no se evidenció estudios similares en la ciudad de Arequipa bajo el contexto de la pandemia. Finalmente, la justificación social, que fundamenta el aporte a la sociedad y a todos los grupos de interés profesional académico mediante la exposición del conocimiento a través de las derivaciones conseguidas en el presente estudio.

De los problemas antes mencionados, se desprende el siguiente objetivo general, Analizar los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público; asimismo ha planteado los siguientes objetivos específicos (a) Conocer el estado procesal de los delitos informáticos perpetrados a través de las redes sociales (b) Identificar las denuncias de delitos informáticos, según artículos específicos de la Ley N°30096 (c) Precisar las formas de afectación a las víctimas los delitos informáticos (d) Especificar el motivo de archivamiento o sobreseimiento de las denuncias por delito informático.

II. MARCO TEÓRICO

Dentro del marco teórico se consideran los siguientes antecedentes: Basándose en los siguientes antecedentes internacionales como:

Tenesaca y Cedeño (2021), en su trabajo de investigación tuvieron como su objetivo realizar el estudio jurídico, respecto a la implementación del delito de estafa mediante las redes sociales a causa del covid-19. Como metodología aplicada fue de enfoque cualitativo no experimental. El resultado principal que se obtuvo es que, dada la situación innovadora en el ámbito jurídico, se tiene que comprender esta nueva realidad. Los autores concluyeron que este delito computarizado es la realización de delitos a través de medios electrónicos, aunque ya no se está en cuarentena.

Sanmartín (2021), en su trabajo de investigación tuvo como su objetivo realizar la importancia que encontramos en las principales aportaciones en el convenio de Budapest, está se encuentra en la regulación de delitos informáticos en el país de Ecuador, su avance dentro de la perspectiva teórica se encuentra sustentada en la revisión de documentación teórica y académica, su metodología enmarca en un enfoque cualitativo, de alcance descriptivo. El resultado principal que se obtuvo, es hallar los principales aportes en delitos, que se encuentran en las normas procesales de investigación y las normas de cooperación internacional que este permitiría una política penal similar y armonizar la contribución internacional entre países que se han adherido el Convenio de Budapest.

Saraguro (2021), en su trabajo de investigación tuvo como objetivo realizar la importancia en investigar que existe la problemática en delitos informáticos y la capacidad de investigación que se efectúa en el país de Ecuador. Como metodología aplicada fue de enfoque cuantitativo, el tipo de investigación descriptivo, métodos descriptivo, inductivo y documental, El autor concluye que es importante el invertir, adecuar y este se pueda reforzar en cuanto a esta investigación, utilizando técnicas para la determinación del vínculo causal en delitos informáticos, así mismo, es fundamental capacitar, actualizar y formar profesionales que intervengan cómo peritos a fin de alcanzar una mayor eficiencia y obtener mejores resultados.

Valencia et al. (2020), en su trabajo de investigaion tuvo como objetivo general que el estado colombiano defina los lineamientos sobre la seguridad de la

protección de datos digitales de las personas residentes en Colombia. Como metodología aplicada fue de enfoque cualitativo, revisión bibliográfica. Los autores concluyeron que, si bien el país ha avanzado bastante en la identificación y persecución de los delitos cibernéticos, aún es muy poca la importancia que se le da a estos, es muy evidente que la academia desde sus niveles más básicos (escuelas, colegios y universidades) por lo cual hace falta mayor capacitación en el asunto. Puede deducirse de la correlación entre los delitos informáticos y las medidas de protección y correctiva que para ciertos delitos existen huecos o vacíos normativos que aún el legislador no ha tenido en cuenta pero que a la luz del derecho comparado se puede ver que países como España, México y Argentina ya tienen normativa en dichos asuntos.

Por otro lado, se encuentra basado en los siguientes antecedentes nacionales como:

Candia (2017 - 2019), en este trabajo tuvo como objetivo fijar si el estado resguarda el Derecho a la Intimidad de la Persona en las Redes Sociales, como metodología aplicada fue de enfoque cualitativo. El autor concluye que la protección penal en el Perú es deficiente. Por no dar tratamiento en el marco de la cyber-delincuencia de forma directa al problema, teniendo en la legislación genérica, que no abarca los aspectos que este resiste a la violación a la intimidad de la persona, encontrándose en legislación especial, resultando deficiente para sancionar estos delitos.

Gómez (2020), en su trabajo de investigación tiene como objetivo establecer la forma que tipifique dentro del marco jurídico penal que el fiscal determine los delitos informáticos contra el Patrimonio, como metodología aplicada fue de enfoque cualitativo, logrando el desarrollo de teoría y lograr representar con la observación. El autor concluyó que dentro del sistema jurídico penal el fiscal desarrolla de una manera incompleta porque los delitos informáticos contra el patrimonio solo se encuentran tipificados dentro del delito de fraude informático resultando poco para combatir estas situaciones.

Por otro lado, se encuentra basado en los siguientes antecedentes local como:

Herrera (2021), en su trabajo de investigación tiene como objetivo analizar la resistencia de dos derechos fundamentales que continuamente vienen chocando

entre sí y que esta necesita de manera primordial indicar un precedente en las Ley 30096 a nivel constitucional en el momento de verse comparada en un juicio de valor, si se encuentra de manera especial si este enfrentamiento se da por medios electronicos tales como en las redes sociales. Su metodología aplicada fue de enfoque cualitativo y el diseño no experimental. El autor concluyó que dentro del derecho a la libertad de expresión en las redes sociales este vulnera el derecho a la intimidad.

Zambrano (2020), en este trabajo tiene el objetivo de realizar y definir si este uso del sistema móvil inicia los delitos informáticos contra el patrimonio en en departamento de Arequipa. Su metodología aplicada fue de enfoque cualitativa. El autor concluyó que el medio electronico promueve los delitos informáticos contra el patrimonio en la ciudad de Arequipa, sustrayendo fondos monetarios de clientes, ya que al ser un delito computarizado no se logra identificar a los autores.

En tanto respecto a delitos informáticos. En el capítulo I, la finalidad y el objeto de esta Ley en su artículo 1: El objeto de la Ley señala que:

La Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (Ley 30096, 2013, p.1)

Los delitos informáticos están en las redes sociales que están divididos dentro de las denuncias de los delitos informáticos y afectación a las víctimas. (Ministerio Público Fiscalia de la Nación, 2021)

El abuso de los mecanismos y dispositivos informáticos: señalada dentro del Capítulo VII Disposiciones comunes en el Artículo 10: El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. (Ley 30096, 2013, p. 6)

Suplantación de identidad: señalada en el Capítulo VI Delitos informáticos

contra la fe Pública:

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (Ley 30096, 2013, p. 6)

Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos: señalada en el Capítulo III Delitos informáticos contra la indemnidad y libertad sexuales en el artículo 5:

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. (Ley 30096, p. 3)

Forma de Afectación a las víctimas, de manera económica/ de forma patrimonial, existe afectación psicológica y moral, afectación a la intimidad, a la libertad personal, a la libertad e indemnidad sexual.

La afectación de la víctima depende de la modalidad del delito informático; es así que la afectación puede ser económica o patrimonial, pero también puede ser moral o psicológica. En este último caso, la afectación también podría estar generada por la pérdida de sus cuentas en redes sociales y por la frustración al no poder identificar a los autores de los delitos. (Ministerio Público Fiscalia de la Nación, 2021)

El Tratamiento Judicial según los estados procesales de los delitos informáticos se pueden encontrar archivadas, en proceso, sobreseimiento, sentencia, Terminación anticipada. Encontramos también los motivos de archivamiento por la falta de colaboración de la parte afectada, en la falta de información y falta de pericias. (Ministerio Público Fiscalia de la Nación, 2021)

Es importante resaltar el incremento de delitos informáticos que este es perpetrado a través de las redes sociales, ya que esta pandemia en la que vivimos nos ha visto obligados a vivir en aislamiento, este nos haya conducido de una forma

brusca, al uso de la tecnología donde nos permitió poder conectarnos y de la misma forma lograr acceder frecuentemente a las redes sociales, hemos usado esta herramienta digital donde se logró que los usuarios compartieran información personal con la comunidad de su interés. Los delitos informáticos son un tema desconocido en donde no se logra percibir el grado de peligro que esta representa, los ciberdelincuentes se aprovechan de esta situación, donde primero a través de las redes sociales se tiene toda la información personal brindada por todos los usuarios en las diferentes plataformas y que esta se almacena en entorno digital, es así que se logra cometer actos ilícitos, pero si tomamos medias de prevención se lograra disfrutar de una manera confiable y segura de las redes sociales.

De esta manera no seremos víctimas de los ciberdelincuentes que cometen estos actos delictivos a través de medios electrónicos.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Se enmarca en un tipo básico, porque su finalidad es la compilación de información contribuyendo al conocimiento científico con una información analizada y debidamente seleccionada. Hernández (Hernández et al., 2018)

El diseño investigativo es teoría fundamentada. Asimismo, es descriptivo, por ello, la presente investigación analiza características y fenómenos.

3.2. Categorías, Subcategorías y matriz de categorización

Tabla 1

Matriz de categorización

CATEGORÍAS	SUBCATEGORÍA	CRITERIOS
Delitos informáticos a través de las redes sociales	Denuncia en delitos informáticos	Abuso de mecanismos y dispositivos informáticos. Suplantación de identidad. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Contra datos y sistemas Informáticos. Contra la intimidad y el secreto de las comunicaciones. Fraude informático.
	Afectación a las víctimas	De manera económica/ de forma patrimonial. Existe afectación psicológica y moral. Afectación a la intimidad, a la libertad personal. A la libertad e indemnidad sexual.

Tratamiento Judicial	Estado procesal de los delitos informáticos	Archivadas En proceso Sobreseimiento Sentencia Terminación anticipada
	Motivo de archivamiento	Falta de cooperación de la víctima. Por falta de información. Falta de pericias.

Nota: Informe de análisis N°04. Ciberdelincuencia en el Perú: Oficina de Análisis Estratégico Contra la Criminalidad (2021)

3.3. Escenario de estudio

El estudio se llevó a cabo en la ciudad de Arequipa, cuyos entrevistados fueron abogados de derecho penal.

3.4. Participantes

Se tomó como participantes para la presente investigación a 6 abogados especialistas en derecho penal, hayan tratado delitos informáticos.

N°	Nombre y apellido	CÓDIGO	Colegiatura
1	Jose Luis Mendoza Mirando	J.L.M.M.	C.A.A. 6769
2	Sthepahnie C. Zorrilla Galiano	S.C.Z.G.	C.A.A. 12136
3	Victor R. Gallegos Basurco	V.R.G.B.	C.A.A. 10835
4	Walter E. Loayza Arista	W.E.L.A.	C.A.A 9126
5	Guisella Sofia Zevallos Valdez	G.S.Z.V.	CAP 693
6	Cristhian Ortiz Astorga	C.O.A.	C.A.A. 10959

3.5. Técnicas e instrumentos de recolección de datos

Como técnica se empleó la entrevista y como instrumentos la guía de entrevista que permitió recopilar la información y dar respuesta a los principales objetivos de la presente investigación. La guía de entrevista fue validada por un experto en derecho penal.

3.6. Procedimientos

Las denuncias de los delitos informáticos en la actualidad han tomado mayor crecimiento ya que con el aislamiento social nuestras vidas se han desarrollado junto a la tecnología siendo esto aprovechado por los ciberdelincuentes. Es así que surgió la interrogante ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público?, en ese sentido se revisó diversas fuentes primarias, entrevistas aplicadas a 6 abogados especialistas en derecho penal y como fuentes secundarias revisión bibliográfica con prestigio y rigurosidad académica como google académico, redalyc, scielo, Microsoft academy, consited, y repositerios de universidad licenciada por SUNEDU.

3.7. Rigor científico

Basado en el análisis de los resultados previa planificación y desarrollo de la información con un enfoque cualitativo, método inductivo, como estrategia de razonamiento a partir de la Ley de delitos informáticos, recopilación de información confiable, y entrevistas de especialistas en derecho penal, validada por un experto que analizó y evaluó la objetividad, claridad y pertinencia de las preguntas de la guía de entrevista.

3.8. Método de análisis de datos

Por tratarse de una investigación de enfoque cualitativo, se empleó un método interpretativo naturalista, Hernández-Sampieri et al. (2014) concluyeron que, “se enfoca en comprender los fenómenos, explorándolos desde las perspectivas de los participantes en un ambiente natural y en relación con su contexto” (p. 358), ya que recopilo la información mediante técnicas como la entrevista.

3.9. Aspectos éticos

La presente investigación cumple con los aspectos éticos respecto a la forma del documento, puesto que su redacción se ciñe a la Norma APA 7ma edición, respetando las citas ya sean textuales y parafraseadas, además fue evaluada por el programa Turnitin arrojando porcentajes bajos de similitud. Respecto al fondo se desarrolló de forma honesta, empleando rigurosidad científica en la discusión y análisis de resultados.

IV. RESULTADOS Y DISCUSIÓN

Análisis de resultados

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?

Tabla 2

Pregunta n.° 1: respuestas

Entrevistado	Respuesta de la pregunta n.° 1
J.L.M.M.	Delitos contra la indemnidad y libertad sexual, fraude informático, estafa virtual.
S.C.Z.G.	El robo de datos personales.
V.R.G.B.	Acoso sexual, difamación, extorción, estafa, etc.
W.E.L.A.	Con respecto a la ciberdelincuencia podríamos indicar que son: los fraudes informáticos, las estafas virtuales, suplantaciones de identidad, difamación por redes sociales, Facebook, Whattsapp, Masenger.
G.S.Z.V.	Delito a la intimidad, delito de hurto agravado por transferencia electrónica de fondos, telemática en general y empleo de claves secretas, delito de falsificación de documentos informáticos, delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos, delito contra los derechos de autor de software, delito de estafas virtuales, delito de suplantaciones de identidad.
C.O.A.	Fraudes cibernéticos, suplantación de identidad.

Tabla 3:

Pregunta n.° 1: análisis

Convergencia	Divergencia	Interpretación
1. Fraude informático 2. Contra datos y sistemas informáticos 3. Suplantación de identidad 4. Proposiciones a niños, niñas y	No se evidencia desacuerdo respectos a los delitos informáticos perpetrados a través de las redes sociales.	El fraude informático es uno de los delitos perpetrados a través de las redes sociales señalados en la Ley 30096, en el Capítulo v, delitos informáticos contra el patrimonio, que implica clonación de tarjeta, compras fraudulentas por internet,

adolescentes con fines sexuales por medios tecnológicos 5. Contra la intimidad y el secreto de las comunicaciones	o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; en tiempos de pandemia este delito se agudizó, así como delitos: Contra datos y sistemas informáticos, Suplantación de identidad, proposiciones a niños, niñas y adolescentes con fines sexuales y contra la intimidad y el secreto de las comunicaciones.

2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?

Tabla 4:

Pregunta n.° 2: respuestas

Entrevistado	Respuesta de la pregunta n.° 2
J.L.M.M.	Tiene la facultad para solicitar la intervención y control de las comunicaciones y documentos privados.
S.C.Z.G.	La denuncia correspondiente, e investigación en conjunto con la policía.
V.R.G.B.	La victima realiza la denuncia en la comisaria o en la Fiscalía, posteriormente realizar una investigación preliminar para verificar si el hecho denunciado encuadro en un delito penal; en muchos casos estos delitos son archivados.
W.E.L.A.	Se ha creado la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional conjuntamente con la División de Alta Tecnología (DIVANDAT)
G.S.Z.V.	Al igual que los procesos comunes se realiza una investigación preliminar para posteriormente realizar la investigación preparatoria, haciendo uso de peritos expertos en la materia.
C.O.A.	Con la apertura de la denuncia y la investigación preliminar.

Tabla 5:

Pregunta n.° 2: análisis

Convergencia	Divergencia	Interpretación
1. La apertura de la denuncia. 2.La investigación preliminar y preparatoria 3. La División de Investigación de Delitos de Alta Tecnología	No se evidencian desacuerdos	Los profesionales coinciden que el tratamiento judicial parte de la denuncia para que de esta manera la División de Investigación de Delitos de Alta Tecnología, pueda investigar, y se logre combatir Los Delitos Informáticos.

3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?

Tabla 6:

Pregunta n.° 3: respuestas

Entrevistado	Respuesta de la pregunta n.° 3
J.L.M.M.	Ambas modalidades. Sus repercusiones son mínimas.
S.C.Z.G.	Virtual, la investigación tiene plazos, que por pandemia no se cumplieron.
V.R.G.B.	Con la pandemia en el Poder Judicial implemento la mesa de partes virtual y en muchas ocasiones hubo demora excesiva para la recepción de una denuncia, no se permitía la entrevista del Fiscal con la victima causando incertidumbre, la recopilación de pruebas de los delitos informáticos fue dificultosa.
W.E.L.A.	En mi caso las denuncias se hacen presencialmente ante la Policía Nacional y/o Fiscalía. A raíz de la Pandemia por el covid-19, estos delitos se incrementaron en un alto índice. Afecto definitivamente en la duración y calidad de investigación, debido a las limitaciones por confinamientos y protocolos de seguridad. Llegando muchos de estos casos a archivarse debido a la falta de elementos de convicción
G.S.Z.V.	Por la emergencia sanitaria que vivimos a partir de marzo del año 2020, las denuncias se vienen realizando de forma virtual y como consecuencia el aumento de la carga procesal, y por ende, la demora en el desarrollo del trámite de los procesos.

C.O.A.	Virtual, ocasiono un atraso, porque la mayoría de las personas no dominan los sistemas de denuncias virtuales.

Tabla 7:

Pregunta n.° 3: análisis

Convergencia	Divergencia	Interpretación
Las denuncias se hicieron de una forma virtual, por pandemia. Afecto en la duración y calidad del desarrollo del trámite de los procesos.	De 6 abogados solo 1 indica que las repercusiones fueron mínimas.	A partir de la emergencia sanitaria es que las denuncias se hicieron de una forma virtual y esto afecto en la recepción de las denuncias porque hubo una demora excesiva.

4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?

Tabla 8

Pregunta n.° 4: respuestas

Entrevistado	Respuesta de la pregunta n.° 4
J.L.M.M.	Es variado, algunos en etapa de investigación preliminar, otros en formalización, otros en apelación, otros en ejecución.
S.C.Z.G.	Investigación.
V.R.G.B.	Algunos en etapa de investigación preliminar, otros en formalización, otros en juzgamiento, en apelación y otros en ejecución.
W.E.L.A.	Son pocos los que llegan a juicio oral y tienen sentencia condenatoria.
G.S.Z.V.	Según la fecha de interposición de denuncias estas deben de encontrarse en plena investigación preparatoria y en otros casos deben de encontrarse en control de acusación frente al juzgado.
C.O.A.	Es pobre porque no se visto sentencias algunas sobre estos delitos debido a la falta de capacidad y herramientas que permitan identificar las cuentas registradas.

Tabla 9

Pregunta n.° 4: análisis

Convergencia	Divergencia	Interpretación
1. Que se encuentra en la etapa de investigación preliminar. 2.Investigación preparatoria 3.Formalización 4.Apelación 5. Ejecución y otros en juzgamiento.	No se evidencian desacuerdos	En la etapa de la investigación preparatoria, esta tiene por finalidad reunir elementos de convicción, de cargo y de descargo y se decida si formula acusación o no. En la etapa preparatoria el fiscal dispone en realizar nuevas diligencias. Esperando la etapa de juicio oral. Son muy pocos los juicios orales y casi nada respecto a sentencias condenatorias.

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?

Tabla 10

Pregunta n.° 5: respuestas

Entrevistado	Respuesta de la pregunta n.° 5
J.L.M.M.	Deficiente investigación a nivel policial y fiscal, así como prejuicio de género.
S.C.Z.G.	Falta de especialistas en la provincia de Arequipa, se tiene que recurrir a especialistas en Lima, para la investigación.
V.R.G.B.	La falta de elementos de convicción.
W.E.L.A.	Me parece que es la individualización del autor, puesto que los delincuentes actúan bajo email, sitios web, falsos. La falta de elementos de convicción. La falta de una adecuada investigación pericial.
G.S.Z.V.	Por la misma naturaleza del delito, en la mayoría de los casos no se llega a identificar a los autores de los hechos o en otros casos no se logra probar el delito denunciado por lo que dicta el archivo correspondiente.
C.O.A.	La falta de tecnología y la falta de capacitación en el personal dedicado en los delitos informáticos.

Tabla 11

Pregunta n.° 5: análisis

Convergencia	Divergencia	Interpretación
1. La falta de elementos de convicción 2. La falta de capacitación en el personal. 3.Sobre todo la falta de especialistas descentralizada	No se evidencian desacuerdos	Una de las razones principales para que la mayoría de delitos informáticos sean archivados es porque la falta de pruebas, inadecuada investigación pericial y a esto sumar la falta de capacitación de los peritos tecnológicos que hace que estos delitos sean archivados.

6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?

Tabla 12

Pregunta n.° 6: respuestas

Entrevistado	Respuesta de la pregunta n.° 6
J.L.M.M.	Capacitación a policías y fiscales.
S.C.Z.G.	Solicitar que la investigación se realice con especialistas, saber qué es lo que se pretende.
V.R.G.B.	La recopilación de elementos de convicción inmediatamente, con equipos informáticos que puedan rastrear el IP del equipo y realizar la ubicación del infractor.
W.E.L.A.	Que se creen Juzgados Penales Especializados en delitos informáticos descentralizados y con una operatividad tecnológica de alto alcance de ingeniería informática pericial.
G.S.Z.V.	A efectos de agilizar y optimizar el estado de los procesos lo conveniente sería descentralizar el área de análisis digital forense para descongestionar el cuello de botella en Lima por la alta demanda a nivel nacional.
C.O.A.	Crear más juzgados especializados de crimen cibernético con sus respectivos equipos especializados en identificación de cuentas cibernéticas.

Tabla 13

Pregunta n.° 6: análisis

Convergencia	Divergencia	Interpretación
1. Capacitación a los fiscales. 2. Creación de juzgados especializados y descentralizar el área de análisis. 3. Especialistas y equipos de alta tecnología.	No se evidencian desacuerdos.	Para agilizar y optimizar el estado procesal es importante las herramientas que se brinde a los profesionales como capacitar, descentralizar, crear juzgados y contar con equipos de alta tecnología.

7. ¿Qué delitos informáticos son lo más recurrentes?

Tabla 14

Pregunta n.° 7: respuestas

Entrevistado	Respuesta de la pregunta n.° 7
J.L.M.M.	Fraude y estafa.
S.C.Z.G.	Robo de datos personales.
V.R.G.B.	Chantaje, acoso sexual, extorción, difamación, estafa, etc.
W.E.L.A.	Son: los fraudes informáticos, las estafas virtuales, suplantaciones de identidad, difamación por redes sociales, Facebook, Whattsapp, Masenger, Clonación de tarjetas de crédito, compras fraudulentas por internet, transferencia, retiros de fondos no autorizados.
G.S.Z.V.	Son: fraude informático, estafas virtuales, suplantaciones de identidad.
C.O.A.	El fraude informático y la suplantación de identidad.

Tabla 15

Pregunta n.° 7: análisis

Convergencia	Divergencia	Interpretación
1. Fraude 3.Suplantación de identidad 4. Delitos informáticos contra la intimidad y el secreto de las comunicaciones	No hay contradicciones.	Los delitos más recurrentes son: fraude (artículo 8), suplantación de identidad (artículo 9), tráfico ilegal de datos (artículo 6).

8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta

Tabla 16

Pregunta n.° 8: respuestas

Entrevistado	Respuesta de la pregunta n.° 8
J.L.M.M.	Si, por cuanto las penas establecidas son proporcionales al bien jurídico protegido en estos delitos; más aún que, en caso se establecieran penas más duras se contravendrían el fin resocializador de la pena.
S.C.Z.G.	Sí, conforme a la proporcionalidad de la gravedad del delito cometido.
V.R.G.B.	No, ya que muchas veces las denuncias son archivadas por falta de pruebas.
W.E.L.A.	No, creo que es este caso para unos las penas son benignas y para otros excesivas tratándose de delitos informáticos, primero tendríamos que empezar por regular la investigación y luego el juicio para su respectiva pena. Si bien es cierto las penas son razonables lo incierto es que mucho no llegan a esa condena por lo ya mencionado en las otras preguntas.
G.S.Z.V.	No, porque las penas estipuladas en nuestro ordenamiento legal son demasiadas benignas, de ahí que la comisión de los delitos día a día va aumentando.
C.O.A.	No siempre, las penas deberían endurecerse más en lo que es pornografía infantil en línea o cualquier tipo de delito contra la indemnidad sexual.

Tabla 17

Pregunta n.° 8: análisis

Convergencia	Divergencia	Interpretación
Tenemos 4 profesionales que indican que no, pues muchas de las denuncias quedan archivadas,	Tenemos 2 que indican que sí, ya que las penas están establecidas son proporcionales al bien jurídico protegido.	Coincido con los 4 profesionales que las penas no se ajustan razonablemente a los delitos informáticos.

9. ¿Considera que la Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?

Tabla 18

Pregunta n.° 9: respuestas

Entrevistado	Respuesta de la pregunta n.° 9
J.L.M.M.	No, por cuanto se han previsto todas las modalidades de delitos informáticos que a la fecha vienen cometiéndose.
S.C.Z.G.	No, lo que debe mejorar es el desarrollo del proceso de investigación del delito.
V.R.G.B.	Si, la recopilación de pruebas no son las adecuadas, son muy lentos en el proceso y no existe un mecanismo adecuado.
W.E.L.A.	Sí, falta precisar bien el tipo penal; falta precisar mejor el ilícito y el elemento subjetivo (que intención tiene el sujeto activo), podría aplicarse algunas teorías de error en la acción. La Ley no precisa en algunos artículos claramente un resultado como exigencia de la lesión,
G.S.Z.V.	Si, por cuanto su amplitud y crecientes modalidades que día a día se van presentando hacen que en la Ley se encuentren vacíos.
C.O.A.	Sí, porque la tecnología avanza todos los días y cada vez salen más programas que son ignorados por nuestra legislación.

Tabla 19

Pregunta n.° 9: análisis

Convergencia	Divergencia	Interpretación
Tenemos que 4 profesionales coinciden que sí vacíos legales que imposibilitan la sanción de los delitos informáticos,	Tenemos 2 que indican que no hay vacíos y que se ajusta a las modalidades delictivas.	Coincido con los 4 profesionales que Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos. Falta precisar el tipo penal.

10. ¿De qué manera el delito informático afectó a las víctimas?

Tabla 20

Pregunta n.° 10: respuestas

Entrevistado	Respuesta de la pregunta n.° 10
J.L.M.M.	Les causo principalmente afectación patrimonial, ya que la mayor parte de los delitos informáticos es por fraude y estafa.
S.C.Z.G.	El no poder identificar físicamente a la persona que perpetra el delito es limitarte y desconcertante para el agraviado.
V.R.G.B.	Existe daño psicológico, daño económico, daño a la imagen y buena reputación de una persona.
W.E.L.A.	De una manera económica patrimonial y porque no decirlo hasta psicológica al verse vulnerados y no tener la tutela jurisdiccional del estado.
G.S.Z.V.	La afección que sufran es psicológica, moral y económica. Ya que en muchos casos no se logra ni siquiera a que se formalice la denuncia ante el poder judicial, ya que sus denuncias terminan archivándose en sede Fiscal.
C.O.A.	Tanto en lo económico por los delitos de estafa, como en lo emocional y psicológico por la pérdida de su patrimonio o por su suplantación ante las redes sociales.

Tabla 21

Pregunta n.° 10: análisis

Convergencia	Divergencia	Interpretación
1.Afectación psicológica 2. Afectación económica. 3. Afectación patrimonial. 4. Afectación moral.	No se evidencian contradicciones	Los delitos informáticos si afectan a las víctimas, de una manera psicológica, económica, patrimonial y afectación moral.

11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?

Tabla 22

Pregunta n.° 11: respuestas

Entrevistado	Respuesta de la pregunta n.° 11
J.L.M.M.	No pueden desistirse, pues son delitos perseguibles de oficio. En todo caso, lo que si ocurre en algunas ocasiones es que las víctimas no colaboran con la investigación a través de su declaración; y, ello es así, pues no tienen confianza en que la Policía llegue a dar con la identidad de los autores.
S.C.Z.G.	Porque no se le da la importancia que merece, siendo que en la actualidad es relevante el uso de la tecnología.
V.R.G.B.	Porque el proceso es muy largo y no tienen fe en el Ministerio Publico.
W.E.L.A.	Porque los procesos son muy largos, tanto a nivel fiscal como procesal. Y los vacíos que se dan en la Ley.
G.S.Z.V.	Por la falta de jerarquía en la red, el anonimato de los cibernautas, la facilidad de acceso a la información para alterar datos.
C.O.A.	Porque no encuentran respuestas por las entidades, no encuentran asesoría suficiente, por falta de tiempo, porque los procesos largos y tediosos.

Tabla 23

Pregunta n.° 11: análisis

Convergencia	Divergencia	Interpretación
1. Porque es un proceso muy largo. 2. Porque no encuentran respuestas en las entidades. 3. No hay confianza con la autoridad.	No pueden desistirse, ya que son delitos perseguibles.	Las oficinas no cuentan con la logística necesaria, esto hará que el proceso lleve tiempo y las victimas desistan del proceso.

12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta

Tabla 24

Pregunta n.° 12: respuestas

Entrevistado	Respuesta de la pregunta n.° 12
J.L.M.M.	No, por cuanto la propiedad de los usuarios respectos de una red social aún no es un bien jurídico trascendental y vital para el desarrollo de una persona ni de la sociedad.
S.C.Z.G.	La suplantación de identidad es un delito que debe ser sancionado, conforme a las leyes peruanas.
V.R.G.B.	Sí, ya esto permitiría la regulación en el Código Penal y estos delitos estadísticamente van en incremento.
W.E.L.A.	Sí, la falta de tipificación del delito informático de apropiación ilícita, debería estar tipificado en el Código Penal, ya que esta apropiación se desarrolla en redes sociales más utilizadas en nuestro país, como lo son Facebook y twiter y la Ley que lo contempla tiene débiles regulaciones. Es obligación del Estado cautelar las garantías constitucionales. Se debe garantizar la utilización de redes sociales, para mejorar el desarrollo económico, tanto en el ámbito público y privado. Es indispensable que el Estado cuente con el articulado que permita juzgar este tipo de acciones peligrosas para la sociedad de la tecnología.
G.S.Z.V.	Si, por cuanto la manipulación de claves de acceso personal se ha proliferado, en vista de que dicho delito no se encuentra legislado en nuestra Ley peruana

C.O.A.	Sí, porque va contra la libertad que toda persona tiene sobre el uso de las redes sociales.

Tabla 25

Pregunta n.° 12: análisis

Convergencia	Divergencia	Interpretación
1. Sí, ya que la suplantación es un delito que debe ser sancionado. 2. Va contra la libertad que toda persona tiene.	No, por cuanto la propiedad de los usuarios respectos de una red social aún no es un bien jurídico trascendental y vital para el desarrollo de una persona ni de la sociedad.	La apropiación ilícita de las redes sociales si debe tener sanción en el código penal, ya que este código tiene por objeto la prevención de delitos y faltas como medio protector de la persona humana y de la sociedad.

13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?

Tabla 26

Pregunta n.° 13: respuestas

Entrevistado	Respuesta de la pregunta n.° 13
J.L.M.M.	No se logra identificar a los autores y en algunos otros casos no existen suficientes elementos de convicción sobre la responsabilidad penal de los implicados.
S.C.Z.G.	Falta de prueba.
V.R.G.B.	La falta de elementos de convicción.
W.E.L.A.	Falta de una imputación concreta, falta de elementos de convicción no se realizan los actos urgentes e inaplazables, deficientes investigación.
G.S.Z.V.	El archivamiento y sobreseimiento de las denuncias se suscitan generalmente porque durante la investigación preparatoria no se ha logrado identificar al autor

	de los hechos y en otros casos no se ha logrado acopiar suficientes medios probatorios del delito denunciado.
C.O.A.	La falta de preparación y capacitación, así como la falta de tecnología.

Tabla 27

Pregunta n.° 13: análisis

Convergencia	Divergencia	Interpretación
1. No se logra identificar al autor. 2. Falta de prueba. 3. Falta de preparación y capacitación.	No se evidencian contradicciones.	Los motivos de archivamiento o sobreseimiento de las denuncias por delito informático son porque no se logra identificar al autor, la falta de pruebas y sobre todo que nuestro personal no tiene la preparación y capacitación debida.

14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?

Tabla 28

Pregunta n.° 14: respuestas

Entrevistado	Respuesta de la pregunta n.° 14
J.L.M.M.	Porque no tienen confianza en que la Policía llegue a dar con la identidad de los autores.
S.C.Z.G.	Trámites muy engorrosos.
V.R.G.B.	Porque desconocen de informática y en muchos casos el Ministerio Público no tiene la logística para perseguir el delito.
W.E.L.A.	Desisten por que no ven resultados de las investigaciones y ante su frustración lo dejan abandonado. Tratan de cooperar, pero en esta clase de delitos el ciudadano común y corriente no está con la capacidad de brindar más información a un delito que no se individualiza al sujeto activo, ni mucho menos detalla las circunstancias precedentes concomitantes y posteriores.

G.S.Z.V.	Muchas veces porque no disponen de tiempo para cooperar en las investigaciones, además que lo manifestado en su declaración es lo único que puede aportar como prueba y consideran que después de las investigaciones no se llegue a probar los delitos denunciados.
C.O.A.	Por la falta de tiempo, otra por desconocimiento del proceso.

Tabla 29

Pregunta n.° 14: análisis

Convergencia	Divergencia	Interpretación
1. La falta de tiempo. 2. No tienen confianza con la policía. 3. Los ciudadanos desconocen del proceso. 4.Logistica	No se evidencian contradicciones.	La victima desiste y no coopera con el proceso de los delitos informáticos, ya que muchas veces no tienen tiempo, se suma la confianza ante la policía y sobre todo el desconocimiento del proceso y trámites engorrosos.

15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?

Tabla 30

Pregunta n.° 15: respuestas

Entrevistado	Respuesta de la pregunta n.° 15
J.L.M.M.	En algunos casos sí, pues la pericia, como elemento de convicción que es, debe ser desarrollada y evacuada eficientemente; sin embargo, por falta de especialistas suficientes y debidamente acreditados, es que no se realizan las mismas o, de realizarse son defectuosas.
S.C.Z.G.	Sí, porque no se cuenta con especialistas en cada región, que puedan seguir con la investigación en etapa policial.
V.R.G.B.	Sí, porque los peritos o equipos son insuficientes y no existe un adecuado procedimiento para perseguir el delito.
W.E.L.A.	Sí, la informática forense recién se está especializando en nuestro país, la actividad de la recolección de evidencias debe hacerse con mucha cautela, ya que el mínimo descuido la investigación se cae y se archiva. Hoy en día los

	ciberdelincuentes son muy astutos, audaces y los expertos criminalistas forenses tienen que evolucionar.
G.S.Z.V.	En la mayoría de los casos sí, porque en nuestro medio no existen muchos peritos especializados en la materia y los laboratorios existentes se encuentran centralizados en la ciudad de Lima.
C.O.A.	Sí, es por falta de personal capacitado y en especial por la falta de tecnología y falta de instituciones especializadas.

Tabla 31

Pregunta n.° 15: análisis

Convergencia	Divergencia	Interpretación
1. La falta de pericias si es motivo de archivamiento.	No se evidencian contradicciones.	Las pericias cumplen un rol estratégico en la investigación prueban que el imputado sí cometió el delito.

DISCUSIÓN

OBJETIVO GENERAL

Analizar los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público

El fraude informático es uno de los delitos perpetrados a través de las redes sociales señalados en la Ley 30096, en el Capítulo v, delitos informáticos contra el patrimonio, que implica clonación de tarjeta, compras fraudulentas por internet, o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; en tiempos de pandemia este delito se agudizó, así como delitos: contra datos y sistemas informáticos, suplantación de identidad, proposiciones a niños, niñas y adolescentes con fines sexuales y contra la intimidad y el secreto de las comunicaciones, así mismo los profesionales coinciden que el tratamiento judicial parte de la denuncia para que de esta manera la División de Investigación de Delitos de Alta Tecnología, pueda investigar, y se logre combatir los Delitos Informáticos. A partir de la emergencia sanitaria es que las denuncias se hicieron de una forma virtual y esto afecto en la recepción de las denuncias porque hubo una demora excesiva siendo que la mayoría se quedan archivadas y no se logran resolver.

Los investigadores Tenesaca y Cedeño (2021) concluyeron que este delito computarizado es la realización de delitos a través de medios electrónicos, aunque ya no se está en cuarentena, en ese sentido tiene similitud al dar a conocer el contexto bajo la pandemia por covid-19, que le dio una nueva normalidad a las dinámicas sociales puesto que a raíz de las restricciones se incrementaron las comercializaciones electrónicas, compras, ventas, suscripciones, uso de las plataformas cibernéticas, a fines personales, económicos, sociales, educativos y académicos, a consecuencia de la virtualidad se incrementaron los delitos informáticos como el fraude, a razón que ahora se han convertido en parte de la dinámica social y de la necesidad de usar estos medios cibernéticos a causa de las restricciones por la pandemia de covid–19.

OBJETIVO ESPECÍFICO

Conocer el estado procesal de los delitos informáticos perpetrados a través de las redes sociales

El estado procesal de los delitos informáticos perpetrados a través de las redes sociales, es que son archivados. Una de las razones principales para que la mayoría de delitos informáticos sean archivados es por la falta de pruebas, inadecuada investigación pericial y a esto sumar la falta de capacitación de los peritos tecnológicos que hace que estos delitos sean archivados. En la etapa de la investigación preparatoria, esta tiene por finalidad reunir elementos de convicción, de cargo y de descargo y se decida si formula acusación o no. En la etapa preparatoria el fiscal dispone en realizar nuevas diligencias. Esperando la etapa de juicio oral. Son muy pocos los juicios orales y casi nada respecto a sentencias condenatorias. Para agilizar y optimizar el estado procesal es importante las herramientas que se brinde a los profesionales como capacitar, descentralizar, crear juzgados y contar con equipos de alta tecnología.

El investigador Saraguro (2021), concluyo que es importante el invertir, adecuar y reforzar en cuanto a esta investigación, utilizando técnicas para la determinación del vínculo causal en delitos informáticos, así mismo, es fundamental capacitar, actualizar y formar profesionales que intervengan como peritos, a fin de alcanzar una mayor eficiencia y obtener mejores resultados, del mismo modo es importante que se utilicen técnicas que permita desarrollar la investigación y que no se archive el proceso.

OBJETIVO ESPECÍFICO

Identificar las denuncias de delitos informáticos, según artículos específicos de la Ley N°30096

Los delitos más recurrentes que son: fraude (artículo 8 capítulo V delitos informáticos contra el patrimonio) suplantación de identidad (artículo 9 capítulo VI delitos informáticos contra la fe pública), tráfico ilegal de datos (artículo 6, capitulo II delitos contra datos y sistemas informáticos), además la Ley N°30096 presenta algunos vacíos legales que imposibilitan la sanción de los delitos informáticos, las penas no se ajustan razonablemente a los delitos informáticos falta precisar el tipo penal.

Los investigadores Tenesaca y Cedeño (2021), concluyeron que este delito computarizado es la realización de delitos a través de medios electrónicos, aunque ya no se está en cuarentena, si bien es cierto que ya no estamos en cuarentena las denuncias de delitos informáticos se siguen sumando a pesar que ya estos están tipificados en la Ley N°30096.

OBJETIVO ESPECÍFICO

Precisar las formas de afectación a las víctimas los delitos informáticos

Los delitos informáticos si afectan a las víctimas, de una manera psicológica, económica, patrimonial y afectación moral, además las oficinas no cuentan con la logística necesaria, esto hará que el proceso lleve tiempo y las victimas desistan del proceso. La apropiación ilícita de las redes sociales si debe tener sanción en el código penal, ya que este código tiene por objeto la prevención de delitos y faltas como medio protector de la persona humana y de la sociedad.

El investigador Candia (2017 - 2019) concluyó que la protección penal en el Perú es deficiente. Por no dar tratamiento en el marco de la cyber-delincuencia de forma directa al problema, teniendo en la legislación genérica, que no abarca los aspectos que este resiste a la violación a la intimidad de la persona, encontrándose en legislación especial, resultando deficiente para sancionar estos delitos.

OBJETIVO ESPECÍFICO

Especificar el motivo de archivamiento o sobreseimiento de las denuncias por delito informático.

Los motivos de archivamiento o sobreseimiento de las denuncias por delito informático son porque no se logra identificar al autor, la falta de pruebas y sobre todo que el personal no tiene la preparación y capacitación debida es así que la victima desiste y no coopera con el proceso de los delitos informáticos, ya que muchas veces no tienen tiempo, se suma la desconfianza ante la policía y sobre todo el desconocimiento del proceso y trámites engorrosos. Las pericias cumplen un rol estratégico en la investigación prueban que el imputado sí cometió el delito.

El autor Saraguro (2021), concluyo que es importante el invertir, adecuar y este se pueda reforzar en cuanto a esta investigación, utilizando técnicas para la determinación del vínculo causal en delitos informáticos, así mismo, es fundamental capacitar, actualizar y formar profesionales que intervengan cómo peritos a fin de alcanzar una mayor eficiencia y obtener mejores resultados, del mismo modo que indica el investigador es necesaria reforzar al Ministerio público para que las denuncias no terminen en archivamiento y se logre identificar al autor de estos delitos.

V. CONCLUSIONES

1. Los delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público es el fraude informático señalado en la Ley 30096, en el Capítulo v, delitos informáticos contra el patrimonio, que implica clonación de tarjeta, compras fraudulentas por internet, o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, a consecuencia de la pandemia puesto que se aumentó el comercio electrónico y los niveles de compras por medio de aplicaciones, tiendas virtual y sitios webs.
2. El estado procesal de los delitos informáticos perpetrados a través de las redes sociales es que son archivados por falta de pruebas, inadecuada investigación pericial y la falta de capacitación de los peritos tecnológicos, son muy pocos los juicios orales y casi nada respecto a sentencias condenatorias.
3. Las denuncias de delitos informáticos, según artículos específicos de la Ley N°30096, son fraude (artículo 8 capítulo V delitos informáticos contra el patrimonio) suplantación de identidad (artículo 9 capítulo VI delitos informáticos contra la fe pública), tráfico ilegal de datos (artículo 6, capitulo II delitos contra datos y sistemas informáticos).
4. Las formas de afectación a las víctimas los delitos informáticos manera psicológica, económica, patrimonial y afectación moral, además las oficinas no cuentan con la logística necesaria, esto hará que el proceso lleve tiempo y las victimas desistan del proceso.
5. El motivo de archivamiento o sobreseimiento de las denuncias por delito informático son porque no se logra identificar al autor, la falta de pruebas y sobre todo que el personal no tiene la preparación y capacitación debida es así que la víctima desiste y no coopera con el proceso de los delitos informáticos, ya que muchas veces no tienen tiempo, se suma la desconfianza ante la policía y sobre todo el desconocimiento del proceso y trámites engorrosos.

VI. RECOMENDACIONES

El Ministerio Público, debe de descentralizarse e indica que el delito específico con mayor cantidad de denuncias es el fraude informático se necesita la descentralización e implementación de laboratorios tecnológicos modernos, para que de esta manera se logre identificar al autor del delito.

Creación de Fiscalías y Juzgados especializados en Ciberdelincuencia para coadyuvar en la investigación de estos delitos, la frecuente capacitación a los especialistas acompañados de peritos informáticos.

Ley N°30096 debe ser revisada y actualizada constantemente, por la dinámica y avance tecnológico y la participación activa que tienen los ciudadanos por el uso de las redes sociales, compra y venta por plataformas de internet.

La escuela del Ministerio Público tiene que realizar actividades de capacitación y educación digital, a fin de educar a la comunidad sobre las medidas, cuidados y protección de datos personales utilizados en redes sociales y comercialización digital.

El Ministerio Público debe implementar oficinas descentralizadas a fin de agilizar la investigación de las denuncias por delitos informáticos, así evitar la burocracia y demora en la resolución de los casos.

REFERENCIAS

Candia Román , G. (2017 - 2019). Los delitos informáticos y la afectación al derecho a la intimidad de la persona en las redes sociales del distrito de Wanchaq - Cusco 2017 - 2019. Cusco, Perú, Tesis de Derecho de la Universidad Andina de Cusco: https://t.ly/EfBo

Gómez Vásquez, J. C. (2020). El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019. Lima, Perú. https://t.ly/9zb0

Guerrero Argote, C. (junio de 2018). *De Budapest al Perú - Proceso de implementación del convenio de Ciberdelincuencia.* Obtenido de Impacto en el corto, mediano y largo plazo: https://t.ly/swAB

Hernández - Sampieri , R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* México: Mc Graw Hill.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación* (6ta ed.). Mexico: Mc Graw Hill Education.

Herrera Huarilloclla, X. W. (2021). Análisis del derecho a la libertad de expresión en redes sociales y la vulneración del derecho a la intimidad, Arequipa 2021. AREQUIPA, AREQUIPA, PERÚ. Obtenido de https://t.ly/SRy4

Ministerio Público Fiscalia de la Nación. (febrero de 2021). *Informe de Análisis N 04 Ciberdelincuencia en el Perú: Pautas para una investigación Fiscal Especializada.* Obtenido de Oficina de Análisis Estratégico contra la Criminalidad: https://t.ly/2VPS

Peruano, P. d. (22 de enero de 2022). *Ministerio Público Fiscalía de la Nación*. Obtenido de https://t.ly/xRlL

República, C. d. (22 de octubre de 2013). Ley de Delitos Informáticos Ley Nº 30096. Lima, Perú: https://t.ly/QGri.

Rios Ramirez, R. R. (2017). *Metodología para la investigación.* Servicios Académicos Intercontinentales S.L.

Sanmartín Mora , W. C. (2021). Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio. Quito, Ecuador. Obtenido de https://t.ly/Sozz

Saraguro Olalla, A. B. (2021). LA DEBILIDAD DEL PROCESO INVESTIGATIVO DE LOS DETILOS. Ibarra, Ecuador. Obtenido de https://t.ly/_jZZ

Tenesaca Gusqui, V. S., & Cedeño Heras, I. A. (ABRIL de 2021). Análisis del delito de estafa en redes sociales en medios electrónicos en la ciudad de Guayaquil a consecuencia de la cuarentena producto de la pandemia del coronavirus en el año 2020. Guayaquil, Ecuador. GUAYAQUIL, ECUADOR. Obtenido de https://t.ly/HuFl

Valencia Gómez, M. O., Espejo Pérez, M. M., & Cano Ramírez, P. A. (ABRIL de 2020). Los delitos informáticos virtuales en redes sociales y las medidas que ha tomado el Estado colombiano para garantizar la protección integral de los ciudadanos al año 2019. *EDUCACIÓN INCLUSIÓN Y DERECHO, PRIMERA*, 231. COLOMBIA. Obtenido de https://t.ly/HuFl

Zambrano Gomez, A. A. (2020). El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de arequipa, 2020. AREQUIPA, AREQUIPA. Obtenido de https://t.ly/w1Tg

ANEXOS

Anexo A

Validaciones

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y nombres: Juan Manuel Siguas Quesquen
1.2. Cargo e institución donde labora: Docente de la Universidad Cesar Vallejo
1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista
1.4. Autor(a) de Instrumento: Jery Paola Canelo Pacheco

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE					MÍNIMAMENTE 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

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

IV. PROMEDIO DE VALORACIÓN: 90 %

Lima, 23 de Abril de 2022

FIRMA DEL EXPERTO INFORMANTE

DNI N.º 09316514 - Telf.: 984675578

Anexo B

Entrevista 1: Jose Luis Mendoza Miranda

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?
   Delitos contra la indemnidad y libertad sexual, fraude informático, estafa virtual.
2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?
   Tiene facultad para solicitar la intervención y control de las comunicaciones y documentos privados.
3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?
   Ambas modalidades. Sus repercusiones son mínimas.
4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?
   Es variado, algunos en etapa de investigación preliminar, otros en formalización, otros en juzgamiento, otros en apelación, otros en ejecución.
5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?
   Deficiente investigación a nivel policial y fiscal, así como prejuicio de género.
6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?
   Capacitación a policías y fiscales.
7. ¿Qué delitos informáticos son lo más recurrentes?
   Fraude y estafa.
8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta
   Sí, por cuanto las penas establecidas son proporcionales al bien jurídico protegido en estos delitos; más aún que, en caso se establecieran penas más duras, se contravendría el fin resocializador de la pena.

José Luis Mendoza Miranda
Especialista Legal
Primer Juzgado de Paz Letrado
Módulo Básico de Justicia de Paucarpata
CORTE SUPERIOR DE JUSTICIA DE AREQUIPA

9. ¿Considera que la Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?
   No, por cuanto se han previsto todas las modalidades de delitos informáticos que a la fecha vienen cometiéndose.
10. ¿De qué manera los delitos informáticos afectó a las víctimas?
    Les causó principalmente afectación patrimonial, ya que la mayor parte de los delitos informáticos es por fraude y estafa.
11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?
    No pueden desistirse, pues son delitos perseguibles de oficio. En todo caso, lo que sí ocurre en algunas ocasiones es que las víctimas no colaboran con la investigación a través de su declaración; y, ello es así, pues no tienen confianza en que la Policía llegue a dar con la identidad de los autores.
12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta
    No, por cuanto la propiedad de los usuarios respecto de una red social aún no es un bien jurídico trascendental y vital para el desarrollo de una persona ni de la sociedad.
13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?
    No se logra identificar a los autores y en algunos otros casos no existen suficientes elementos de convicción sobre la responsabilidad penal de los implicados.
14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?
    Porque no tienen confianza en que la Policía llegue a dar con la identidad de los autores.
15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?
    En algunos casos sí, pues la pericia, como elemento de convicción que es, debe ser desarrollada y evacuada eficientemente; sin embargo, por falta de especialistas suficientes y debidamente acreditados, es que no se realizan las mismas o, de realizarse, son defectuosas.

José Luis Mendoza Miranda
Fiscal Adjunto Provincial
Primer Despacho
Módulo Básico de Justicia Paucarpata
CORTE SUPERIOR DE JUSTICIA AREQUIPA

Entrevista 2: Sthepahnie C. Zorrilla Galiano

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?
   El robo de datos personales
2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?
   La denuncia correspondiente, e investigación en conjunto con la policía.
3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?
   Virtual, la investigación tiene plazos, que por pandemia no se cumplieron
4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?

Investigación

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?
   Falta de especialistas en la provincia de Arequipa, se tiene que recurrir a especialistas en Lima, para la investigación.
6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?
   Solicitar que la investigación se realice con especialistas, saber qué es lo que se pretende
7. ¿Qué delitos informáticos son lo más recurrentes?
   Robo de datos personales
8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta
   Si, conforme a la proporcionalidad de la gravedad del delito cometido.
9. ¿Considera que la Ley N°30096 tiene algunos vacios legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?
   No, lo que debe mejorar es el desarrollo del proceso de investigación del delito.

10. ¿De qué manera los delitos informáticos afectaron a las víctimas?
    El no poder identificar físicamente a la persona que perpetra el delito es limitarte y desconcertante para el agraviado.
11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?
    Porque no se le da la importancia que merece, siendo que en la actualidad es relevante el uso de la tecnología.
12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta
    La suplantación de identidad es un delito que debe ser sancionado, conforme a las leyes peruanas.
13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?
    Falta de pruebas
14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?
    Trámites muy engorrosos
15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?
    Si porque no se cuenta con especialistas en casa región, que puedan seguir con la investigación en etapa policial.

STEPHANY C. ZORRILLA GALIANO
ABOGADA
C.A.A. N°12136

Entrevista 3: Victor R. Gallegos Basurco

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?
   Acoso sexual, difamación, extorción, estafa, etc.

2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?
   La víctima realiza la denuncia en la comisaria o en la Fiscalía, posteriormente realizar una investigación preliminar para verificar si el hecho denunciado encuadro en un delito penal; en muchos caso estos delitos son archivados.

3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?
   Con la pandemia en el Poder Judicial implemento la mesa de partes virtual y en muchas ocasiones hubo demora excesiva para la recepción de una denuncia, no se permitía la entrevista del Fiscal con la victima causando incertidumbre, la recopilación de pruebas de los delitos informáticos fue dificultosa.

4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?
   Algunos en etapa de investigación preliminar, otros en formalización, otros en juzgamiento, en apelación y otros en ejecución.

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?
   La falta de elementos de convicción.

6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?
   La recopilación de elementos de convicción inmediatamente, con equipos informáticos que puedan rastrear el IP del equipo y realizar la ubicación del infractor.

7. ¿Qué delitos informáticos son lo más recurrentes?
   Chantaje, acoso sexual, extorción, difamación, estafa, etc

8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta

No, ya que muchas veces las denuncias son archivadas por falta de pruebas.

9. ¿Considera que la Ley N° 30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?
   Si, la recopilación de pruebas no son las adecuadas, son muy lentos en el proceso y no existe un mecanismo adecuado.

10. ¿De qué manera los delitos informáticos afectó a las víctimas?
    Existe daño psicológico, daño económico, daño a la imagen y buena reputación de una persona.

11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?
    Porque el proceso es muy largo y no tienen fe en el Ministerio Publico.

12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta
    Si, ya esto permitiría la regulación en el Código Penal y estos delitos estadísticamente van en incremento.

13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?
    La falta de elementos de convicción.

14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?
    Porque desconocen de informática y en muchos casos el Ministerio Publico no tiene la logística para perseguir el delito.

15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?
    Sí, porque los peritos o equipos son insuficientes y no existe una adecuado procedimiento para perseguir el delito.

Victor R. Gallegos Basurco
ABOGADO
C.A.A. 10835

Entrevista 4: Walter E. Loayza Arista

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?

   Con respecto a la Ciberdelincuencia podríamos indicar que son: los fraudes informáticos, las estafas virtuales, suplantaciones de identidad, difamación por redes sociales, Faccebook, Whattsapp, Masenger.

2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?

   Se ha creado la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional conjuntamente con la División de Investigación de Alta Tecnología (Divandat).

3. ¿Las denuncias se hicieron de forma presencial o virtual?

   En mi caso las denuncias se hacen presencialmente ante la Policía Nacional y/o Fiscalía.

   ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?

   A raíz de la Pandemia por el Covid 19, estos delitos se incrementaron en un alto índice, afectó definitivamente en la duración y calidad de investigación, debido a las limitaciones por confinamientos y protocolos de seguridad. Llegando muchos de estos casos a archivarse debido a la falta de elementos de convicción.

4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?

   Son pocos los que llegan a juicio oral y tienen sentencia condenatoria.

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?

   Me parece que es la individualización del autor, puesto que los delincuentes actúan bajo email, sitios web, falsos. La falta de elementos de convicción. La falta de una adecuada investigación pericial.

6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?

Que se creen Juzgados Penales Especializados en Delitos Informáticos Descentralizados y con una operatividad tecnológica de alto alcance de ingeniería informática pericial.

7. ¿Qué delitos informáticos son lo más recurrentes?

Son: los fraudes informáticos, las estafas virtuales, suplantaciones de identidad, difamación por redes sociales, Faccebook, Whattsapp, Masenger. Clonación de tarjetas de crédito, compras fraudulentas por internet, transferencia, retiros de fondos no autorizados

8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta

No, creo que es este caso para unos las penas son benignas y para otros excesivas. Tratándose de delitos informáticos, primero tendríamos que empezar por regular la investigación y luego el juicio para su respectiva pena. Si bien es cierto las penas son razonables lo incierto es que muchos no llegan a esa condena por lo ya mencionado en las otras preguntas.

9. ¿Considera que la Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?

Si, falta precisar bien el tipo penal; falta precisar mejor el ilícito y el elemento subjetivo (que intención tiene el sujeto activo), podría aplicarse algunas teorías de error en la acción. La ley no precisa en algunos artículos claramente un resultado como exigencia de la lesión.

10. ¿De qué manera los delitos informáticos afectó a las víctimas?

De una manera económica patrimonial y porque no decirlo hasta psicológica al verse vulnerados y no tener la tutela jurisdiccional del estado.

11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?

Porque los procesos son muy largos, tanto a nivel fiscal como procesal. Y los vacíos que se dan en la Ley.

12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta

    Si, la falta de tipificación del delito informático de apropiación ilícita, debería estar tipificado en el Código Penal, ya que esta apropiación se desarrolla en redes sociales más utilizadas en nuestro país, como son Facebook y twiter y la ley que lo contempla tiene débiles regulaciones. Es obligación del Estado cautelar las garantías constitucionales. Se debe garantizar la utilización de redes sociales, para mejorar el desarrollo económico, tanto en el ámbito público y privado. Es indispensable que el Estado cuente con el articulado que permita juzgar este tipo de acciones peligrosas para la sociedad de la tecnología.

13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?

    Falta de una imputación concreta, falta de elementos de convicción, no se realizan los actos urgentes e inaplazables, deficiente investigación.

14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?

    Desisten por que no ven resultados de las investigaciones y ante su frustración lo dejan abandonado. Tratan de cooperar, pero en esta clase de delitos el ciudadano común y corriente no está con la capacidad de brindar más información a un delito que no se individualiza al sujeto activo, ni mucho menos detallan las circunstancias precedentes concomitantes y posteriores.

15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?

    Si, La informática forense recién se está especializando en nuestro país, la actividad de la recolección de evidencias debe hacerse con mucha cautela, ya que el mínimo descuido la investigación se cae y se archiva. Hoy en día los ciberdelincuentes son muy astutos, audaces y los expertos criminalistas forenses tienen que evolucionar.

Entrevista 5: Guisella Sofia Zevallos Valdez

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?

- Delito a la intimidad.
- Delito de hurto agravado por transferencia electrónica de fondos, telemática en general y empleo de claves secretas.
- Delito de falsificación de documentos informáticos.
- Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.
- Delito contra los derechos de autor de software.
- Delito de Estafas virtuales
- Delito de suplantaciones de identidad.

2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?

Al igual que los procesos comunes se realiza una investigación preliminar para posteriormente realizar la investigación preparatoria, haciendo uso de peritos expertos en la materia.

3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?

Por la emergencia sanitaria que vivimos a partir de marzo del año 2020, las denuncias se vienen realizando de forma virtual y como consecuencia el aumento de la carga procesal y, por ende, la demora en el desarrollo del trámite de los procesos.

4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?

Según la fecha de interposición de denuncias estas deben de encontrarse en plena investigación preparatoria y en otros casos deben de encontrarse en control de acusación frente al juzgado.

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?

Por la misma naturaleza del delito, en la mayoría de los casos no se llega a identificar a los autores de los hechos o en otros casos no se logra probar el delito denunciado por lo que dicta el archivo correspondiente.

6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?

A efectos de agilizar y optimizar el estado de los procesos lo conveniente seria descentralizar el área de análisis digital forense para descongestionar el cuello de botella en Lima por la alta demanda a nivel nacional.

7. ¿Qué delitos informáticos son lo más recurrentes?

- Fraudes informáticos.
- Estafas virtuales.
- Suplantaciones de identidad.

8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta

No, porque las penas estipuladas en nuestro ordenamiento legal son demasiadas benignas, de ahí que la comisión de los delitos día a día va aumentando.

9. ¿Considera que la Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?

Si, por cuanto su amplitud y crecientes modalidades que día a día se van presentando hace que en la ley se encuentren vacíos.

10. ¿De qué manera los delitos informáticos afectaron a las víctimas?

La afección que sufren es psicológica, moral y económica. Ya que en muchos casos no se logra nj siquiera a que se formalice la denuncia ante el poder judicial, ya que sus denuncias terminan archivándose en sede Fiscal.

11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?

Por la falta de jerarquía en la red, el anonimato de los cibernautas, la facilidad de acceso a la información para alterar datos.

12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta

Si, por cuanto la manipulación de claves de acceso personal se ha proliferado, en vista de que dicho delito no se encuentra legislado en nuestra ley peruana.

13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?

El archivamiento y sobreseimiento de las denuncias se suscitan generalmente porque durante la investigación preparatoria no se ha logrado identificar al autor de los hechos y en otros casos no se ha logrado acopiar suficientes medios probatorios del delito denunciado.

14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?

Muchas veces porque no disponen de tiempo para cooperar en las investigaciones, además que lo manifestado en su declaración es lo único que puede aportar como prueba y consideran que después de las investigaciones no se llegue a probar los delitos denunciados.

15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?

En la mayoría de los casos sí, porque en nuestro medio no existen muchos peritos especializados en la materia y los laboratorios existentes se encuentran centralizados en la ciudad de Lima.

GUISELA SOFIA ZEVALLOS VALDEZ
CAP. 693

Entrevista 6: Cristhian Ortiz Astorga

ANEXOS

ENTREVISTA

1. ¿Cuáles son los delitos informáticos perpetrados a través de las redes sociales?

Fraudes Cibernéticos, Suplantación de identidad.

2. Respecto con la primera pregunta, ¿cuál es el tratamiento judicial en el Ministerio Público?

Con personal capacitado en ciberdelincuencia y equipos de última generación que permitan identificar los imei de los equipos que operan los delincuentes.

3. ¿Las denuncias se hicieron de forma presencial o virtual? ¿Cuánto afecto esta nueva normalidad en el desarrollo del proceso, respecto a los delitos informáticos?

Virtual, ocasiono un atraso, porque la mayoría de las personas no dominan los sistemas de denuncias virtuales.

4. ¿Cuál es el estado procesal de los delitos informáticos perpetrados a través de las redes sociales?

Es pobre porque no se ha visto sentencias algunas sobre estos delitos debido a la falta de capacidad y herramientas que permitan identificar las cuentas registradas.

5. ¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?

La falta de tecnología y la falta de capacitación en el personal dedicado en los delitos informáticos.

6. ¿Cuáles considera que deben ser las estrategias para agilizar y optimizar el estado procesal de los delitos informáticos?

Crear más juzgados especializados de crimen cibernético con sus respectivos equipos especializados en identificación de cuentas cibernéticas.

7. ¿Qué delitos informáticos son lo más recurrentes?

El fraude informático y la suplantación de identidad.

8. ¿Las penas se ajustan razonablemente a los delitos informáticos? Fundamente su respuesta

No siempre, las penas deberían endurecerse más en lo que es pornografía infantil en línea o cualquier tipo de delito contra la indemnidad sexual.

9. ¿Considera que la Ley N°30096 tiene algunos vacíos legales que imposibilitan la sanción de los delitos informáticos? Si o no ¿Por qué?

Sí, porque la tecnología avanza todos los días y cada vez salen más programas que son ignorados por nuestra legislación.

10. ¿De qué manera los delitos informáticos afectó a las víctimas?

Tanto económico por los delitos de estafa como en lo emocional y psicológico por la pérdida de su patrimonio o por suplantación ante las redes sociales.

11. ¿Por qué cree que la mayoría de las victimas desisten del proceso?

Porque no encuentran respuestas por las entidades, no encuentran asesoría suficiente, por falta de tiempo, porque los procesos son largos y tediosos.

12. ¿Considera que la apropiación ilícita de las redes sociales debe tener sanción en el código penal? Fundamente su respuesta

Si, porque va contra la libertad que toda persona tiene sobre el uso de las redes sociales.

13. ¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?

La falta de preparación y capacitación, así como la falta de tecnología.

14. ¿Por qué la victima desiste y no coopera con el proceso de los delitos informáticos?

Por la falta de tiempo, otra por desconocimiento del proceso.

15. ¿Los motivos de archivamiento es por falta de pericias? Si o no ¿Por qué?

Sí, es por falta de personal capacitado y en especial por la falta de tecnología y falta de instituciones especializadas.

Cristhian Ortiz Astorga
ABOGADO
C.A.A. 10959