UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DERECHO

El levantamiento del secreto de las comunicaciones en los delitos informáticos

TESIS PARA OBTENER EL TITULO PROFESIONAL DE:
ABOGADO

AUTORES:

Lunarejo Guevara, Erick Bryan (ORCID: 0000-0001-5693-7829)

Rodriguez Gil, Karla Olinda (ORCID: 0000-0003-3994-4749)

ASESORA:

Dra. Alcántara Francia Olga (ORCID: 0000-0001-9159-1245)

Dr. Vega Aguilar, Jorge Alberto (ORCID: 0000-0002-4189-3496)

LÍNEA DE INVESTIGACIÓN:

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

CHIMBOTE — PERÚ

2021

DEDICATORIA

De Erick Bryan Lunarejo Guevara:

Dedicado a mi madre que se sacrificó y esforzó para que yo siempre siga adelante, a mi padre que fue mi fortaleza para no caer. A mis tíos abuelos, que me criaron y que nunca dudaron de mí. A mi hermano, mi primer compañero de vida, uno de los motivos por los cuales nunca desistí, para demostrarle que todos podemos ser alguien en la vida y ser mejores de lo que fuimos.

Para mi futuro acompañante de vida, mi hijo.

Para el Estudio Jurídico Pisfil & Asociados, donde realicé mis prácticas y encontré buenos amigos que me impulsaron a ser mejor cada día.

De Karla Olinda Rodriguez Gil:

Dedicado a mis padres Luis y Clara, por apoyarme durante toda mi vida, impulsándome a ser mejor cada día y cumplir todas mis metas; a mi hermano Carlos por haberme aconsejado y apoyado en cada decisión tomada, y a mi hermanita Paola por hacerme sonreír con sus ocurrencias y brindarme su amor incondicional.

Dedicado al Dr. Wilson Andrade y la Dra. Josselyn Izáziga por haberme brindado sus conocimientos, impulsándome a ser mejor cada día, a la Dra. Fiorella y Dra. Vania por haberme enseñado y apoyado ante cada error cometido para ser mejor.

Dedicado a mi mascota Pirata por haberme acompañado a lo largo de mi vida, siendo la razón de mi felicidad y dedicación; y en memoria de mi mascota Cokcer por haber sido mi amigo incondicional y haber estado durante los momentos en los que pensé no seguir adelante, por haberme dado alegría con su mirada.

AGRADECIMIENTO

Agradecemos a Dios por bendecirnos y guiarnos en nuestro camino, permitiendo tener la fortaleza para culminar esta etapa.

A nuestros padres y familias, por estar presentes en cada etapa de nuestra vida.

De la misma manera, expresamos nuestra gratitud y agradecemos por sus enseñanzas durante el trayecto de nuestra investigación a nuestra asesora metodológica Dra. Olga Alejandra Alcántara Francia y nuestro asesor metodológico Dr. Jorge Alberto Vega Aguilar.

Asimismo, agradecer a nuestros docentes por habernos guiado a lo largo de nuestra carrera universitaria y por habernos brindado el apoyo para desarrollarnos profesionalmente y seguir cultivando valores.

Finalmente, a nuestros verdaderos amigos por darnos fuerzas, palabras de aliento y apoyarnos mutuamente para salir adelante.

ABREVIATURAS

DI	Delitos Informáticos
SDI	Sistemas y Datos Informáticos
TIC	Tecnologías de la Información y la Comunicación
BJ	Bien Jurídico
SI	Sistemas Informáticos
Sc	Secreto de las Comunicaciones
LEDI	Ley de Delitos Informáticos
LSC	Levantamiento del Secreto de las Comunicaciones
CP	Código Penal
CPP	Código Procesal Penal
LECrim	Ley de Enjuiciamiento Criminal
PPL	Pena Privativa de Libertad
MP	Ministerio Público
TC	Tribunal Constitucional

En adelante, las palabras establecidas estarán referidas conforme a sus abreviaturas.

RESUMEN

Para el presente desarrollo de tesis, se planteó como pregunta de investigación: ¿En qué medida la incorporación de los delitos informáticos como supuesto especial dentro del levantamiento del secreto de las comunicaciones facilitaría la investigación realizada por el Ministerio Público a este tipo penal?, teniendo como objetivo general, proponer la incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones el cual facilitaría la investigación del Ministerio Publico y como objetivos específicos, determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones, y analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones. En este sentido durante el desarrollo de la presente investigación se recopilo y estudio información que permita demostrar la hipótesis planteada, para esto se tomó en consideración fuentes doctrinarias, legislación extranjera y estadistas oficiales, utilizando la investigación cualitativa de tipo aplicada, teniendo como técnica de recolección de información la entrevista semiestructurada y como instrumento la guía de entrevista a los participantes, obteniéndose como resultado que la principal dificultad en la investigación de los delitos informáticos, radica en la denegatoria de los requerimientos del levantamiento del secreto de las comunicaciones debido a que estos delitos no cumplen con los presupuestos establecidos por la norma procesal; generando que no existe una tutela efectiva de los bienes jurídicos de los delitos informáticos, debido a que levantamiento resulta ser importante en la investigación para poder identificar al titular de la acción u obtener indicios de la identidad del autor, por lo cual resultaría necesario incorporar los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones.

Palabras Claves: Ciberdelitos, delitos informáticos, levantamiento del secreto de las comunicaciones.

ABSTRACT

For the present development of the thesis, it was posed as a research question: To what extent would the incorporation of computer crimes as a special assumption within the lifting of the secrecy of communications facilitate the investigation carried out by the Public Ministry to this criminal type? As a general objective, to propose the incorporation of computer crimes as a special assumption for the lifting of the secrecy of communications which would facilitate the investigation of the Public Ministry and as specific objectives, to determine that the investigation of computer crimes presents difficulties due to the denial of the lifting the secrecy of communications, and analyzing the foreign criminal law on computer crimes and lifting the secrecy of communications. That is why, during the development of this research, information was collected and studied to demonstrate the hypothesis raised, for this, sources such as doctrinaire, foreign legislation and official statesmen were taken into consideration, using qualitative research of applied type, applying as a technique The semi-structured interview was used to collect information, and as an instrument the interview guide for the participants, from which it was obtained as a result that one of the main difficulties in the investigation of computer crimes lies in the denial of the requirements of the lifting of the secrecy of communications due to the fact that these crimes do not comply with the requirements established by the procedural norm; generating that there is no effective protection of the legal assets of computer crimes, because the survey turns out to be important to be able to identify the owner of the action or obtain indications of the identity of the author, for which it would be necessary to incorporate computer crimes as special assumption for the lifting of the secret of the communications.

Keywords: Cybercrimes, computer crimes, lifting of communications secrecy.

INDICE DE CONTENIDO

INTRODUCCIÓN

La constante evolución de las tecnologías e internet en los últimos años, ha originado que las personas se encuentren interconectadas desde diferentes partes del mundo, adquieran diferentes equipos tecnológicos o digitalicen sus datos personales, existiendo en la actualidad bases de datos virtuales que almacena información básica como nombres, cumpleaños hasta las cuentas bancarias, etc; en ese sentido la digitalización y el avance tecnológico ha llevado a los delincuentes a buscar nuevas modalidades para cometer actos ilícitos, dando origen a la cibercriminalidad, que consiste en aquellas conductas ilícitos que se cometen mediante el uso de las TIC con la finalidad de dañar o vulnerar los datos o sistemas informáticos e incluso utilizando la tecnología como medio para configurar las conductas ilícitas tradicionales. Es así que, el avance tecnológico ha ocasionado que las legislaciones a nivel mundial y la legislación penal peruana presente deficiencias en la regulación de estas nuevas conductas ilícitas y en su investigación, limitando a los fiscales a que encuadren estas nuevas conductas en tipos penales similares con la finalidad de poder continuar con la investigación.

El gran impacto que ha tenido la comisión de estos delitos se ha visto reflejado durante el último año en el Perú debido a la carencia normativa sobre los ciberdelitos y la vulnerabilidad del sistema informático y datos informáticos de las instituciones públicas y empresas privadas; a consecuencia de la pandemia COVID-19 debido a que el Gobierno Peruano durante los meses en que se estableció la inmovilización social obligatoria provocó que miles de peruanos dejen sus labores, por lo cual se otorgó a la ciudadanía el Bono Universal para enfrentar la pandemia, siendo estos bonos otorgados por el Banco de la Nación, provocando que los delincuentes se aprovechen de esta situación sustrayendo el dinero de las cuentas bancarias mediante la modalidad del “Phishing”; evidenciando esta sucesos que aún estamos atrasado en la lucha contra la cibercriminalidad.

Sin embargo, el problema radica en la investigación de este tipo de ilícitos realizada por el fiscal debido a las limitadas herramientas de investigación en este tipo de delitos, siendo la principal limitación la autorización solicitada a los jueces para poder realizar el LSC, en las cuales se obtiene la denegatoria por no cumplir con los presupuestos establecidos en el art. 230 - C.P.P., que el delito debe tener una

pena no menor de 4 años de PPL, dificultando la investigación para poder identificar al imputado provocando el archivamiento de los casos argumentando que no se ha individualizado al imputado; esto se evidencia en el Informe sobre Ciberdelincuencia en el Perú elaborado por el Ministerio Público, en el cual se obtuvo como resultado que la principal dificultad es la denegatoria del LSC por parte del juez, debido a que el delito no cumple con los presupuestos de la norma, frustrando el poder recabar información relevante para identificar al autor del ilícito entre otros elementos de convicción, que serían de vital importancia para la continuación investigación y posterior enjuiciamiento; aunado a ello, el Boletín Estadístico del 2019 emitido por el MP, se constata que de marzo del 2018 a marzo del 2019 han existido un total de 1536 casos registrados en fiscalías provinciales penales y mixtas, de marzo del 2017 a marzo del 2018 existieron 769 delitos informáticos, por lo que tenemos que hubo un incremento de 767 casos más entre 2018 a 2019.

Por lo tanto, ante esta situación existe la necesidad de investigar y dar una solución a la limitación en la investigación de los delitos informáticos, con el objetivo de que se autorice el LSC para la adecuada investigación de los delitos informáticos, por lo que se plateo el siguiente problema: ¿En qué medida la incorporación de los delitos informáticos como supuesto especial dentro del levantamiento del secreto de las comunicaciones facilitaría la investigación realizada por el Ministerio Público a este tipo penal?. De este modo se planteó como objetivo general: Proponer la incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones el cual facilitaría la investigación del Ministerio Publico, del cual se desprendieron como objetivos específicos: a) Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones, y b) Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones; en ese sentido se estableció como hipótesis: La incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones, facilitaría la investigación realizada por el Ministerio Público.

Asimismo, el trabajo está conformado por seis capítulos; I) Ciberdelitos o Delito Informáticos; II) Levantamiento del Secreto de las Comunicaciones; III) Legislación Extranjera sobre los Delitos Informáticos y el Levantamiento del Secreto de las Comunicaciones; IV) Los Delitos Informáticos como supuesto especial del Levantamiento del Secreto de las Comunicaciones; V) Aspectos Metodológicos; y, VI) Resultados y Discusión.

Finalmente, en la presente tesis se han elaborado conclusiones y recomendaciones a las que se establecieron luego de un análisis y estudio del tema materia de investigación.

CAPÍTULO I: LOS CIBERDELITOS

1.1. Aspectos Generales

1.1.1. Origen del Fenómeno Informático

El humano durante los siglos ha buscado la forma de facilitar su actividades diarias, tanto en la forma de poder comunicarse, transmitir información o procesarla; es así que Hernández (2006), señala que el ser humano movido por la necesidad de hallar mecanismos de fácil y rápido acceso, ha creado diversos métodos que ayuden a procesar información, con este fin se dio origen a la informática, la cual es una ciencia encargada de estudiar y desarrollar los métodos y máquinas, con la finalidad de facilitar trabajos rutinarios y repetitivos.

Vega (2010), indica que el Ábaco fue el primer invento creado para administrar abundante información y transmitirla, esta herramienta fue utilizada para el cómputo de las actividades comerciales hace aproximadamente cuatro mil años; por otro lado, refiere que durante el siglo XVII nace la primera concepción de la calculadora por Pascal, con la cual solo se realizaban operaciones básicas (suma y resta), posterior a esto se crea un modelo más complejo capaz de a realizar operaciones complejas, es así que en 1835 se crea una maquina más compleja que realizaba operaciones de carácter analítico, siendo esta el primer precedente de las operaciones que puede realizar una computadora en la actualidad, por otra parte, en Estados Unidos durante 1890 aparece la computadora debido a la necesidad de manejar la información estadística obtenida durante el censo poblacional, por lo que Hollerith elaboro una computadora con capacidad limitada; mientras que en la década de los 70 y 80 surgen los primeros microprocesadores con los cuales se buscaba perfeccionar cada vez más aquellas operaciones y herramientas que actualmente son de parte esencial de las computadoras. (p. 04 - 05)

Para Chiluisa (2021), la constante evolución y el uso de herramientas tecnológicas ha facilitado el desarrollo del ser humano en diferentes áreas, tales como: profesional, educativo académico, comunicativo, laboral, cultural social, las cuales tienen influencia en la vida cotidiana del ser humano; toda vez que la tecnología es útil para ahorrar tiempo y dinero en tramites o procedimientos que antes acarreaban una excesiva tardanza, es por eso que esta revolución tecnológica trajo consigo avances en la vida moderna, por lo cual se requiere para su eficacia que este

supeditada a la aplicación y regulación normativa como base hegemónica en la ciudadanía, en ese sentido la tecnología ha originado significativos avances para la ciencia y a la par ha evolucionado de forma negativa por el mal uso que se le da a esta herramienta. (p. 8)

1.2. Definición del Ciberdelitos

Los ciberdelitos o delitos informáticos a lo largo de los años han tenido diferentes concepciones o definiciones dadas por diversos autores que trataron de explicar esta nueva tendencia delictiva, debido a que cada día estamos expuestos a diversas vulnerabilidades tecnológicas, es así que tenemos a Huerta y Líbano (1982) citado en Acurio (2016), quienes definen a los ciberdelitos como aquellas omisiones u acciones, realizas en contra de la persona natural o jurídica, utilizando un sistema de tratamiento de información destinado a causar daño al bien jurídico del individuo mediante atentados a la técnica informática. (p. 14)

Por otro lado, la Unión Europea (2005), define a los ciberdelitos como aquella delincuencia en la cual se utilizan las tecnologías de comunicación e información, para perjudicar la red o base de datos de información y comunicación, sin tener dificultades geográficas, debido a la circulación de los datos intangibles y volátiles que se encuentran en el ciberespacio. De igual forma, Serrano (2009), señala que se puede utilizar el término de cibercrimen en el sentido tipológico y normativo; en el sentido tipológico lo define como aquel comportamiento que está compuesto por una serie de características criminológicas que se encuentran vinculadas con el ciberespacio, mientras que en el sentido normativo este término se utiliza para identificar o enmarcar un tipo penal que se realiza en el ciberespacio y que vulnera los bienes jurídicos protegidos por la norma. (pp. 39 - 40)

Mientras que Romeo (2006), señala que es un conjunto de conductas ilícitas que se realizan a través de las TIC, siendo estas conductas: el acceso, intercambio, apropiación o la disposición de información de la red telemática, siendo este su lugar comisivo; dichas conductas se perpetran sin el consentimiento de la persona natural o jurídica, afectando los bienes jurídicos individuales o colectivos. (p. 09)

Por otra parte, Tabares (2010), señala que es aquella conducta que se produce mediante el uso de la informática o sus técnicas, o como aquel comportamiento criminal en el cual se utiliza una computadora como medio comisivo, como material

u objeto de acción delictiva, en conclusión, define a los ciberdelitos como cualquier conducta criminal en la cual se haga uso de la tecnología electrónica e informática, siendo utilizada como método, medio o fin para la comisión del ilícito.

Por otro lado, Vega (2010), señala que la definición más apropiada para esta nueva data de delitos es el término de Criminalidad Informática, ya que estos ilícitos son modalidades innovadoras de criminalidad, que afectan los bienes jurídicos amparados en la legislación penal peruana. (p. 40) De igual forma, Acurio (2016), señala que los DI, son las conductas o actos de carácter criminal, con la finalidad de alterar, destruir, socavar o manipular los sistemas informáticos o sus componentes, teniendo como finalidad dañar o perjudicar los bienes jurídicos. (p. 14)

Mientras que Miro (2012), define al cibercrimen como aquella conducta que se realiza en una dimensión virtual en espacio y tiempo diferente, caracterizándose este tipo de delitos por su transnacionalidad y su universalización debido a la evolución constante del ciberespacio; por consiguiente, el autor señala como cibercrimen puede ser un delito tradicional en donde las TIC jueguen un papel importante para su comisión.

“Los delitos informáticos, son aquellos delitos tradicionales en donde las TIC se utilizan como herramienta para su comisión, objetivo de un delito, o un dispositivo de almacenamiento.” (Levin y Ilkina, 2013, p. 14).

Los autores Martinez y Abreu (2015), definen a los ciberdelitos como aquellas acciones, que se realizan mediante la informática o tiene como finalidad dañar o destruir ordenadores, las redes de Internet y medios electrónicos, asimismo, señalan que existen conductas criminales que no pueden ser consideradas delitos debido a que la tecnología e informática evoluciona constantemente dificultando a los legisladores plantear nuevas normas penales que abarquen las nuevas modalidades de ilícitos.

Rayon y Gómez (2014), definen a los ciberdelitos como aquella infracción punible, que puede ser una falta o un delito, en el cual se utiliza el internet o un equipo, para la comisión de un hecho ilícito o que pueda ser objeto del mismo delito.

Para Castellanos (2020), son aquellas actividades ilícitas relacionadas con el uso de las TIC, que buscan perjudicar la confidencialidad, integridad y disponibilidad de la información que forma parte del ciberespacio; asimismo, para Villavicencio (2014), los ciberdelitos son conductas dirigidas a vulnerar los sistemas de seguridad de los dispositivos, mediante la intromisión a correos, computadoras o base de datos mediante el uso de claves de acceso; precisando que son delitos tradicionales que solo se pueden ser cometer mediante la tecnología" (p. 286)

Aguilera (2009), definió al delito Informático como toda acción u omisión culpable realizada por el ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena.

Finalmente, para Loredo (2017), los DI son aquellas acciones dolosas que realiza un individuo, ocasionando perjuicio a las plataformas virtuales o tecnológicas que utilizan las personas o las entidades, pero que dichos actos no necesariamente deben conllevar a un beneficio para el autor del ilícito. (p.15).

1.3. Clasificación del Cibercrimen

El avance de las TIC ha originado que se creen nuevas conductas ilícitas y que las existentes se puedan configurar mediante la utilización de estas, en ese sentido se busca clasificar aquellas conductas como:

1.3.1. Ciberataques Puros

Los ciberataques puros para Cano (2020) son todas aquellas conductas delictivas de nueva creación que únicamente se pueden realizar mediante el uso de las TIC como medio de comisión, tratándose de acciones específicas que no presentan una modalidad en el mundo físico, sin perjuicio de poder incluir determinadas conductas en tipos penales tradicionales. Mientras que, Miró (2012) nos dice que el ciberespacio y las TIC, han supuesto el nacimiento de nuevos bienes y servicios que tienen un valor económico y social, en consecuencia, se han originado nuevas conductas que solo pueden realizarse mediante el uso de las TIC, en ese sentido ha surgido un conjunto de comportamientos ilícitas que se caracterizan por

perjudicar los servicios, terminales o bienes que operen en el ciberespacio; denominándose a estos como ciberdelitos puros debido a que solo se realizan en el ciberespacio. (pp. 52-53)

A. El Hacking

Miro (2012), nos dice que el Hacking, es aquel acceso ilícito a los sistemas que contienen información, que es denominado como violación de datos, que consiste en modificar, destruir o acceder a los datos informáticos de una empresa, superando barreras informáticas para el acceso a un sistema, o configuración de un programa funcional, siendo esta su concepción más amplia, mientras que en su concepción estricta, es conocida como intrusismo informático, conducta que vulnera la esfera de exclusividad del titular del sistema informático, no importando si el agente tiene acceso a la información contenida en el sistema; concluyendo así que el hacking consiste en acceder al sistema y a los datos, sin el propósito de producir un daño.

Mientras que para Vega (2010), define como hacking el ingresar a un sistema o su interferencia con la finalidad de apoderarse, conocer o usar de forma indebida la información contenida en esta. (p. 101). Por otra parte, Cano (2020), señala que el hacking es aquel acceso ilegítimo a un sistema informático con el fin de obtener información.

B. Infecciones de malware y otras formas de sabotaje cibernético

a. Malware

Las infecciones de malware según Miro (2012), consiste en enviar virus informáticos a través de redes telemáticas que utilizan la red para multiplicarse y acceder a terminales, causando un perjuicio a dichas terminales, en otras palabras, es probable que el daño a la red afecte el propio sistema informático y otros elementos hardware que lo constituyen y tienen valor económico; por la información contenida en el sistema anterior, y que pueda tener valor económico o personal para el titular. (p. 57).

Por otra parte, Cano (2020), define a los malware como aquellos softwares maliciosos, que tienen por finalidad sabotear el funcionamiento de un sistema informático, este tipo de ataques pueden afectar a una persona natural o jurídica

comprometiendo sus datos y servicios, que causan repercusiones económicas, otra modalidad de malware es mediante la creación de botnets, conocidos como un conjunto de sistemas infectados que sirven para lanzar ataques coordinados. Asimismo, OECD (2008), nos dice que existen distintas modalidades de software maliciosos que tratan de arruinar un sistema o su información, siendo estos los worms o troyanos, los botnets o los rootkits, los keystroke loggers o spyware. (p.15).

b. Ataque DoS

Para Miro (2012), consiste en ataques de denegación de servicios, los cuales mediante la utilización de técnicas que impiden cargar los recursos del ordenador o negar el acceso del servidor a otros sistemas informáticos. (p. 63)

Por otra parte, Fernández (2007), señala que el objetivo de los ataques de DoS es saturar el servidor del sistema para lograr que el individuo se centre en la solicitud que realiza el agente sin poder continuar con el común funcionamiento del sistema, produciendo así la denegación de servicios; estos ataques se manifiestan mediante el envió de un mensaje que interviene en el normal funcionamiento del sistema, estos ataques se pueden dar mediante dos modalidades como: el ataque de vulnerabilidad o ataque de inundación. (p.63) De igual forma, Amazon (2021), señala que es un intento malicioso de afectar el funcionamiento del sistema, generando diversos paquetes o requerimientos con la finalidad de sobrecargar el sistema objetivo, en este tipo de ataques se utiliza múltiples fuentes de vulnerabilidad o controladas.

c. Spam

Yeargain, Settoon y McKay (2004), es aquel correo electrónico no solicitado que se envía a diversas direcciones electrónicas mediante direcciones electrónicas o desde un sistema informático infectado, que se convirtió en bot e integra una botnet que es utilizado por el agente que tiene acceso a estas direcciones hackeando los sistemas informáticos o la Red; el spam tiene por finalidad enviar publicaciones ilícitas o infectar el sistema a causa de un malware, intentando cometer el ilícito de phishing.(p. 15) En todo caso, Miro (2012), señala que el spam, es un ataque a una terminal y a su normal funcionamiento, incrementando la posibilidad de infectar mediante un malware que será utilizado para defraudar al sujeto pasivo. (p. 66)

C. Ocupación o uso de redes sin autorización

Según Miro (2012), es el ataque directo que consistiendo en utilizar una terminal de comunicación, esto es debido la facilidad de conexión con las redes de Internet conocida como WIFI, o de las telecomunicaciones, los servicios, la difusión de contenidos en las telecomunicaciones, son afectadas por la piratería de señales de transmisión de radio, televisión e Internet, que se instalan en los sistemas informáticos mediante la creación de software específico para establecer una conexión a las antenas o duplicando claves, poniendo en peligro los intereses comerciales difusión de contenidos digitales. (p. 67)

1.3.2. Ciberataques Replica

Los ciberataques replica según Miró (2012), son aquellas acciones que no requieren un mundo físico solo para realizarse, sino que también pueden cometerse mediante las TIC a través del ciberespacio, estas conductas son las que comprenden los ciberdelitos réplica, consistiendo en la realización de delitos tradicionales a través de las redes, en este caso el ataque se ejecuta a través de la Red, siendo este un nuevo medio comisivo; sin embargo, debido al nuevo ámbito de realización criminal produce que se cree una nueva conducta. (p.68)

A. Ciberfraudes

Dentro de esta modalidad de ilícito según Miro (2012), ingresan aquellos fraudes de Internet, que son cometidos mediante el uso de las TIC para obtener un beneficio económico producto de un perjuicio económico a una víctima, existiendo diversas modalidades, las cuales pueden ser el acceso a la información sobre el patrimonio de una persona, empleando diversas formas de relación comercial del ciberespacio, las debilidades de seguridad de los sistemas informáticos facilitando el acceso patrimonial, al contener claves o datos bancarios de los usuarios. (p. 69) Stadler (2010), plantea diversas formas de fraude tales como: fraudes a tarjetas de crédito, cheques, las estafas piramidales, estafas de lotería, las ventas en línea, las estafas de inversión, ataques de scam. (p. 492 - 493)

a. Ciberfraudes burdos o scam

Según Yar (2005), es aquel envío de correos electrónicos con el nombre de scam, siendo estafas en las que el medio es el uso del internet, correo electrónico o las redes sociales. (p. 81).

Shadel (2012), señala que es aquel engaño poco elaborado y en el que la víctima cae en error, caracterizada por inducir interés en la víctima o ganarse su confianza, con el fin de que la propia víctima ponga a disposición su patrimonio, en ese sentido, pese a que los sistemas técnicos con los niveles de protección a nivel de hardware y software hayan evolucionado siendo cada día más seguros, en este tipo de delitos el sujeto pasivo es quien se pone en una situación de vulnerabilidad para que el engaño tenga éxito.

b. Phishing

Jakobsson (2005) señala que el avance de los sistemas de seguridad de la banca electrónica ha originado que el ciberdelincuente dirija sus ataques para obtener información secreta, mediante los spyware o malware o gracias a la intervención del propio sujeto, para posteriormente utilizar dicha información haciéndose pasar por el usuario para obtener un beneficio patrimonial.

Mientras que, Jaishankar (2008), señala que es un mecanismo criminal que utiliza la ingeniería social y técnicos, con la finalidad de sustraer información sobre la identidad del consumidor, tarjetas de crédito o cuentas bancarias. (p.12)

El típico ataque del phishing está compuesto por: el mensaje, interacción y robo: consiste en que la víctima recibe un mensaje a través del medio electrónico, remitido por el agente, siendo este un correo electrónico, VoIP, mensaje en una red social o en videojuegos con diversos participantes. (Hong, 2012, p.74).

c. Ciberblanqueo de capitales y ciberextorsión

Miro (2012), señala que existen diversas maneras para lavar dinero de forma virtual, siendo las más típicas son el uso de mulas para el envío de dinero y el logro de divisas a través de los juegos en línea, en el caso de las mulas en el campo del phishing, se refiere a los usuarios de Internet que poseen o abren una cuenta bancaria y son reclutados en línea bajo la apariencia de un contrato de trabajo realizado en casa, que incluye recibir dinero en sus cuentas bancarias que luego

son envías a las cuentas corrientes del delincuentes, y en los juegos en línea, consiste en la creación de una economía virtual en la que se intercambia moneda real por moneda virtual para participar en el juego, con la finalidad de ser cambia a moneda real posteriormente. En cuanto, a la ciberextorsión el ciberespacio se convierte en un nuevo medio de intimidación, que puede resultar ser fácil e incluso beneficioso para aprovechar el hecho de que la víctima obedece la solicitud del delincuente sin ser atacada, estas conductas suelen estar relacionadas con páginas web dedicadas a las apuestas y juegos de azar online que están interesadas en pagar una pequeña cantidad a la mafia a cambio de no ser objeto de denegación de servicio o ataque similar en determinadas circunstancias. (p. 83)

d. Ciberacoso

Miro (2012), señala que se puede amenazar, coaccionar, difamar y agredir el honor o la libertad de una persona a través del ciberespacio, el ciberacoso es una categoría amplia de todos los comportamientos, donde se utilizan diferentes herramientas de comunicación, como Messenger, correos electrónicos, Skype, Twitter o Facebook u otras redes sociales. (p. 84)

e. Cyberstalking

El cyberstalking según Basu y Jones (2007), define aquella acción mediante la cual se hostiga, persigue o amenaza a alguien utilizando las TIC. (p. 13)

Por su parte, Miro (2012), manifiesta que la dinámica del stalking mediante el uso de las TIC consiste en un conjunto de conductas tales como el envío correos o mensajes mediante las redes sociales, al acceso de fotos, mensajes o correos de la víctima en páginas web, usualmente se elige a la víctima a través de chats, foros; los medios más comunes de cyberstalking son: el correo electrónico donde se puede enviar mensajes de acoso o amenaza u odio, mensajes obscenos o incluir imágenes hirientes, o instar a usuarios de Internet a acosar o amenazar a la víctima mediante fotos o chats, enviar archivos infectados con la intención de dañar los sistemas informáticos de la víctima y el robo de identidad, el tiempo de comisión de estos ilícitos son amplios debido a que el agente puede enviar un correo electrónico amenazante pero la victima puede leerlo días después. (pp. 89-90).

Por otra parte, Henson (2010), señala que el cyberstalking consiste en aquella conducta en usa un equipo de comunicación electrónica, deliberada y voluntariamente para realizar actos con un propósito ilícito, siendo los siguientes: contactar o intentar entablar comunicación con alguien después de pedirle que deje de contactar, acosar, torturar o intimidar; robos o intentos de robos de la identidad de alguien o dañar su información; hacer provocaciones sexuales innecesarias o infundadas y amenazar con causar daño físico a alguien. (p. 254)

1.3.3. Ciberataques de contenido

Miró (2012), nos menciona que se debe considerar que el internet funciona de forma simultánea tanto como medio de comunicación, en el sentido que la comunicación entre emisor y receptor se va a difuminar en el espacio informático, de forma que un usuario puede terminar siendo un comunicador o productor de contenidos de lo que era un receptor, es por ello que se debe tener en consideración que el Internet se ha popularizado y hay una gran facilidad para acceder como para enviar información, el uso que podrían darle los menores a este sistema de comunicación, deduciéndose así que desde hace ya más de diez años ha surgido una evidente inquietud por los contenidos, debido a la aparición de un conjunto de diversas conductas ilegales y no por el medio que se usó sino por el contenido que se ha distribuido por el Internet. (p. 100-101)

A. Ciberpiratería Intelectual

La ciberpiratería intelectual según Miró (2012), se origina debido al aumento del valor de los bienes en una sociedad de información, por la potencialidad de las TIC que son medios de difusión o por materializarse en diversos softwares con el mismo valor, convirtiéndose en bienes económicamente importantes, surgiendo la explotación ilegal de obras protegidas, siendo estas la venta de forma directa de obras digitalizadas, la comunicación pública vía streaming a cambio de una suma de dinero, en ese sentido las TIC han dado lugar a diversas conductas que perjudican los derechos de propiedad intelectual. (p. 104)

B. Pornografía Infantil en Internet

Con respecto a la pornografía infantil en internet, Miró (2012), señala que la definición que facilita la INTERPOL, como forma de representación o promoción de

la explotación sexual de los niños, incluyendo material escrito u audios, que se concentren tanto como en la conducta sexual o en los órganos genitales de los menores, esta última descripción se aproxima mejor a los diversos tipos de comportamientos que se pueden incluir dentro del macro concepto de pornografía de menores, siendo un fenómeno que a pesar de no ser meramente informático va a estar vinculado al uso de las nuevas tecnologías, hasta el punto de que en nuestra actualidad desde una perspectiva criminológica puede decirse que en su mayoría estos comportamientos van a realizarse básicamente a través del uso de Internet. (p. 106, 107)

C. Online Hate Speech

Miró (2012), citando a Romeo Casabona manifiesta que la pornografía de menores no va a ser el único contenido ilegal que se puede difundir a través de la Red, ya que, la posibilidad de encajar información en la Red con diversos contenidos ilícitos y difundirlos a través de ella, ha convertido a la Red en un medio potente para que se comentan delitos como la apología terrorista, este tipo de delito informático (ciberterrorismo) consiste en la difusión de mensajes de incitación a la violencia en un ámbito terrorista. (p. 114)

Por otra parte, Miro (2012), señala que cyberhate speech o incitación al odio étnico en el ciberespacio, es un ilícito que consiste en el atacar a una persona o un grupo utilizando información sobre su religión, raza, creencias, genero u orientación sexual o discapacidad, incrementándose esta conducta debido a que se configura en el ciberespacio, por lo que existe el ámbito transnacional y mundial, siendo un lugar peligroso para difundir mensajes racistas y violentos, que se vierten con más facilidad en Internet ante la dificultad de perseguir a la cibercriminalidad.

Como señalan Keats y Norton (2011), que la red permite sustituir prospectos y folletos racistas que antes eran difundidos de forma física, siendo ahora compartidos mediante las webs o blogs de fácil alcance y que resultan más eficaces para transmitir ideas odiosas a la sociedad. (p. 1435)

1.4. Perfil del Ciberdelincuente

El ciberdelincuente según Villavicencio (2014), debe tener ciertas habilidades y conocimientos en el manejo del sistema informático, caracterizándose estas como:

tener conocimientos informáticos u ocupar lugares estratégicos en los lugares donde desarrollan sus laborales, manejando información clasificada o el acceso al sistema, sin embargo, no están excluidos los individuos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática, por lo que se tratan de delitos de dominio. Para Manson (2013), los ciberdelincuentes no son delincuentes comunes y corrientes, sino que son personas con alto coeficiente de la informática, poseyendo habilidades para el manejo y uso de los sistemas informáticos que por su situación laboran lugares estratégicos manejando información sensible.

1.4.1. Hackers

Los Hacker para Belcic (2021), es alguien que aplica sus conocimientos y habilidades informáticas a la resolución de un problema, encontrando tres tipos de hackers:

- Hackers de sombrero negro, es aquel que rompe los sistemas de ciberseguridad para acceder ilegalmente a un equipo o una red, con la finalidad de obtener un beneficio patrimonial, ya sea mediante la venta de información comprometida o la extorsión, o simplemente causar un caos en el sistema.
- Hackers de sombrero blanco, son aquellos que cuentan con habilidades en la informática, pero en lugar de dañar el sistema o datos informáticos, busca encontrar sus puntos débiles para reforzar su seguridad, este tipo de hacker realizan las defensas digitales de las empresas, por lo cual ingresan de manera intencionada a un sistema, con permiso de su propietario, para identificar los puntos débiles que hay que reparar.
- Hackers de sombrero gris, buscan debilidades de los sistemas y luego establecen una comunicación con las empresas titulares de los sistemas, para ofrecer sus servicios, por una compensación económica, otros hackean a las empresas para obligarlas a tomar acciones contra una determinada debilidad.

Para Villavicencio (2014), son personas que se comprometen a violar los llamados procedimientos y sistemas impermeables por aficiones u otros intereses, les gusta investigar por todas partes para entender cómo funcionan los sistemas informáticos; son personas que utilizan esta actividad como un desafío intelectual, cuyo único propósito es descifrar y comprender el sistema informático sin causar

ningún daño, los hackers son individuos que sin contar con acceso de un sistema, acceden a estos sin la intención de querer causar un perjuicio o manipulación, fraude, espionaje o sabotaje, sino solo para entretenimiento no autorizado. (p. 08)

De igual modo, Long (2010), diferencia entre white hat hacker, hackers éticos o crackers, siendo los primeros aquellos que cuentan con autorización para probar, revisar o modificar los sistemas informáticos teniendo la finalidad de detectar vulnerabilidades para luego crear y aplicar medidas de seguridad; mientras que los segundos acceden al sistema con el fin de robar o destruir información, cometer fraudes y generar un perjuicio actuando de manera ilícita.

1.4.2. Crackers

Villavicencio (2014), señala que son aquellas personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios, y causar problemas a los sistemas, procesadores o redes informáticas, estos individuos son conocidos como piratas electrónicos; los crackers usan programas ya creados que pueden adquirir vía internet o pueden crearlos; mientras que los hackers crean sus propios programas, debido al conocimiento sobre los programas y los lenguajes informáticos que poseen. (p. 09) Del mismo modo, Belcic (2020), manifiesta que los hackers crean y los crackers destruyen, en ese sentido el cracker tiene por objetivo causar un daño como: robar datos, suplantar a alguien o incluso usar software de pago gratis.

Por otra parte, Vega (2010), indica que es aquel individuo que tiene la capacidad de romper sistemas y software, dedicándose exclusivamente a crackear sistemas, siendo estos los más peligrosos debido a que se encargan de difundir la información o la vulnerarla a través de la red para conocimientos de otros. (p. 24).

Finalmente Miro (2012), señala que son aquellos que utilizan el acceso informático para robar información relevante o buscan causar un perjuicio, pueden actuar de forma solitaria o pueden ser captados por mafias organizadas para realizar actividades ilícitas en el ciberespacio, o pueden formar grupos transnacionales dedicados a realizar conductas delictivas a través del uso de las TIC. (p.235-236)

1.5. Bienes Jurídicos vulnerados por los delitos informáticos

Villavicencio (2014), señala que el bien jurídico protegido es principalmente la información o informática de forma genérica, o los bienes jurídicos tradicionales como la indemnidad o libertad sexual, intimidad, patrimonio, seguridad nacional, etc; como información se puede entender al contenido de las bases o banco de datas o el producto que almacena información; por lo tanto se constituye en un bien autónomo con valor dinerario y es la importancia del valor económico de la información lo que permite que se incorpore como bien jurídico protegido; sin embargo, la información no solo tiene un valor económico, sino que posee un valor intrínseco de la persona por el trafico jurídico y la fluidez, y por los sistemas que lo van a procesar o automatizar a los mismos que equiparan a los bienes tutelados tradicionales tales como la intimidad, el patrimonio y la confidencialidad de los datos, seguridad; por lo tanto, en este tipo de delitos la información es el principal BJ y existen diversos bienes jurídicos que también pueden ser perjudicados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. (pp. 06-07)

Por otra parte, Vega (2010), resalta que el estudio de los BJ en este nuevo tipo de delitos, en ese sentido señala que es todo aquel BJ que se va a encontrar protegido o amparado dentro de los diversos aspectos del derecho; asimismo, se va a emplear en el derecho penal para referirnos al interés protegido frente a la comisión de ilícitos, llamados como bien jurídico protegido o bien jurídico tutelado, de igual forma se puede afirmar que el bien jurídico protegido surge como consecuencia de los intentos por controlar el desmedido crecimiento del derecho penal, debido a que no hay manera como limitar las conductas pertinentes para proteger a la sociedad como ultima ratio; finalmente hallamos que con relación a los bienes jurídicos tutelados en los delitos informáticos afectan tanto bienes jurídicos individuales como bienes jurídicos colectivos, y que el delito informático es un delito pluriofensivo, ya que lesiona más de un bien jurídico. (p. 46)

Al respecto Reyna (2001) señala que el bien jurídico penal protegido va a ser la información como valor económico de empresa, el mismo que cumple con las exigencias de merecimiento de protección y necesidad de tutela; y que no solo constituye un interés social vital. (p. 252)

1.6. El Estado peruano frente a los delitos informáticos

El Estado peruano ante el avance tecnológico y el gran impacto que ha tenido este en la criminalidad, se vio en la necesidad de crear normas que permitan sancionar aquellas nuevas conductas que se realizaban mediante el uso de las TIC, es así que el legislador en el año 1991 busco incorporar estos nuevos comportamientos dentro del Código Penal, como una regulación innovadora y la vanguardia de la nuevas formas de criminalidad; posteriormente en el 2000 a través de la Ley N° 27309, se incorpora en el CP los primero delitos informáticos, de este modo el legislador consideró pertinente modificar y agravar algunos delitos amparados en la normatividad penal existente adecuándolas a las TIC. Sin embargo, dichos articulados no cumplían con la verdadera esencia de los delitos informáticos, por lo tanto, el legislador se vio en la necesidad de promulgar una ley que abarcara los parámetros establecidos por el Convenio de Budapest, dando sí el nacimiento de la Ley N° 30096 que fue modificada por la Ley N° 30171 debido a deficiente y ambigua de la primera; en ese sentido se debe conocer de forma detallada cada avance normativo que tuvo la legislación peruana rumbo a la actual normatividad de los delitos informáticos.

1.6.1. Delitos Informáticos en el Código Penal Peruano

La regulación de los DI tuvo su primera aparición en el CP de 1991, como lo indica Salinas (2013), al incorporarse el Hurto Telemático como aquella conducta que se realizará mediante uso de sistemas de transferencia electrónica de fondos, telemática o violaciones al uso de claves estará sujeto a una sanción gratuita de no menos de 3 a 6 años, o una multa de días (pp. 1300-1301).

Asimismo, en el año 2000 el legislador impulso la tipificación de nuevas conductas ilícitas, incorporando al código un capítulo dedicado a los DI, comprendiendo los artículos 207-A, 207-B y 207-C, teniendo como bien jurídico al patrimonio, encontrándose regulados en los delitos contra el patrimonio; siendo estos según Pastor (2015):

A. Espionaje Informático – Articulo 207-A

El cual prescribía el hacking como aquella conducta de ingresar o utilizar sin permiso un sistema, una red o una base de datos, para alterar, diseñar o

ejecutar algún esquema, con la finalidad de interceptar, interferir, acceder o copiar información almacenada en una base de datos, teniendo una sanción no menor de 02 años; o teniendo como pena no mayor de 03 años en su agravante si el agente buscaba obtener un beneficio económico. En este delito se tenía en consideración que el delincuente, puede ser cualquier individuo que realice este accionar, mientras que el agraviado puede ser una persona natural o jurídica, teniendo como modalidades la descritas en el primer párrafo, siendo un delito completamente doloso, que no requiere resultado lesivo, con respecto a sus penas estas pueden ser de carácter suspendido o reserva de fallo. (pp. 53-55)

B. Sabotaje – Articulo 207-B

Este delito sancionaba a aquel que utilizaba, ingresaba o interfería sin autorización en una red, programa computacional o base de datos, con el objetivo de alterar, dañar o destruir esta, teniendo como sanción una pena menor de 03 ni superior de 05 o días multa; siendo el agente cualquier individuo, y el agraviado aquella individuo o empresa que es titular del sistema, base de datos, red, ordenador o programa, es un delito doloso, que no requiere un resultado lesivo, debido a la pena esta puede ser de carácter suspendido o efectiva, sin embargo este tipo penal presentaba dificultades al momento de su probanza debido a que solo se requería que el sujeto ingresara con animus de dañar o violentar, siendo esto difícil de probar. (pp. 56-58)

C. Modalidad Agravada – Articulo 207-C

En este artículo se plasmaron aquellas agravantes de los dos primeros artículos antes mencionados, teniendo una sanción no menor de 05 ni superior de 07 años, cuando el agente acceda a un sistema, red o base de datos, haciendo uso de información clasificada que manejaba debido a la función que realizaba, o cuando se ponga en peligro la seguridad nacional; en el primer agravante el sujeto activo tiene una cualidad debido a la función de su cargo que desempeñaba, mientras que en el segundo agravante el sujeto no requiere una cualidad. (pp. 58-60)

Por otra parte, Elias (2014) señala que la incorporación de los artículos anteriormente mencionados presentaros problemas tales como:

a. El parlamentario identificaba a los ciberdelitos con el fraude informático, por lo cual encuadro hecho dentro de los delitos contra el patrimonio, en razón a que se creía que estas nuevas conductas ilícitas eran una simple extensión de los previsto en el agravante del Hurto, conocido como hurto telemático, siendo el principal bien jurídico el patrimonio. Es por eso que, el agrupar dentro de un solo Capítulo comportamientos que protegen diversos bienes jurídicos generó un grave error.
b. La segunda controversia de estos ilícitos es que fueron considerados como delitos de peligro debido que el bien jurídico protegido era el patrimonio, en ese sentido no se requería el resultado para configurarse un delito informático, pues solo bastaba la intención; creando el legislador una paradoja al tipificar los delitos informáticos como delitos contra el patrimonio, debido a que el solo ingreso en la base de datos no era un hecho punible al no poner en riesgo o lesionar el patrimonio del titular. En ese sentido, se debió reconocer que en los delitos informáticos se protege los derechos informáticos.
c. El tercer problema radica en que el legislador decidió sancionar estas conductas empleando al Derecho Penal como prima ratio, pues no busco la vía más adecuada para sancionar comportamientos que debido a la gravedad no necesitan un mayor reproche punitivo, asimismo, el legislador se lanzó a promulgar nuevas leyes sin contar como una capacitación y personal especializado que permitan facilitar la investigación y persecución de los DI.
d. Posteriormente, a la incorporación de los DI en el CP, los congresistas durante cada periodo legislativo presentaron diversos proyectos, con la finalidad de tipificar nuevas modalidades delictivas, subir las penas, adecuar la redacción legislativa de los tipos penales a los parámetros establecidos a nivel internacional.
e. Finalmente, en el 2013 se incorporó el tráfico ilegal de datos al C.P., por la Ley No. 30076, la cual fue promulgada con el fin de luchar contra la inseguridad ciudadana. (pp. 5-8)

Sin embargo, en la actualidad aún existen en el Código Penal (2021), algunos ilícitos en los cuales se emplea las TIC como medio comisivo de otros delitos, tales como:

a. La pornografía infantil – Art.129-M, teniendo como agravante el utilizar las TIC para difundir dicho material pornográfico.
b. En el Capítulo I de los delitos contra los derechos de autor y conexos regulados en los art. 220-A, art. 220-B y art. 220-C.
c. Penalizan la clonación o modificación de las terminales de telefonía celular actualmente regulada en el Art. 222-A, este hecho fue tipificado debido al alto índice de hurto de celulares, lo cuales podrían ser utilizados por delincuentes para cometer otros delitos.
d. La apología al terrorismo regulada actualmente en el art. 316-A, configurando como circunstancia agravante cuando la apología al terrorismo se difunde mediante el uso de las TI.
e. El indebido ingreso de artefactos tecnológicos en los centros penitenciarios u otros, regulados en los art. 368 - A y B, estos delitos fueron incorporados en la legislación penal con el fin de luchar con los delitos cometidos o direccionados de los centros penitenciarios.

Finalmente, el legislador se dio cuenta que tenía la necesidad de regular los DI en una ley especial, para brindar una especial protección a los sistemas y datos informáticos al considerarlos un BJ, y proteger aquellos bienes afectados mediante el uso de las TIC.

1.6.2. Los Delitos Informáticos regulados en la Ley N° 30096

El legislador debido a la necesidad de adaptar la normatividad penal a los avances tecnológicos y los fenómenos producidos por este, opto por promulgar una ley especial, en un primer momento la Ley N° 30096 el 22 de Octubre del 2013, siendo conocida en la actualidad como la LEDI, compuesta por siete Capítulos.

Ley N° 30096 (2013), cuenta con:

- Capítulo I: En el referido capítulo se establece el fin y objeto de la norma, el cual consiste en prevenir y sancionar aquellos comportamientos ilícitos que vulneran los datos y sistemas informáticos, o aquellos bienes jurídicos que

tengan relevancia penal, los cuales se pueden realizar mediante el uso de las TIC.

- Capítulo II: Regula:
    - Acceso Ilícito – Artículo 2, sancionando a aquella persona que ingresa sin consentimiento a un sistema informático, teniendo como pena no menor de 01 ni superior de 04 años, y con días multas.
    - Atentado con la integridad de datos informáticos – Artículo 3, sanciona a aquel que mediante el uso de las TIC busca dañar los datos informáticos, con una pena no menor de 03 ni superior de 06, y con días multa.
    - Atentado contra la integridad de SI – Art. 4, sanciona aquel que mediante el uso de las TIC causa un perjuicio total o parcial a un sistema informático, con una pena no menor de 03 ni superior de 06, y con días multa.
- Capítulo III: Regula los delitos contra la indemnidad y libertad sexual, sancionando a aquella persona que mediante el uso de las TIC establece contacto con una menor de edad, con el fin de obtener material pornográfico, o favores sexuales, con una pena no menor de 04 ni superior de 08, e inhabilitación. Por otro lado, sanciona con una pena no menor de 03 ni mayor de 06 años, si la parte agraviada tiene entre 14 y 18 años de edad.
- Capítulo IV: Regula los delitos:
    - Tráfico Ilegal de Datos – Artículo 06, que sanciona aquella conducta de ingresar o usar la base de datos de un individuo o una entidad privada, con la finalidad de comercializar dicha información, con una pena no menor de 03 ni superior de 05 años.
    - Interceptación de datos informáticos – Art. 7, sanciona al sujeto que mediante el uso de las TIC obstruye datos informáticos dirigidos, originadas o efectuadas en un sistema informático, o las emisiones electromagnéticas que transportan datos informáticos de un sistema informático, con una pena no menor de 03 ni superior de 06. Asimismo, sus agravantes son: cuando los datos informáticos se encuentren clasificados como secreta, o cuando el delito descrito en el párrafo anterior ponga en peligro la seguridad nacional.

- Capítulo V: Regula el Fraude Informático – Art 8, sanciona al que mediante el uso de las TIC pretende un provecho ilícito en perjuicio de un tercero alterando los datos informáticos o interfiriendo en el funcionamiento de un sistema informático, con una pena no menor de 03 ni mayor de 08 y con días multa, o con una pena de no menor de 05 ni mayor de 10 años, cuando el patrimonio del estado se vio afectado.
- Capítulo VI: Regula la suplantación de identidad – art. 9, sancionando al que utilizando las TIC reemplaza la identidad de una persona natural o jurídica, con la finalidad de generar un perjuicio.
- Capítulo VII: En este acápite se plasmaron las siguientes disposiciones:
    - Disposiciones Comunes: Regula el Abuso de mecanismos y dispositivos informáticos; y establece las agravantes aplicables a los delitos de la mencionada ley, siendo el agravante la cualidad del agente que comete el delito.
    - Disposiciones Complementarias Finales: Comprenden la codificación de la pornografía infantil, el Agente encubierto en los delitos informáticos, la coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público, Cooperación Operativa, Capacitación para los operadores de justicia, las medidas de seguridad, las buenas practicas entre el Estado Peruano y otros Estados, los Convenios multilaterales, la terminología de datos y sistemas informáticos, la regulación e imposición de multas por la SBS y AFP, y la regulación e imposición de multas por OSIPTEL.
    - Disposiciones Complementarias Modificatorias: Aquí se plasmaron las siguientes modificatorias:
        - Modifica el art. 1 - Ley 27697, incorporando los delitos informaticos.
        - Modifica el inciso 9 del art. 3 – Ley contra el Crimen Organizado.
        - Modifica los artículos del CPP: el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473.
        - Modifica los art. 162, 183-A y 323 del CP.

- En la Disposición Derogatoria, se derogó el intento fallido del legislador al regular DI en el CP de 1991 y los delitos incorporados en el año 200, derogándose el numeral 4 del segundo párrafo del art. 186 y los art. 207-A, -B, -C y -D el C.P.

Sin embargo, la ley de delitos informáticos aun necesitaba adecuarse a los estándares establecidos en el Convenio de Budapest, por lo que casi un año después de su promulgo la Ley N° 30171.

1.6.3. Ley N° 30171 que modifica la ley de delitos informáticos

Seis meses después de la promulgación de la Ley N° 30096, el legislador aún se vio en la necesidad de adecuar dicha ley siguiendo los parámetros establecidos en el Convenio sobre Cibercriminalidad, por lo cual se optó por modificar diversos articulados que a la actualidad se encuentran vigentes.

Ley N° 30171 (2014), cuenta con las siguientes modificatorias, incorporaciones y derogatorias:

- En el artículo 1 se plantean las modificaciones a los art. 2, 3, 4, 5, 7, 8 y 10 de la LEDI, incorporando a la redacción ya establecidas la posibilidad de realizar el hecho delictivo de forma deliberada o ilegítimamente.
  - Acceso Ilícito – Artículo 2, sancionando al que deliberadamente e ilegítimamente ingresa sin consentimiento a un sistema informático.
  - Atentado con la integridad de datos informáticos – Artículo 3, sanciona al que deliberadamente e ilegítimamente causa un perjuicio a los datos informáticos.
  - Atentado contra la integridad de sistemas informáticos – Art. 4, sanciona al que deliberadamente e ilegítimamente incapacita total o parcial a un sistema informático o su adecuado funcionamiento.
  - Proposiciones sexuales a los menores de edad, por medios tecnológicos – Art. 5, sancionando a aquella persona que establece contacto mediante internet o medios análogos con una menor de 14 años, con la finalidad de obtener material pornográfico, o actividades sexuales. Por otro lado, sanciona con una pena superior, si la parte agraviada tiene entre 14 y 18 años de edad.

- Interceptación de datos informáticos – Artículo 7, sanciona al que deliberadamente e ilegítimamente obstruye datos informáticos dirigidos, originadas o efectuadas en un sistema informático, o las emisiones electromagnéticas que transportan datos informáticos de un sistema informático; asimismo, se tiene como agravantes: cuando los datos informáticos se encuentren clasificados como secreta, o cuando el delito descrito en el párrafo anterior se ponga en peligro la seguridad de la nación.
- Fraude Informático – Artículo 8, sanciona al que deliberadamente e ilegítimamente busca general un beneficio indebido en perjuicio de un tercero alterando los datos informáticos o interfiriendo en el funcionamiento de un sistema informático.
- Abuso de mecanismos y dispositivos informáticos – Art. 10, sanciona al que deliberadamente e ilegítimamente produce o comercializa programas, mecanismos, dispositivos, contraseñas, códigos o datos informáticos para cometer un hecho delictivo.

- En el artículo 2 se modificaron las disposiciones complementarias número 3, 4 y 11 de la ley.
  - La tercera disposición fue modificada incorporando a otros órganos del gobierno como: Pe-CERT, ONGEI y los Organismos Especializados de las Fuerzas Armadas, estableciendo con estas una coordinación interinstitucional.
  - La cuarta disposición se incorporó nuevos organismos públicos como Pe-CERT, ONGEI y los Organismos Especializados de las Fuerzas Armadas y empresas del sector privado que luchan contra la cibercriminalidad, entablando una cooperación operativa más amplia y diversa.
  - La undécima disposición atravesó una modificación en el primer párrafo al eliminarse la imposición de multas a las empresas operadoras de acuerdo a la complejidad y circunstancias del caso, e incorporan un nuevo párrafo sobre la organización que establecerá las operadoras de las telecomunicaciones con el fin de cumplir los previsto en el numeral 4 del art. 230 del C.P.P., en el tercer párrafo al igual que en el primero se eliminaron las cualidades que debe tener el caso para imponer la multa.

- En el artículo 3 se incorpora el artículo 12 a la Ley N° 30096, regulando que las personas que realicen las conductas establecidas en los artículos 2, 3, 4, y 10, quedan exentos de responsabilidad penal si es que realizaron esas conductas con autorización, con el fin de proteger los SI.
- En el art. 4 modifica los artículos 158, 162 y 323 del C.P.
  - En el artículo 158 del C.P., se modifica en el extremo de incluir el artículo 154-A como delito perseguible por la acción penal pública.
  - En el artículo 162 del C.P., se da una redacción más exacta en cuanto a lo considerado como secreto, confidencial o reservado, encontrándose de forma explícita los casos en la Ley N° 27806.
  - El artículo 323 del C.P., se modificó en el extremo se regular aquellos actos discriminatorios o incitación que se realicen mediante el uso del internet u otros medios análogos.
- El artículo 5 incorpora los artículos 154-A y 183-B del C.P.
  - Se incorpora al CP el art. 154-A, que sanciona al que comercializa información de la esfera privada de una persona natural.
  - Se incorpora el artículo 183-B, que sanciona el establecer un contacto con un menor de 14 años, o cuando la víctima tiene entre 14 y menos de 18 años, para obtener material pornográfico u acto sexual, este contacto se realiza sin el uso de las TIC.
- Finalmente, en la última disposición se deroga al art. 6 de la Ley N° 30096.

1.6.4. Suscripción del Perú en el Convenio de Budapest

En el año 2001 en Budapest durante la reunión 109 del Consejo Europeo se desarrolló y firmo Convenio de Ciberdelincuencia, siendo este el primer tratado internacional sobre la lucha contra la ciberdelincuencia y el impacto del uso y avanza de las TIC, entrando en vigor en el 2004; el Convenio sobre la Ciberdelincuencia (2001), establece una política penal común a nivel internacional que se encargue de proteger a la población frente al inminente avance de la ciberdelincuencia, con la finalidad de que los estados formen parte de una legislación pertinente y una mejor cooperación internacional, esta necesidad nació debido a que la globalización al expandió el uso de las TIC, mostrando el gran peligro que podrían suponer estas, al ser utilizadas para cometer ilícitos, poniendo

en riesgo la integridad, confidencialidad y disponibilidad de los sistemas, datos y redes informáticos, en ese sentido el presente convenio tuvo como fin combatir eficazmente contra los ciberdelitos, facilitando la investigación, persecución y sanción, y la cooperación internacional y nacional. (pp. 2-3)

El Gobierno Peruano ante la necesidad de luchar contra la cibercriminalidad solicito en el 2014 suscribirse al referido convenio, siendo aprobados por el Consejo Europeo en el 2015, posteriormente, por Resolución Legislativa N° 30913 del 2019, el Congreso aprobó el Convenio Budapest, y mediante Decreto Supremo N° 10-2019-RE del Poder Ejecutivo fue ratificado, entrando oficialmente en vigor el primero de Diciembre del mismo año. Es así que, Elías (2014), señala que las principales directrices adoptadas por el legislador peruano fueron al momento de definir los sistemas informáticos como aquel aislado o conjunto de dispositivos interconectados o relacionados que tiene como función el automatizar los datos en ejecución de un programa, y datos informáticos como aquel hecho, información o concepto que se preste a un manejo informático. (p. 12)

1.7. Posturas Doctrinarias:

Los ciberdelitos o delitos informáticos han sido regulados en diversas legislaciones extranjeras, originando que este tipo de delitos sean estudiados por los juristas para dar nacimiento a la doctrina sobre esta materia; es así que en el Perú estas conductas ilícitas fueron reguladas en la Ley N° 30096, con la finalidad de asegurar la persecución y la sanción de dichas conductas, pero estos delitos a la actualidad han presentado complicaciones en el desarrollo de su investigación para poder identificar al autor y recabar suficientes elementos de convicción que ayuden en la persecución del ilícito, se tiene que las técnicas de investigación que pueden ser de vital importancia en estos delitos son las medidas limitativas derecho, tal como el LSC, pero dicha norma presenta limitaciones a los fiscales al momento de solicitarla mediante requerimiento al juez debido a que uno de los requisitos establecidos en el artículo es que el delito debe tener una pena no menor de cuatros años, situación que complica el requerimiento debida a que los delitos informáticos tienen en su mayoría como límite de la pena en no menor de tres años de pena privativa de libertad, es así que este requisito supone un obstáculo en las funciones investigativas de los fiscales. De lo antes expuesto, existen una variedad de

estudios referentes a los temas abarcados en el presente proyecto de investigación, logrando encontrar posturas sobre la cibercriminalidad, funciones de investigación del fiscal y sobre el LSC; las cuales se expondrán a continuación.

1.7.1. La Cibercriminalidad

Sobre la cibercriminalidad encontramos posturas que contribuyen como criterios para mejorar la legislación del cibercrimen, en ese sentido tenemos a **Posada (2017)** en su artículo sobre los efectos en la teoría de la tipicidad en el cibercrimen, refiere que la evolución social y tecnológica genera el surgimiento de nuevas modalidades criminales que necesitan un correcto análisis terminológico, doctrinal y de la política criminal para una adecuada regulación, la evolución trae el nacimiento del cibercrimen que tiene lugar en la realidad virtual o simulado del ciberespacio, requiriendo una protección a objetos inmateriales como los datos, información, teniendo en cuenta que este tipo de delitos se desarrollan mediante la utilización de técnicas especiales. De igual forma **Mayer (2017)** en su artículo sobre los delitos informáticos, mencionó que existe una afectación a la funcionalidad informática como interés colectivo, siendo este el interés social del individuo, esta vulneración al correcto funcionamiento informático afecta el desarrollo de las personas que usan dispositivos tecnológicos y el internet, conteniendo estos dispositivos información del sujeto, por lo cual pueden verse afectados otros bienes jurídicos, es así que nace la necesidad de resguardar y conservar los sistemas informáticos. Además, **Cristiano (2015)** en su proyecto de investigación sobre la criminología del cibercrimen, sostiene que el estudio criminológico del cibercrimen es de vital importancia para comprenderlo, a raíz de que es una terminología nueva que debe ser estudiada desde el ámbito tipológico y normativa, teniendo como lugar de consumación en el ciberespacio, complicando la determinación de modalidad y la investigación adecuada, siendo prueba de esto la falta de pronunciamiento jurisprudencial sobre esta nueva forma de delitos.

Por otra parte, **Villavicencio (2014)** en su artículo sobre Cybercrimes, refiere que el desarrollo de la tecnología ha ocasionado la aparición de nuevas modalidades delictuales que tienen por medio y finalidad los sistemas o datas informáticas, asimismo, el avance tecnológico facilito que delitos tradicionales tengan una nueva forma de comisión, asimismo se realicen ataques contra la infraestructura de la

información, por lo cual se necesita la criminalización de estas nuevas conductas que circulan en torno al internet y las tecnologías, generando la exigencia de una legislación que cuente con una adecuada técnica de redacción legislativa e interpretación para evitar la violación del principio de legalidad. Por último tenemos a **Rayón y Gómez (2014),** quienes en su artículo sobre las particularidades del cibercrimen en su investigación y enjuiciamiento, afirmaron que la tecnología ha facilitado la perpetración de conductas ilícitas y su ocultamiento, dificultando la investigación y el enjuiciamiento de estas, debido a la deficiente regulación legal y la sanción punitiva, produciendo que el legislador y el operador jurídico desconozca y comprenda el mundo digital; asimismo, la cibercriminalidad representa una complejidad técnica y jurídica, requiriendo de una política legislativa dinámica, moderna y flexible que permita una adecuada tipificación de estas nuevas conductas que se encuentran en constante cambio, por lo cual se debería reformar los fundamentos del derecho y proceso penal, sobre los cuales se sustenta la responsabilidad criminal (p. 230).

1.7.2. Intervención Fiscal:

Sobre la labor de investigación que realiza los fiscales, tenemos a diversos autores que señalan sus posturas sobre las facultades y complicaciones que presentan en la investigación, es así que, **Montiel (2016)** en su artículo sobre la cibercriminalidad social juvenil, señaló que las características de los cibercriminales, las víctimas y los investigadores se da un círculo vicioso, debido al retraso de los avances legales, la inexperiencia y falta de recursos humanos especializados debido a la complejidad de las investigaciones. Seguidamente **Matusan (2013)** en su estudio sobre la afectación de los derechos fundamentales, señala que el Fiscal tiene la función de recabar y asegurar las evidencias o medios probatorios idóneos que pueda sostener la teoría del caso y poder llegar precluir con la investigación llegando a un acuerdo con la defensa del investigado, lastimosamente en los delitos informáticos es complicado llegar a individualizar al imputado por la complejidad de la investigación.

Por otro lado, **Nuñoz y Correa (2017)** en su artículo sobre la prueba ilícita en las diligencias que vulneran los derechos fundamentales, manifestaron que la labor de investigación de los fiscales no se desarrolla en un mundo abstracto, sino que se

ejecuta en una sociedad donde existen relaciones interpersonales que son titulares del derecho, por lo cual debe existir una clara delimitación en la investigación para que ésta no vulnere el derecho fundamental del secreto de las comunicaciones. Por el contrario **Elias (2014)** en su estudio sobre la lucha contra el cibercrimen en el Perú, sostuvo que el legislador penalizo conductas e instituciones para la investigación y la prevención de los delitos informáticos, pero los operadores jurídicos como los fiscales y jueces aún no cuentan con los conocimientos y capacidades técnicas requeridas para la investigación y persecución para la investigación de los ciberdelitos, asimismo los legisladores deben adaptar un marco que respete los principios o lineamientos constitucionales, que cuente con una técnica de redacción legislativas adecuada y un correcto estudio de la política criminal al ser el derecho penal de ultima ratio. Igualmente, **Rayón y Gómez (2014)** en su artículo sobre las particularidades del cibercrimen en su investigación y enjuiciamiento, precisaron que en el ámbito jurídico existe un gran desconocimiento del avance tecnológico de la información y comunicaciones, por lo cual se necesita la formación básica sobre los ciberdelitos a los intervinientes en la investigación y juzgamiento para la eficacia del proceso judicial de los delitos informáticos (p. 231).

Por último tenemos a **Castellanos (2020)** en su ensayo sobre el cibercrimen en épocas de pandemia Covid-19, afirmando que la cibercriminalidad en la actualidad ha tenido un mayor aumento de denuncias y complicaciones en la investigación, al no contar con un desarrollo tecnológico en la materia, falta de capacidades técnicas y humanas en los Órganos Investigativos; asimismo existen limitaciones en la investigación obstaculizando el trabajo de los especialistas por la falta de cooperación de empresas (redes sociales), al tener estas empresas políticas diferentes a la legislación penal, igualmente indica que la entidad rectora de la investigación no puede acceder a información confidencial mediante el LSC siendo este requerimiento de vital importancia, en razón a la falta de prioridad por parte del Órgano Judicial.

1.8. Resultados de Investigaciones:

1.8.1. Investigaciones Internacionales:

En los últimos años se han realizado estudios a nivel internacional sobre la cibercriminalidad, a consecuencia de la constante evolución de las tecnologías,

teniendo a autores como Pons (2018) que en su tesis doctoral sobre el ciberterrorismo, en la cual empleó la metodología de la investigación cualitativa, realizando un estudio a la legislación y jurisprudencia extranjera dentro del actual contexto social de la lucha contra los ciberdelitos, concluyendo que la era de la información y tecnología eleva las posibilidades de los delincuentes para buscar nuevas formas de comisión de delitos, poniendo en grave peligro a la sociedad y la economía, por lo cual se necesitan normas que enfrenten esta amenaza mundial, mediante la creación de normas especiales y la cooperación internacional que debe ser actualizada constantemente; asimismo, señala que el ciberespacio no solo es un escenario donde se pueden cometer delitos, si no que este puede ser el principal lugar de conflictos internacionales, recomendando que debe existir una estandarización de leyes contra los delitos informáticos (pp. 421-424); en ese sentido el autor nos muestra que la evolución de la tecnología suponen un constante riesgo a la sociedad, ya que las personas vivimos en una realidad interconectada al internet generando que los delincuentes desarrollen nuevas formas de criminalidad. Así mismo, Arifi y Arifi, (2021) en su artículo científico sobre los retos de las fuerzas del orden en los ciberdelitos, la cual tiene un enfoque cualitativo, en el cual utilizaron el análisis doctrinal, procesal y normativo sobre la investigación de los ciberdelitos, concluyendo que la evolución constante de las modalidades de cibercrimen dificulta la creación de normas que abarquen todas las formas delictivas, generando que las leyes no sean específicas y claras, dificultando su aplicabilidad en los procesos judiciales, siendo su mayor reto la carencia de conocimientos y habilidades técnicas para una adecuada investigación (pp. 12)[1]; en ese sentido se tiene que la falta de conocimientos sobre el cibercrimen genera una deficiencia normativa en los estados al momento de legislar, así como también una carencia del personal profesional especializado que realicen una investigación especializada. Igualmente, Moscoso (2014) en su artículo científico sobre la ley especial del cibercrimen en chile, utilizando la metodología cualitativa mediante el análisis dogmático y jurisprudencial, concluye que las normas referente al cibercrimen presentan diferentes deficiencias con respecto al bien jurídico protegido, los conceptos, nociones jurídicas y comprensión sobre la informática en

[1] Traducción libre.

la actualidad, existiendo defectos en la legislación al no comprender otras formas de vulneración de la informática, asimismo a nivel jurisprudencial no existen conceptualizaciones claras sobre los delitos informáticos, confundiendo la naturaleza de este tipo de delitos con la naturaleza de los delitos tradicionales, provocando que el operador jurídico encuadre un hecho ilícito en otro tipo penal con el fin de no caer en vacíos legales (pp. 73 - 74); este artículo evidencia que las normas, la doctrina y la jurisprudencia sobre los ciberdelitos presenta falencias debido a la escasa información o conceptualización de diferentes términos que se utilizan para legislar las modalidades de los delitos informáticos, entorpeciendo la labor de los fiscales y jueces debido a la confusa redacción legislativa y doctrina existente.

La evolución constante de la tecnología genera que los países estudien la nueva realidad tecnológica, con la finalidad de elaborar legislaciones que regulen las nuevas conductas delictuales, como lo señala Abushihab (2016) en su estudio sobre la delincuencia informática, en la cual empleó la metodología cualitativa mediante el análisis doctrinario y legislativo, concluyendo que es necesaria analizar las instituciones básicas del derecho penal para poder desarrollar normas acordes a la protección de los sistemas informáticos, en razón a que las normas existentes aún tienen falencias, que dificultan su aplicación y ejecución por parte de los operadores jurídicos (pp. 52-53). En ese sentido los estados buscan regular las conductas o nuevas modalidades delictivas en la actualidad debido al avance tecnológico que sufre la sociedad, con la finalidad de proteger a la población, por lo cual se debe realizar un adecuado análisis a la política criminal. De igual modo, Chavarría, Jirón y Miranda (2016), en su tesis sobre la regulación jurídica de la ciberdelincuencia en Centroamérica, la cual contó con el método comparativo, inductivo y deductivo para el estudio de las legislaciones internacionales, en donde concluyeron que los avances tecnológicos y las recientes modalidades de comisión de delitos en Centroamérica, es producto de la insuficiente regulación de la era virtual y de las nuevas conductas de comisión de ilícitos, ya que estas deberían abarcar las posibles vulneraciones a los derechos constitucionales del ciudadano (p. 3, 95); esta tesis nos muestra que en la actualidad debe existir una mejor regulación del mundo digital que evoluciona constantemente y la implementación de personas especializadas en esta materia.

Por otra parte, al tratarse de delitos que se realizan en el ciberespacio o con uso de tecnologías que se encuentran al alcance de todos los individuos, no se tiene un lugar específico de origen de la conducta delictiva por lo que se requiere de una cooperación internacional, tal como lo señala Şcheau y Pop (2018) en su artículo científico sobre la evolución del cibercrimen, utilizando el enfoque cualitativa, mediante el análisis dogmático de las nuevas tendencias de la ciberdelincuencia en la actualidad a nivel mundial, concluyeron que debe existir una cooperación entre el sector privado y público, con la finalidad de que las autoridades gubernamentales en cooperación con entidades expertas desarrollen normas, para combatir y prevenir el cibercrimen (pp. 4)[2]; mostrando así que existe una deficiencia en torno a la cooperación internacional entre los países, así como una falta cooperación entre los gobiernos y entidades privadas para brindar una investigación y prevención de este tipo de ilícitos. De la misma forma Lusthaus (2016) en su tesis sobre la industria del anonimato en el cibercrimen, empleando la metodología de investigación cualitativa, obteniendo mediante el enfoque exploratorio al estudio 200 entrevistas realizadas desde el 2011 a agentes del orden, miembro del sector de tecnología, ex ciberdelincuentes y especialistas en el tema, que el ciberdelito es un fenómeno mundial, que puede afectar a diferentes personas a lo largo del mundo, por lo cual se necesita la cooperación internacional (pp. 39, 277) [3]; Lusthaus nos muestra que los estados deben contar con apoyo internacional de instituciones especializadas en la investigación de los ciberdelitos, así como también con el apoyo de las grandes empresas que manejan el mundo del internet, la tecnología y las redes sociales.

1.8.2. Investigaciones Nacionales:

A nivel nacional encontramos investigaciones que desarrollan el tema de los ciberdelitos, tal como Díaz (2019), quien en su tesis sobre la ley de los ciberdelitos, en la cual empleó el enfoque cualitativo, mediante la entrevista aplicada a especialistas del derecho penal, en donde concluyó que la ley sobre los ciberdelitos no cumple con su finalidad de sancionar de forma adecuada las conductas ilícitas que vulneran los datos y sistemas informáticos o que se realizan mediante la

[2] Traducción libre.

[3] Traducción libre

tecnología, por la complejidad de la investigación de los delitos informáticos, originando el archivamiento o sobreseimiento por la falta de individualización e identificación del autor o autores del ilícito (pp. 34); como se observa este trabajo resulta relevante debido a que la normatividad de la cibercriminalidad no resulta suficiente para garantizar una adecuada investigación por parte de los operadores jurídicos, asimismo estos no se encuentran capacitados para enfrentar la complejidad de estas nuevas modalidades delictuales. Del mismo modo Fernandez (2019) en su tesis sobre los delitos informáticos que vulneran la indemnidad sexual, utilizando el método de estudio cualitativo, mediante el análisis documental, teniendo como participantes del estudio a especialistas en el derecho penal a quienes se les aplicó una entrevista, obteniendo como resultado que para la efectividad de las normas penales se requiere de un adecuado análisis de política criminal y una correcta técnica legislativa para que la norma sea efectiva y eficaz para prevención de la cibercriminalidad. (pp. 24, 40-45); de ello resulta relevante que el análisis de la política criminal y la técnica legislativa es la base principal para la efectividad de las normas penales, al ser esta de ultima ratio, en ese sentido debe existir un mayor estudio del cibercrimen para poder regular aquellas conductas más reprochables para la sociedad.

Con respecto a la legislación impartida en el país sobre los delitos informáticos, diversos autores tales como Gallardo (2020), quien en su tesis sobre las innovaciones realizadas a la tipificación de los delitos informáticos producto de la ratificación del Convenio de Budapest, utilizando el método cualitativo mediante la técnica de análisis documental del Convenio de Budapest, la Ley N°30096 y el Código Penal, refiere que existen delitos comprendidos en el convenio sobre la cibercriminalidad, que no se encuentran tipificados en las normas penales del Perú. (pp. 66, 105). De acuerdo a lo obtenido por el autor podemos determinar que la legislación peruana ha dado su mayor esfuerzo para regular correctamente las modalidades del cibercrimen, pero aún existen algunas conductas que no están completamente amparadas en nuestras normas peruanas, por lo cual este trabajo tiene incidencia en nuestro proyecto al reflejar que es necesario tener una adecuada regulación o tipificación de los delitos informáticos. Asimismo, Paredes (2013) en su tesis sobre el uso de sistemas informáticos en la comisión de delitos, empleó el método de análisis dogmático, histórico y analítico, aplicando las técnicas

de análisis documental, entrevista y cuestionario, concluyó que es necesario reformar de forma integral el código penal para adecuar las diferentes conductas ilícitas tradicionales a las nuevas formas de comisión, ampliar el objeto material o inmaterial de protección del bien jurídico, introducir nuevas conductas punibles en la cual se usen los sistemas informáticos. (pp. 26-27, 248). De ello, nos damos cuenta que es necesaria una reforma normativa referente a los delitos informáticos, con la finalidad de tener una adecuada aplicación de la norma penal y una investigación optima; consideramos relevante la presente tesis para nuestra investigación por que indica cual es la situación de los delitos cibernéticos en el Perú, mencionando que aspectos de la norma son necesarios modificar.

Con referente a la investigación de los casos de los delitos informáticos no existen las suficientes herramientas de investigación y personal capacitado para realizar una adecuada investigación, como lo señala Gómez (2020) en su tesis sobre la investigación de los delitos informáticos contra el patrimonio, empleando el enfoque cualitativo de tipo aplicado, mediante la entrevista a los fiscales de Lima Norte, concluyendo que no existen herramientas para realizar una adecuada investigación o recabar elementos de convicción que sean suficientes para la continuación de la investigación preparatoria, debido a la intangibilidad de esta modalidad delictiva, asimismo señala que la legislación penal peruana no ha presentado avances en la persecución e investigación de los ciberdelitos, debido a que el legislador ha regulado de forma genérica esta nueva modalidad delictiva (pp. 10-12, 28); de ello tenemos que en el sistema penal peruano no ha buscado mejorar o implementar nuevas formas de investigación o facilitar los requisitos de medidas ya existentes para una correcta investigación, por lo cual este trabajo es relevante para nuestra investigación. En ese mismo sentido Cabrera (2020), refiere en su tesis sobre los fundamentos jurídicos que utilizan los fiscales para archivar las investigaciones de delitos informáticos, en la cual utilizó la metodología de investigación cualitativa, realizando la recolección de datos mediante la técnica de fichaje y la guía de análisis documental, concluyó que los fundamentos usualmente utilizados por el representante del ministerio público se debe la falta de individualización del autor, acción penal privada, el hecho no es justificable o es un hecho atípico, evidenciando que no se cumple con el objeto y finalidad de la ley de delitos informáticos, la cual es de prevenir y sancionar las conductas o hechos ilícitos que vulneran los datos y

sistemas informáticos (pp. 22-24, 133-134); este trabajo evidencia que existen dificultades en la investigación realizada por los fiscales al no poder identificar al autor del ilícito debido a la falta de sujetos capacitados y especializados en este tipo de delitos que son de alta complejidad, así como también la falta de técnicas de investigación, la complejidad al presentar los requerimientos del levantamiento del secreto de las comunicaciones o del secreto bancario.

CAPITULO II: LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES

2.1. Derecho al Secreto de las Comunicaciones

El derecho al secreto de las comunicaciones es aquella protección objetiva que se brinda a las personas al poder comunicarse libremente con otros individuos sin tener algún tipo de limitación, ya sea en el contenido de la conversación, la existencia de la misma y quienes son los participantes en esta. Es así que en la legislación encontramos diversas normas que amparan este derecho.

El Convenio Europeo de Derecho Humanos (2021), protege este derecho en el art.8 prescribiendo que los individuos poseen el derecho a que se respete su vida en el ámbito privado, en el ámbito familiar, ámbito domiciliario y su correspondencia; no obstante también señala que no deberá haber injerencia por parte de la autoridad pública en el ejercicio de este derecho, a menos que dicha injerencia esté amparada por la ley y constituya una medida que es necesaria en el ámbito de la seguridad pública, seguridad nacional, el bienestar de la economía del país, defensa del orden y prevenir delitos penales, la protección de los derechos y las libertades de las personas. (p. 11)

Por otra parte, Coronado y Segura (2018), precisan que el convenio antes mencionado es de vital importancia para el ordenamiento jurídico debido a que esta norma resulta de ayuda para la interpretación de este derecho fundamental en la legislación peruana. (p. 23)

Es así que en el Perú la protección del SC está protegido en el artículo 2 inciso 10 de la Carta Magna del Perú (1993), que establece que toda persona tiene derecho a la confidencialidad e inviolabilidad sobre las comunicaciones y documentos privados, de esta forma, indica que las comunicaciones, telecomunicaciones o

herramientas solo pueden ser abiertas, incautadas, interceptadas o interferidas con el permiso de un juez con motivo legítimo. (p. 2)

Igualmente, Coronado y Segura (2018), mencionan que la constitución busca garantizar la protección del secreto de las comunicaciones de las personas o entidades, teniendo excepciones cuando se requiera con urgencia la necesidad de intervenir en las comunicaciones al encontrarse en peligro derechos fundamentales de mayor relevancia; en ese sentido el autor delimita los conceptos de: secreto, siendo este una presunción de pleno y absoluto derecho de confidencialidad de la información que se está comunicando, no importando si la información ingresa o no a la esfera de lo personal; mientras que la comunicación está compuesta por cinco elementos, tales como: un emisor, un receptor, un código o sistema de señales, el contenido, y el medio por el cual se realiza la comunicación (p. 24)

Por otra parte, el TC mediante la sentencia del Expediente N° 867-2011/Apurimac (2011), señala en el fundamento número 2, prohíbe que el derecho al secreto y la inviolabilidad de las comunicaciones sean intervenidas o conocidos por terceros, quienes son ajenos a dicha comunicación, aunque sean órganos públicos o particulares, sin embargo, estas pueden ser interceptadas cuando exista autorización judicial debidamente motivada, asimismo, TC en reiterada jurisprudencia ha precisado la conceptualización de dicho derecho fundamental, señalando que este derecho comprende a la misma comunicación, sin importar el contenido, que la comunicación pertenezca o no al ámbito personal, intimo o reservado del individuo; en el fundamento número 3 se habla de dicha prohibición contenida en la constitución está dirigida a garantizar que no se pueda vulnerar la comunicación en cualquiera de sus formas o medidas, con la finalidad de que no sufra una intervención externa por parte de otros, ya que la presencia de un tercero que no intervino en el proceso que media comunicación, es aquel elemento que no puede faltar para indicar que se vulnero el derecho al secreto y a la inviolabilidad de las comunicaciones, sin embargo, es constitucionalmente posible manifestar que el derecho a la inviolabilidad de las comunicaciones no vulnera cuando alguna de las personas que intervinieron en la comunicación es la graba para sí la comunicación en la que formó parte o cuando esta permite o autoriza que dicha comunicación sea interceptada, grabada o que cuenten con acceso al contenido de

dicha comunicación; en ese sentido la constitución a vedado la injerencia externa dentro de la comunicación de un ajeno que no tiene ningún tipo de autorización y no el registro o la autorización para el acceso a la propia comunicación. (pp. 3 - 4)

En ese sentido, Varsi (2014), indica que el derecho al SC, se refiere al resguardo que se brinda a los medios de comunicación por donde las personas se comunican entre sí, por lo cual se trata de las comunicaciones en curso, que fueron leídas, y que forman parte de la intimidad del individuo, debido a que es información privada, por lo cual ningún tercero puede acceder, intervenir o escuchar conversaciones que no pertenezcan a su esfera personal o privada, ya que forman parte de la intimidad de otra.

Mientras que Rubio (2008), señala que por secreto se debe comprender al asunto de las comunicaciones o de documentos confidenciales que son propiedad de un individuo, y solo puede ser de conocimiento de la misma, de tal manera, existe la confidencialidad cuando la comunicación solo pertenece aquellos que participaron dentro der esta, existiendo un emisor y un receptor, por lo que solo a ellos conocen el contenido, entonces la inviolabilidad de las comunicaciones consiste en que estas no pueden ser intervenidas; en ese sentido la invulnerabilidad no tiene que ver nada con lo que contiene de la información sino con el desarrollo de intervenir la comunicación o sustraer documentos de la esfera privada.

De igual manera, Lopez et al. (2010), señala que este derecho constituye en una garantía que forma parte de la vida personal, para preservar privacidad de la persona libre de injerencias que realicen terceros o los poderes públicos, asimismo, señala que el Tribunal Constitucional Español, ha configura este derecho como una garantía, que protege la información confidencial de las comunicaciones sin importar el contenido de estas.

Por otro lado, Mesia (2010), señala que la garantía del secreto abarco lo comunicado, sin importar su contenido o si este tiene relación con la intimidad o privacidad del individuo, y que estas solo pueden ser intervenidas cuando exista una autorización judicial o que se cuente con la autorización de la persona. (p. 125)

2.2. Definición de la medida del Levantamiento del Secreto de las Comunicaciones

Toledo (2019), menciona que el LSC es aquella intervención del secreto de las comunicaciones, intervención del registro telefónico, intervención telefónica y otros que denotan similar naturaleza, cabe resaltar que también es confundida con la medida de interceptación y grabación de comunicaciones telefónicas o muchas veces solo llamada interceptación telefónica; poniendo de ejemplo la legislación española, señalando que esta medida fue recientemente incluida en la redacción de la Ley de Enjuiciamiento Criminal que fue modificada en el 2015 bajo la sección incorporación al proceso de datos electrónicos de tráfico o asociados y el artículo 588 ter j con el nombre de datos obrantes en archivos automatizados de los prestadores de servicios; asimismo, manifiesta también que es una medida que tiene por finalidad la obtención de datos de la forma de la comunicación, es decir, de las condiciones en las que la comunicación se llevó a cabo; estas condiciones incluyen la identificación de los comunicantes y los terminales que se usaron, el marco temporal y temporal en el cual se desarrolló la comunicación, entre otras; el LSC tiene como objeto solo las comunicaciones que al momento de su autorización hayan sido concluidas. (pp. 45 - 46)

2.3. Regulación en la Legislación Peruana

Toledo (2019) aclara sobres esta figura jurídica que no se encuentra estipulada como tal en nuestra legislación sino que las únicas medidas de control reconocidas son las que se encuentran mencionadas en el art. 230 del CPP, no obstante, es la práctica judicial la que permite visualizar que existen requerimientos que no son adecuados a ninguna de las figuras, por lo que da pie a la idea de una medida sui generis, el LSC busca información de comunicaciones que ya concluyeron; es decir, la interceptación y geolocalización van a perjudicar a comunicaciones venideras, mientras que el levantamiento del secreto de las comunicaciones, siempre perjudicará a comunicaciones antiguas. (p. 47)

Además, dentro del levantamiento encontramos que se restringe un derecho que se encuentra expresamente amparado en la Constitución en el art. 2 inciso 10 señalándolo como el derecho al secreto y la inviolabilidad de las comunicaciones, en la cual se estipula que toda persona tiene derecho al secreto y a la inviolabilidad

de sus comunicaciones, sin embargo dicho artículo hace precisión de que este derecho se puede limitar siempre y cuando sea por orden de judicial y será necesario; el derecho al secreto y la inviolabilidad de las comunicaciones también se verifica en el Código Procesal Constitucional - Ley N° 28337 en el que en el art. 37 prescribe que el amparo procede en defensa de la inviolabilidad y secreto de documentación.

2.4. Presupuestos de la Medida

Toledo (2019), señala que el LSC solo procede cuando se cumplan con los presupuestos de la medida, siendo estos supuestos debidamente fundamentados en el requerimiento fiscal, el cual debe encontrarse debidamente sustentado con suficientes elementos de convicción; esta medida procede en las investigaciones de delitos con una pena superior a los 4 años de sanción y si la autorización superase el análisis de proporcionalidad, del mismo modo, el levantamiento usa el trámite con total reserva en todos los requerimientos, sobre las personas afectadas, la medida del levantamiento tiende a omitir el numeral 2 del art. 230 debido a que, su uso tiende a ser más amplio que el de una interceptación telefónica y limitar su aplicación solo a los imputados que terminaría afectando lo viable de la investigación; asimismo, la afectación a una persona diferente del imputado va a expresar una contradicción a la ley que se usa de forma supletoria para los requisitos, esta afectación se debe considerar un caso excepcional y debe ser motivado de manera adecuada para justificar el porqué de la autorización. (pp. 47 - 48)

Respecto al 4to numeral del art. 230 se tiene que este se aplica a los concesionarios de servicios públicos de telecomunicaciones, los cuales tiene la obligación de dar facilidades para obtener información en vez de estar buscándola. Por último, es que, por ser una medida que se ejecuta de forma inmediata es que no se hará aplicación del numeral mencionado al cese de la medida como tampoco lo es el numeral que prescribe la duración máxima de esta medida, en conclusión, tenemos que se configura como una medida sui generis en razón a que tiene muchas diferencias entre su finalidad, su ámbito de aplicación, la afectación a una parte distinta de la comunicación y carece claramente de una acertada regulación. (p. 49)

2.5. Autorización Judicial

Coronado y Segura (2018), aclara que en la jurisprudencia del Tribunal Supremo se fijan los requerimientos que de no efectuarse harán que no se haga posible la autorización o el resultado que se obtenga no podrá usarse como prueba, es así que tenemos requisitos como que solo se podrán ordenar de modo excepcional, en razón a que no exista alguna otra manera de la obtención de los mismos resultados de no ser por la intervención telefónica u otra parecida; para el requerimiento y la autorización de la intervención de las comunicaciones donde debe existir indicios suficientes de la comisión del ilícito; no basta la mera sospecha; los resultados de la investigación tienen un control por parte de la autoridad judicial, sin embargo, si el registro de las comunicaciones quedara a cargo de otro funcionario como PNP o empresas de telefonía, pues dicho control también va a quedar a cargo del Fiscal del caso. (p.29)

2.6. Control de la Medida

Coronado y Segura (2018), con respecto al requerimiento presentado por el fiscal a cargo del caso precisa que se debe de tener en cuenta que todo dato personal de titular u usuario va a formar parte del secreto de las comunicaciones, esto va a comprar como la identificación del titular o usuario, el código del cliente, los servicios u equipos contratados, entre otros. (p.23).

2.7. Valor Probatorio

Neyra y Tresierra (2017), mencionan que la finalidad de la intervención de comunicaciones telefónicas es el esclarecimiento de los hechos, a través de la obtención de datos relevantes contenidos en los registros (pasados o futuros) y/o grabaciones de dichas comunicaciones, a efectos de poder determinar la realización o no de un hecho punible y la autoría o participación de los imputados en el marco de un proceso penal. (p. 155)

2.8. Principios que rigen la Medida

Los principios que permiten la medida del Levantamiento son:

A. Proporcionalidad

Coronado y Segura (2018) citando a San Martin (2017), indican que la medida ha de ser imprescindible, entendiéndose que debe existir otros medios de investigación menos nocivos y cuando la investigación de las circunstancias no ofrezca probabilidad alguna de ser exitosa o se va a tornar difícil, en ese sentido se trata de dos perspectivas respecto a la necesidad, tanto desde la probabilidad de ser útil como de su cualidad de no poder ser sustituible, pues si la medida no garantiza obtener información importante y relevante para continuar con la investigación o se pueda obtener esta información por medios que no ocasionen una vulneración a los derechos fundamentales, este principio de proporcionalidad se vetaría su adopción; es por eso que esta medida se solicita cuando se trata de delitos graves y de trascendencia social. (p. 26)

B. Especialidad

Coronado y Segura (2018), señalan que se debe especificar los indicios de la comisión del delito y la persona que sindicada como sospechosa del delito; es por eso que existe la necesidad de que se haya incoado una investigación preparatoria, mínimamente en el nivel de diligencias preliminares, el delito debe referirse a un hecho concreto plenamente subsumible dentro de un tipo legal grave, del que existan indicios de criminalidad razonable, señalar a una persona en concreto, siendo este el investigado que está vinculado al delito objeto de investigación o sobre quien recaiga la medida; sin embargo, no es necesaria una identificación exhaustiva de la identidad del sospechoso o investigado.

C. Necesidad

Para Coronado y Segura (2018), señalan que la necesidad es un subprincipio de proporcionalidad, en el que la intervención en los derechos fundamentales, es necesaria cuando otros medios están ausentes, sin embargo, debe revestir como mínimo la idoneidad para lograr el objetivo, la existencia de un hecho delictivo supone el inicio de la actividad jurisdiccional, pues es la legalidad la que determina cuando se inicia el proceso penal, por lo que este principio de necesidad es también el mecanismo para evitar riesgos importantes en la aplicación del derecho penal, pues pretende impedir que los delitos queden impunes. (p. 56)

2.9. Posturas Doctrinarias:

2.9.1. Levantamiento del Secreto de las Comunicaciones:

Acerca del LSC diversos autores han estudiado los diferentes ámbitos de este medida, comenzando con el estudio al derecho del secreto de las comunicas hasta arribar el análisis de la finalidad de la medida limitativa, en ese sentido tenemos a Toledo (2019), quien en su tesis sobre el LSC, refiere estar de acuerdo con que las medidas limitativas sean solicitadas por parte del Ministerio Público y que requieran la autorización del juez, asimismo que dicha medida debe cumplir dos finalidades: ser medidas de coerción procesal o ser medidas con la finalidad de obtener pruebas; en el caso del levantamiento de las comunicaciones resulta ser de importancia la obtención de pruebas, ya que solo así el fiscal va a realizar una investigación más completa, no sobrepasando las reglas y límites establecidas por la ley; de igual forma señala que no existe una denominación al LSC, debido a que no tiene un nomen iuris propio en la legislación, sino que se encuentra sujetas a otras denominaciones, en dicho sentido la práctica judicial es la que debe observar la existencias de requerimientos que no se adecuen las figuras, asimismo refiere que la finalidad de esta medida, es la obtención de información de las comunicaciones o telecomunicaciones pasadas que se encuentran almacenadas debido a su conclusión, cabe señalar que esta medida procede a solicitud del requerimiento fiscal, cumpliendo con todos los requisitos establecidos en la norma, siendo la principal que todo delito debe superar la pena de no menor de cuatro años. (pp. 39-47)

Por otra parte, Vilvila (2016), en su tesis sobre falta de motivación e indebida afectación del secreto de las comunicaciones telefónicas, señala que las comunicaciones no pueden ser intervenidas, ya que el titular de las comunicaciones es el único que puede autorizar su divulgación, de tal manera que el bien jurídico protegido de la intimidad tiene una protección en un determinado ambiente inmaterial, asimismo precisa que este derecho no es absoluto porque nuestra Constitución se estipula que mediante un mandato del juez se puede restringir este derecho, otorgando la facultad al representante del Ministerio Público para que haga la intervención y control de comunicaciones en casos excepcionales para la obtención de pruebas para identificar al imputado, estas intervenciones pueden ser

por diversas motivaciones como de orden político, económico, investigaciones privadas o investigaciones por un delito cometido, etc.; por ende es que la orden judicial debe brindar las garantías necesarias para esta vulneración amparada por la ley, en ese mismo sentido lo propuesto por el artículo 227 del C. P. P. en precisando que el representante del Ministerio Público es el encargado de la ejecución de manera inmediata de la interceptación e incautación para después presentarlo al juez para un control (pp. 94, 129 - 130); siendo que estamos de acuerdo con esta postura dada que el Fiscal es quien conduce la investigación desde la etapa de diligencias preliminares para que recabar los elementos de convicción necesarios para armar su teoría del caso.

Finalmente tenemos a Neyra y Tresierra (2017), quienes en su tesis sobre el procedimiento de grabación, intervención o registro de comunicaciones, alegan que las medidas limitativas de derecho del secreto de las comunicaciones necesariamente requieren una resolución judicial que autorice previamente a la intervención de comunicaciones telefónicas, ya que va a limitar un derecho como lo es el secreto de las comunicaciones, por ende, se necesita que para llevarse a cabo esta medida el representante del Ministerio Público debe presentar una solicitud al órgano judicial, ya que de darse el caso en que se afecte el derecho fundamental debido a la intervención de las comunicaciones sin la autorización del juez, todo lo obtenido mediante esta medida se consideraría como prueba prohibida teniendo así que carencia probatoria, además señalan que estas medidas que por su propia naturaleza de restringir derechos, no se pueden realizar primero y luego solicitar la confirmatoria judicial, debido a que nuestro ordenamiento señala expresamente que debe haber una resolución judicial firme para acceder a esta medida. (pp. 120, 135) De igual forma señalan que la Ley N° 27697 otorga al Fiscal la facultad para la intervención, pero solo en casos excepcionales y con un requisito indispensable: la autorización judicial; debido a que esta medida limita ciertos derechos constitucionales con el fin de brindar pruebas a las investigaciones que realiza el representante del Ministerio Público; precisan que si bien todos los ciudadanos gozamos del derecho a la inviolabilidad de las comunicaciones, pues este derecho no es absoluto, ya que puede verse restringido a causa de una resolución judicial debidamente motivada, siendo así es que nace la figura de la intervención de las comunicaciones que va a tener como fin el obtener elementos

de convicción que van a servir al Fiscal al momento de realizar una investigación. (pp. 148-149)

2.9.2. Levantamiento del Secreto de las Comunicaciones en la Investigación de los Delitos Informáticos:

Con referente a la utilización de la medida limitativa de LSC para una adecuada investigación en los casos de ciberdelitos, diversos autores han referido que dicha medida es de vital importancia pero que esta presenta requisitos que suponen un obstáculo para obtener la autorización por parte del juez, como lo señala Corona y Segura (2018), en su tesis sobre la actuación del fiscal frente al LSC, señalando que el fiscal debería tener la potestad para permitir la intervención de las comunicaciones para delitos de menor injerencia, con la finalidad de acelerar y facilitar la investigación de este tipo de delitos, que tienen importante relevancia en las diligencias preliminares para lograr adquirir elementos convicción suficientes que ayuden a la identificación del autor, no descartando que después el juez confirme la decisión; asimismo, precisa que existen casos archivados que no contaban con suficientes elementos de convicción, debido a la denegatorio de la autorización para requerir información en las empresas de comunicaciones.

Por otro lado, Chamarro (2019), en su tesis sobre las nuevas medidas de investigación tecnológicas limitativas del secreto de las comunicaciones, señala que la adaptación de una legislación adecuada sobre el derecho procesal penal, ha logrado que no existan vacíos legales para realizar las diligencias de investigación, evitando la vulneración de los derechos fundamentales al obtener información mediante el LSC, desarrollando los tribunales una legislación que introduzca una seria de novedades de investigación bajo el principio de legalidad, para una eficaz persecución de los delitos informáticos.

2.10. Resultados de Investigaciones:

2.10.1. Investigaciones Internacionales:

Los delitos informáticos necesitan herramientas que faciliten su investigación, por lo cual los Estados han establecido a lo largo de los años diferentes técnicas de investigación, siendo la técnica más adecuada para utilizarse en la investigación de los delitos informáticos, siendo el LSC la más adecuada, ya que puede resultar en

un importante elemento de convicción dentro del proceso penal, debido a la información que se obtendrá la intervención de las comunicaciones, pero esta medida aún presenta falencias como refiere Marco Urgell (2010), en su tesis sobre la intervención de las comunicaciones telefónicas, en la cual aplicó la metodología de investigación cualitativa, mediante el análisis doctrinal y jurisprudencial, concluyendo que la intervención de las comunicaciones es un medio lícito de investigación para obtener elementos de convicción y poder utilizarlo como medio de prueba, a su vez como garantía de un proceso justo, no obstante existen deficiencias en la regulación de las intervenciones de las comunicaciones de modo que se tiene la necesidad de una positivización de aspectos concretos, como las modalidades de injerencias de los medios de comunicación, los supuestos en los cuales la injerencia es oportuna en atención a la gravedad de la pena y el control judicial de la proporcionalidad de la medida (pp. 499-505). Debido a ello, podemos decir que existe un criterio compartido con el resultado obtenido por el autor, al referir que existen deficiencias en las normas que regulan la intervención de las comunicaciones por lo cual se necesita una redacción legislativa adecuada que permita una correcta interpretación y aplicación de esta medida de investigación para poder obtener suficientes pruebas.

2.10.2. Investigaciones Nacionales:

Ahora bien, en el sistema procesal peruano se han regulado medidas limitativas de derecho que funcionan como técnicas a utilizarse dentro de una investigación para recabar elementos de convicción que ayuden a esclarecer los hechos ilícitos, es así que el artículo 230 del Código Procesal Penal se ha encuadrado la intervención de las comunicaciones y telecomunicaciones más conocida con el LSC, siendo esta intervención una herramienta procesal penal compleja, la cual requiere de autorización judicial debido a la restricción del derecho fundamental del secreto de las comunicaciones, ya que no es autorizada y desconocida por los sujetos interesados; en ese sentido los autores tales como Neyra y Tresierra (2017), en su tesis sobre la intervención de las comunicaciones telefónicas, optaron por una metodología mixta (cualitativo y cuantitativo), aplicando el estudio de casos, encuesta y entrevista, concluyendo que el requerimiento de levantamiento del secreto de las comunicaciones telefónicas elaborados por el fiscal, al tener un

trámite de resolución reservada debido a que resuelven sobre una medida limitativa de derechos del ciudadano, vulneran las garantías amparadas en la constitución y el código procesal penal, por lo cual debe de modificarse el numeral 1 del artículo 230 del código penal (pp. 222-224); este trabajo evidencia que debe modificarse dicha norma limitativa para garantizar una mejor investigación sin vulnerar los derechos del ciudadano, y así tener una regulación adecuada del LSC. De la misma forma Salazar (2016), en su tesis sobre las repercusiones jurídicas de las intervenciones de las comunicaciones, aplicando el enfoque cualitativo, mediante el análisis doctrinal y jurisprudencial, concluyó que la medida de LSC en el sistema penal peruano presenta deficiencias en comparación a las legislaciones extranjeras, por lo cual el legislador peruano debe tener una adecuada técnica legislativa al regular una medida limitativa de derecho para la investigación de algún acto ilícito, implementar técnicas y especificar la finalidad de dicha medida, asimismo, señala que para la intervención de las comunicaciones se requiere expresamente la autorización del juez de investigación preparatoria con una debida motivación que resguarde los principios constitucionales y procesales (pp. 90-91); de ello podemos señalar que es necesaria una modificación del artículo 230 del Código Procesal Penal para asegurar una investigación adecuada y poder recabar suficientes elementos de convicción.

Por otro lado, Vilvila (2016), en su tesis sobre la afectación del secreto de las comunicaciones, optando por la metodología cuantitativa y cualitativa no experimental, mediante la observación documental y la ficha de observación documental, analizando 26 resoluciones que autorizan la intervención de las comunicaciones en la cuales no se ha realizado una motivación adecuada, al no fundamentar debidamente los principios de idoneidad, excepción, necesidad o proporcionalidad, y solo basar su decisión en la imputación de un delito grave y la necesidad de identificar al autor del ilícito (pp. 192-193); este trabajo revela de que existen falencias en la aplicación de la medida del LSC al no cumplir con requisitos sustanciales para una debida motivación y solo cumplir con los requisitos formales o específicos que la misma norma señala. Igualmente, Coronado y Segura (2018), refirieron en su tesis sobre la actuación del fiscal en el LSC, en la cual emplearon el método cuantitativo, utilizando la encuesta para obtener los conocimientos de los magistrados sobre el LSC, en donde se obtuvo como resultado que diversos casos

fueron archivados debido a la carencia de elementos de convicción para continuar con la investigación, siendo la principal dificultad las denegatorias de los requerimientos del LSC, asimismo que en la código procesal penal no se hace referencia de forma expresa la regulación del requerimientos de datos telefónicos de menor injerencia, puesto que la norma hace referencia a la intercepción telefónica. (p. 101) En ese sentido, lo referido por el autor es sumamente importante para la presente investigación debido a que muestra que existe dificultades en la investigación realizada por el representante del Ministerio Público, al no poder obtener la autorización por parte del juez de investigación preparatorio para realizar el LSC, ya que este es de vital importancia para obtener suficientes elementos de convicción que permitan individualizar al imputado y la continuación de la investigación.

CAPITULO III: LEGISLACIÓN EXTRANJERA

3.1. Legislación Extranjera sobre el Cibercrimen

3.1.1. Delitos Informáticos en Argentina

En la legislación argentina encontramos que no hay una regulación especial como tal, pero hallamos que mediante Ley N° 26.388 (2008), se introducen ciertos delitos informáticos a su Código Penal Vigente, delitos contra la integridad sexual, contra la violación de secretos y la privacidad, contra el acceso informático, acceso a banco de datos, contra la publicación de una comunicación electrónica, contra el fraude informático, daño informático.

Tenemos así la incorporación de estos delitos en mención:

a. Pornografía infantil – Art. 128

   En este artículo incorporado al Código Penal argentino se tiene que cualquier persona que divulgue, distribuya, facilite, publique, financie todo acto de índole sexual de un menor de 18 años a través de cualquier medio incluido cualquier medio digital va a ser sancionado con una pena de entre 6 meses a 4 años.

Se debe mencionar que se sustituye el epígrafe del Cap. III, del Título V del Libro II en el que se añade con el título de “Violación de Secretos y de la Privacidad”, continuando así con los siguientes delitos incorporados:

b. Sobre la violación de secretos y la privacidad – Art. 153

   Se sancionará a aquella persona que se apodere indebidamente de una comunicación electrónica o telecomunicaciones sea interceptando o captando, sancionándole con una pena entre 15 días a 6 meses de prisión.

c. Contra el acceso informático – Art. 153 bis

   Este delito va a sancionar a toda persona que a través de cualquier medio accediese sin autorización a un sistema informático restringido, se agravará la pena si el acceso genera perjuicio a un organismo público.

d. Acceso a banco de datos – Art. 157 bis

   Se va a sancionar a aquellas personas naturales que accedan de forma ilícita a un banco de datos, que proporcionen o revelen información registrada en un archivo o que también inserten o hagan insertar datos a un archivo de datos personales; además si el autor del delito es un funcionario público va a tener una sanción especial que es la inhabilitación. En el primer caso la pena será de entre un mes a dos años y en el supuesto de ser un funcionario la pena será de inhabilitación especial de uno a cuatro años.

e. Fraude informático – Art. 173 inciso 16

   Se sanciona a aquella persona que defraude a través de técnicas de manipulación informática va a alterar el normal desempeño o funcionamiento de un sistema informático o trasmisión de datos.

f. Daño informático – Art. 183

   Este delito se enmarca sancionando conductas como alterar o destruir tanto programas como sistemas informáticos como también sanciona a aquellas personas que vendan o introduzcan.

3.1.2. Delitos Informáticos en Venezuela

Ley Especial contra los Delitos Informáticos la cual se publicó en Gaceta Oficial N° 37.313 y entró en vigencia el 30 de noviembre del 2001, comprende de veintiún tipos penales, los cuales se clasifican en cinco categorías según lo que protegen:

a. Delitos contra los sistemas que utilizan tecnología de la información

   - Acceso Indebido – Art. 6, en este delito prescribe que cualquier persona que sin contar con autorización o si se excede de la autorización que tiene

para obtener, acceder, interceptar o interferir en tecnologías de la información va a ser penado con prisión de uno a cinco años. Aquí el sujeto activo será cualquier persona natural que realizará lo mencionado en líneas arriba y el sujeto pasivo puede ser tanto personal natural como persona jurídica.

- Sabotaje o daño a sistemas – Art. 7, en este delito va referido a las personas naturales que pueda tener conocimientos para alterar o inutilizar un sistema siendo que podrá ser sentenciado de cuatro a ocho años. Comprende además a aquellas personas que destruyan o inutilicen datas o información en cualquier sistema; se tendrá como agravante en el único caso que el sujeto activo del delito realice lo mencionado a través de un virus o programa análogo.
- Favorecimiento culposo del sabotaje o daño – Art. 8, se sanciona a toda aquella persona natural que cometiese el delito del art. Anterior, pero de manera que no tenía intención de cometerlo, sino que para su comisión lo hizo por causa de negligencia o infracción al debido cuidado.
- Acceso indebido o sabotaje a sistemas protegidos – Art. 9, este delito tiene relación con los dos artículos anteriores y es que para este caso se aumentará la pena hasta entre una tercera parte y la mitad cuando de los hechos se pueda apreciar que, para el sabotaje o acceso indebido, se tuvo que vulnerar sistemas con medidas de seguridad y que además contenga tanto información personal como patrimonial de personales naturales o jurídicas.
- Posesión de equipos o prestación de servicios de sabotaje – Art. 10, destinado este delito a personas naturales con conocimientos para el sabotaje y que además puedan contar con equipos sofisticados para la vulneración de sistemas informáticos; teniendo como pena impuesta de entre tres a seis años.
- Espionaje informático – Art. 11, referido a aquellas personas que obtengan información de forma indebida o que revele o difunda datos contenidos en un sistema siendo penado de tres a seis años y se agravará la pena solo si el delito se cometiera con el fin de conseguir algún beneficio sea para él o para otras personas.

- Falsificación de documentos – Art. 12, este delito que comprende la creación, modificación o eliminación de cualquier documento incorporado a un sistema tecnológico será penado de tres a seis años.

b. Delitos contra la propiedad: aquí se incorporan los delitos de fraude, hurto, obtención indebida tanto de servicios y bienes; manejo de forma fraudulenta de tarjetas inteligentes, apropiación de tarjetas inteligentes, posesión de equipos que faciliten las falsificaciones y hurto.
c. Delitos contra la privacidad de las personas y las comunicaciones: violación de la privacidad de las comunicaciones, revelación inadecuada de información de carácter personal, violación de la privacidad de las comunicaciones.
d. Delitos contra los niños, niñas y adolescentes: Difusión/exhibición de material pornográfico y exhibición pornográfico de niños y adolescentes.
e. Delitos contra el orden económico: oferta engañosa o apropiación de propiedad intelectual.

Al igual que en nuestra legislación tenemos que los delitos más relevantes en esa legislación son el delito de acceso indebido (que para nuestra legislación se denomina “acceso ilícito”), sabotaje o daño a sistemas (que para nuestra legislación se denomina “atentado a la integridad de sistemas informáticos”), posesión de equipos o prestación de servicios de sabotaje (no regulado en nuestra legislación) y el espionaje informático (no regulado en nuestra legislación).

3.1.3. Delitos Informáticos en Colombia

En el país colombiano si bien no hay una regulación especial para los delitos informáticos, hallamos la promulgación de una ley en la que se modifica el Código Penal creando un bien jurídico tutelado con la denominación de “protección de la información y de los datos” con el fin de preservar de forma íntegra todo sistema que utilice las tecnologías de la información y las comunicaciones.

Esta Ley N° 1273 (2009), añade los siguientes delitos: el daño informático, el uso de software malicioso, violación de datos privados personales, suplantación de sitios web, obstaculización ilegitima de redes de telecomunicaciones, hurto a través de medios informáticos, transferencia de activos, entre otros.

3.1.4. Delitos Informáticos en España

En la legislación española si bien es cierto que los delitos informáticos no cuentan con una ley especial, pero si se puede encontrar diferentes normas que tienen relación con el tema, como: Ley de Servicios de la Sociedad de La Información, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, Ley General de Telecomunicaciones, Ley de Propiedad Intelectual, entre otras.

La ley española que tipifica diversas conductas delictuales relacionadas con los delitos informáticos es el Código Penal Español, en esta norma podemos hallar delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos como estafas electrónicas que hayan sido realizadas mediante manipulación informática.

3.1.5. Delitos Informáticos en Chile

La legislación chilena si bien es cierto que tiene una Ley especial para sancionar los delitos también es cierto que dicha ley es muy escaza u obsoleta para los avances tecnológicos que se tienen en la actualidad ya que su Ley 19223 (1993), que cuenta con tan solo cuatro artículos que son los siguientes:

a. Art. 1. – Este artículo se aplicará cuando una persona de forma maliciosa destruya o deje inutilizable un sistema mediante el cual se dé tratamiento a información de forma que impida u obstaculice el funcionamiento.
b. Art. 2. – Referido a aquella persona que intercepta, interfiera o accedae a un sistema de tratamiento de información para conocer o usar de forma indebida la información obtenida.
c. Art. 3. – Dirigido contra aquel sujeto que va a alterar, dañar o destruir datos que están contenidos en un sistema de tratamiento de información.
d. Art. 4. – Delito realizado por aquella persona que de forma maliciosa difunda o revele información contenida en un sistema de información.

3.2. Legislación Extranjera sobre el Levantamiento del Secreto de las Comunicaciones

3.2.1. Argentina

En la legislación argentina encontramos diversas normas que hablan sobre esta figura, como punto de partida tenemos a la Constitución Política que es precisa en su art. 18 al mencionar que es inviolable cualquier papel o documento privado salvo que una ley determine en qué casos y además se debe justificar para un allanamiento y ocupación de lo mencionado.

Posteriormente tenemos a la Ley de Telecomunicaciones en su art. 18 que son firmes al manifestar que toda interceptación procederá a requerimiento de un juez competente y que toda correspondencia de telecomunicaciones es inviolable.

En esta misma norma hallamos la inviolabilidad de las telecomunicaciones que constituye prohibiciones como la sustracción, la interceptación, interferencia, publicación, uso, etc.; para que otra persona diferente al destinatario conozca el contenido de dichas informaciones. (Art. 19) En esta norma en mención también tenemos al art. 20 y 21 que declaran que las personas que formen parte del servicio de telecomunicaciones están en la obligación de guardar el secreto respecto a la existencia y contenido como también si fuera el caso que una persona tomara conocimiento del contenido de las telecomunicaciones también tiene la obligación de guardar el secreto.

Seguidamente nos encontramos con la Ley de Inteligencia Nacional (Ley 25.520) que respecto a la inviolabilidad de las comunicaciones en su art. 5 menciona que solo podrán accederse a estas cuando medie orden o dispensa judicial. En ese mismo texto en el art. 18 se aclara que cuando sea necesario para actividades de inteligencia la interceptación o captaciones de comunicaciones privadas se tendrá que la Secretaría de Inteligencia deberá solicitar la pertinente autorización de un juez y que dicha autorización debe realizarse por escrita debidamente fundamentada indicando o precisando tanto los números telefónicos o direcciones electrónicas que se pretendan interceptar.

Finalmente encontramos al Código Procesal Penal Argentino que ya abordando a profundidad nuestro tema, en su art. 236 menciona que el juez tiene la facultad de

ordenar, mediante un auto fundamentado, la intervención de comunicaciones o cualquier medio de comunicación del imputado; además podrá ordenar la obtención de los registros de las comunicaciones del imputado o de quienes se han comunicado con él. También prescribe que, bajo ciertas circunstancias como peligro en la demora, el representante del Ministerio Público Fiscal mediante un auto fundado puede intervenir en las comunicaciones, pero previo debe comunicar de manera inmediata al juez y este debe convalidar esta solicitud en el término improrrogable de 24 horas.

3.2.2. Venezuela

En la República Bolivariana de Venezuela tenemos al Art. 48 que en su Constitución Política (aprobada por 128 diputados el 20 de Diciembre de 1999) garantiza el secreto y la inviolabilidad de las comunicaciones privadas en todas sus modalidades, que no podrán ser interferidas sino por orden un tribunal competente dando cumplimiento a disposiciones legales y se debe preservar el secreto de lo privado o de información que no tenga relación con el proceso que se esté llevando a cabo.

Luego se tiene al Código Orgánico Procesal Penal (publicado en Gaceta Oficial Extraordinaria N° 16.078 de fecha 15 de junio de 2012) que en su art. 205 prescribe que se podrá interceptar o grabar comunicaciones privadas sean ambientales, telefónicas u por otro medio; el contenido se deberá transcribir y agregará a las actuaciones. Para la autorización del levantamiento de las comunicaciones tenemos el art. 206 que menciona que el Ministerio Público debe solicitar razonadamente al juez la autorización correspondiente, en la cual debe estar el tiempo de duración de la medida que no debe exceder de 30 días también se indica los medios técnicos empleados y el sitio desde donde se efectuará; la decisión judicial deberá ser motivada.

Finalmente hallamos a la Ley Orgánica Contra la Delincuencia Organizada (publicada en Gaceta Oficial N° 5.789 de fecha 26 de octubre del 2005) que en su art. 64 mencionan que las autoridades competentes por intermedio del Ministerio Público podrán disponer o aplicar con autorización del juez de control las medidas de interceptación de las comunicaciones, correos electrónicos y de correspondencias.

3.2.3. Colombia

En la legislación colombiana hallamos al Código de Procedimiento Penales (Ley N° 906 – 2004), en su art. 114 inciso 3 manifiestan que la Fiscalía General de la Nación tienen el deber de ordenar registros, allanamientos, interceptaciones de comunicaciones para luego poner a disposición del juez de control de garantías los elementos que se hayan recogido. En esa misma norma en su art. 154 se tiene que para la actuación de poner a disposición del juez de control de garantías se tendrá que realizar un control de legalidad en una audiencia preliminar donde se mostrarán todos los elementos recogidos por la Fiscalía. Se debe aclarar que según art. 55 tenemos que las audiencias preliminares de control de legalidad son de carácter reservado.

Sobre la Interceptación de Comunicaciones tenemos el Art. 235 que menciona que el fiscal tiene la facultad de ordenar la búsqueda de elementos materiales probatorios como evidencia física o búsqueda y ubicación de acusados, indiciados o condenados, que se van a interceptar mediante grabación magnetofónica o parecidas, cualquier tipo de comunicación que se curse por cualquier red de comunicaciones, en donde se va a cursar información o haya interés para los fines de la actuación fiscal. De esta manera, las autoridades adecuadas serán las que se van a encargar de la operación técnica de la respectiva interceptación, así como del procesamiento. Los participantes de estas diligencias están obligados a guardar la debida reserva.

La orden tiene una vigencia máxima de seis (6) meses, pero se podrá prorrogar a juicio del fiscal si subsistiesen motivos fundados que la originaron. La orden del fiscal para prorrogar la interceptación de comunicaciones y similares se tendrá que someter al control previo de legalidad por parte del Juez de Control de Garantías.

Sobre la Recuperación de Información producto de la transmisión de datos a través de las redes de comunicaciones encontramos al Art. 236 en el que si el fiscal tiene motivos razonables fundados para inferir que el imputado puede manipular datos a través de las redes de telecomunicaciones, podrá ordenar a la policía judicial tanto la retención como aprehensión o recuperación de esa información u equipos terminales u dispositivos o servidores que hayan podido ser usados, para que luego los expertos en informática forense puedan obtener elementos materiales

probatorios o evidencias. Luego de realizado esto se tiene que hacer un Control de Legalidad Posterior dentro de las 24 horas siguientes al recibimiento del informe que emitirá la Policía sobre las diligencias realizadas, el fiscal tendrá que comparecer ante el Juez de Control de Garantías donde en audiencia se hará la revisión de la legalidad de todo lo actuado. El juez si lo estima pertinente va a interrogar directamente a los comparecientes y, luego de escuchar los fundamentos dados por el fiscal va a decidir de plano sobre la validez del procedimiento. (Art. 237).

3.2.4. España

En la legislación española tenemos como en todo país se garantiza la protección del secreto de las comunicaciones pero que este derecho puede suspenderse mediante una resolución judicial debidamente motivada, así lo establece el art. 18 inciso 3 de la Constitución española (aprobada por referéndum y entrando en vigor el 29 de diciembre de 1978). Encontramos, en la Ley de Enjuiciamiento Criminal (2015), a partir del art. 588 bis-a los principios rectores para que se puedan interceptar comunicaciones telefónicas como también la captación y/o grabación de comunicaciones orales mediante dispositivos electrónicos y el registro de dispositivos de registros remotos sobre equipos informáticos.

Para que se pueda dar la interceptación de las comunicaciones puede realizarse a través de dos caminos a seguir según la LECrim (2015), art. 588 bis-b:

a. El juez puede disponer de oficio esta medida.
b. El juez podrá disponer de esta medida a pedido de parte de un representante del Ministerio Fiscal o Policía Judicial
    - Cuando una de estas personas solicite dicha medida, la solicitud debe contener no solo la descripción del hecho objeto de investigación sino también la identidad del imputado o de cualquier otra persona que se encuentre afecto a la investigación.
    - Una exposición a detalle de las razones que justifiquen la necesidad de la medida.
    - Los datos para identificar al investigado o encausado.
    - Forma y duración de la medida.

Posteriormente en el art. 588 bis-c se aclara como se emitirá la resolución judicial autorizando la interceptación de las comunicaciones, teniendo que:

a. El juez pertinente va a autorizar o denegar la medida solicitada mediante un auto debidamente motivado, siendo que se tiene un plazo máximo de 24 horas para que se emita este pronunciamiento desde el momento que se ha presentado la solicitud.
b. La resolución judicial además deberá cumplir con ciertos términos como:
    - El hecho punible por el cual se está realizando la investigación y su calificación jurídica.
    - La identidad de las personas que se están investigando y de cualquier afectado por la medida.
    - Duración y forma de la medida.
    - La finalidad que persigue la medida.
    - El sujeto que va a llevar a cabo la medida, dicho sujeto debe guardar el secreto.

Referente a la interceptación con relación a delitos cometidos a través de instrumentos informáticos tenemos que, en la misma de Ley de Enjuiciamiento Criminal, en su art. 588 ter-a prescriba que la autorización para dar la interceptación podrá ser concedida cuando el hecho delictivo se cometa mediante instrumentos informáticos o de cualquier otra tecnología o servicio de comunicación; dicha intervención judicial va a autorizar el acceso al contenido de las comunicaciones como datos electrónicos. Esta medida además puede afectar a terceros cuando conste que el sujeto tercero investigado se sirve de aquella comunicación electrónica para recibir o transmitir información o también porque este tercero esté colaborando con la persona investigada en sus fines ilegales.

3.2.5. Chile

En esta legislación encontramos en su Constitución Política (promulgada el 18 de septiembre de 1925) al art. 19, inciso 4 y 5; que manifiestan que se protege la vida privada, la inviolabilidad de toda comunicación privada y que las comunicaciones pueden interceptarse bajo casos determinados por la ley.

Luego tenemos en su Código Penal (Código que fue promulgado el 12 de noviembre de 1874 y empezó a regir desde el 1 de marzo de 1875) en el art. 161-A que aclaran que se va a castigar o sancionar a todo aquel que intercepte comunicaciones de carácter privado. Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para realizar la interceptación de comunicaciones. Asimismo, en el art. 369 ter se tiene una perspectiva diferente a la de nuestra legislación ya que menciona que cuando existan sospechas fundadas de una persona u organización delictiva.

Finalmente hallamos al Código Procesal Penal (Ley 19696, promulgado el 29 de septiembre de 200 y con última modificación el 30 de noviembre del 2021) que respecto a la interceptación de comunicaciones telefónicas en su art. 222 manifiesta que podrá darse cuando existan fundadas sospechas, pero basándose en hechos determinados de que una persona hubiera cometido o participado en un delito y que además sea imprescindible para la investigación; teniendo así que, el juez competente podrá ordenar que se intercepte y se graben las comunicaciones telefónicas o de otras formas de telecomunicación. Mencionan además que las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida dando las facilidades del caso y que también deberán tratar toda esta información con carácter reservado.

CAPITULO IV: LOS DELITOS INFORMATICOS COMO SUPUESTO ESPECIAL DEL LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES

En el presente capitulo se demostrará la viabilidad de la hipótesis planteada en esta investigación está dirigida a que, con la incorporación de los DI como supuesto especial para el LSC, facilitaría la investigación realizada por el Ministerio Público a este tipo de ilícitos.

4.1. Fundamentos necesarios para la incorporación de los delitos informáticos como supuesto especial en el inciso 1 del artículo 230 del Código Procesal Penal

Los delitos informáticos han presentado dificultades en todos los ámbitos del derecho penal, siendo uno de ellos que el legislador decidió imprudentemente crear un marco punitivo penal para sancionar aquellas modalidades o conductas ilícitas las cuales se realizaban mediante el uso de TIC, en un claro ejemplo de querer luchar contra algo que desconocía, pues este no realizó un adecuado estudio de la política criminal entorno a los avances o uso de las TIC, en ese sentido el legislador siguió cometiendo errores al utilizar una mala técnica de redacción legislativa entorno a estos delitos o peor aún al promulgar normas sin contar con personal técnico especializado en la informática que pueda brindar ayuda a los operadores de justicia, o en su defecto no previo de mecanismos o herramientas de investigación al Ministerio Público, que faciliten la persecución e investigación de estos nuevos ilícitos. Es así que, Rayon y Gomez (2014), señalan que para la investigación y persecución de estos delitos se necesita diversos componentes como: unidades especializadas que estén dotadas de medios técnicos que garanticen la efectividad de la investigación y enjuiciamiento. (p. 03)

En ese sentido, una de las dificultades más relevantes de este tipo penal radica en torno a la solicitud del LSC, debido a que esta medida limitativa de derecho permite intervenir las comunicaciones con la finalidad de obtener información relevante que pueda ayudar a identificar al autor de los hechos o en su defecto recabar suficientes elementos de convicción que permitan continuar con la investigación y su posterior judicialización, sin embargo, al ser una medida limitativa de derechos se planteó en dicha norma que para solicitar el levantamiento se debe cumplir con los presupuestos materiales en un primer momento, es aquí que radica la dificultad de

la investigación de los delitos informáticos, debido a que estos tipos penales establecidos en la Ley N° 30096 no cumplen con la pena mínima requerida, originando las denegatorios en caso de que se solicite dicho levantamiento. Por lo que, dicha situación evidencia la dificultad que atraviesa el representante del Ministerio Público al realizar las investigaciones de los delitos informáticos, debido a que en estos casos se cuenta con poca información de cómo se cometió el ilícito producto de virtualidad, siendo necesarios en estos casos el LSC, pero al encontrarse limitados, usualmente se archivan de plano.

A. Datos estadísticos del Ministerio Público

En primer lugar, se tiene información brindada por la propia entidad encargada de la investigación y su persecución de los ilícitos, quienes evidencian en el gran impacto que ha tenido las nuevas conductas delictuales en la sociedad peruana durante los últimos siete años, según el informe de análisis N° 04, la DIVINDAT desde el 2013 hasta el 2020, ha recibido 12169 denuncias vinculadas a los delitos informáticos, teniendo su mayor incidencia en el año 2020, producto de la pandemia Covid-19. Mientras que, el Ministerio Publico es quien tiene un mayor índice de denuncias siendo estas 21687, que comprenden desde el año 2013 hasta el 2020, teniendo mayor incidencia de denuncias en la provincia de Lima Metropolitana con un total de 10 340, información que fue registrada en el SGF y SIATF. (OFAEC, 2021, p. 20-22)

Esto evidencia, que en los últimos años se ha venido teniendo un incremento en la criminalidad delictual entorno a la comisión de delitos informáticos, debido al constante avance de las TIC, poniendo en mayor peligro a la sociedad peruana al desconocer estas nuevas formas delictivas, y su escaso conocimiento sobre la seguridad informática, encontrándose cada vez más expuestas a estas, debido a la digitalización de la información y la facilidad de poder acceder a estas mediante las tecnologías.

Por otra parte, tenemos que existen hasta la fecha 12608 denuncias archivadas, 8842 en proceso de investigación y juzgamiento, 125 con sobreseimiento, 108 con sentencias y 4 con terminación anticipad, comprendiendo estas estadísticas desde el 2013 hasta el 2020 (OFAEC, 2021, p. 26); estas estadísticas evidencian que no existe una adecuada tutela efectiva de los bienes jurídicos establecidos en la Ley

N° 30096, demostrado mediante el alto porcentaje de denuncias que han sido archivadas.

Ahora bien, las estadísticas antes señaladas nos muestran el gran impacto que, han tenido las TIC en la criminalidad, y el avance exponencial que le lleva a las normas establecidas que tienen como fin sancionar estas nuevas conductas maliciosas.

B. Principales dificultades en la investigación de los delitos informáticos según los representantes del Ministerio Público

Por otro lado, es importante señalar cuales son las principales dificultades por las que atraviesan los representantes del Ministerio Público al realizar la investigación de los delitos informáticos, es así que la Oficina de Análisis Estratégico contra la Criminalidad – OFAEC (2021), realizo una entrevista a aquellos fiscales que tienen mayor incidencia de delitos informáticos, a fin de determinar cuáles son las principales dificultes de investigación y enjuiciamiento, siendo ellos quienes señalan que uno de las dificultades en la investigación, es debido a que los jueces niegan el LSC al no cumplir con los presupuestos materiales del artículo 230 del C.P.P.; asimismo, consideraron que los principales motivos de archivamiento o sobreseimiento es debido a que no se logra identificar al autor de los hechos, falta de capacitación, investigación deficiente, desconocimiento de la obtención y tratamiento de la prueba digital, falta de capacitación a fiscales y personal policial, y la falta de información. (pp. 37-38)

Valga decir que, de las entrevistas aplicadas a los fiscales con mayor incidencia de casos de delitos informáticos, se toma en cuenta que una de las principales dificultades de la investigación de los delitos informáticos radica en el solicitar la autorización del LSC, que serían de gran ayuda para poder obtener la identidad del sujeto agente o recaudar elementos de convicción que permitan el enjuiciamiento posterior, pero los delitos informáticos al no cumplir con uno de los presupuestos materiales de dicha norma, debido a las bajas penas que se imponen en estos tipos penales, por lo cual no podrían brindarle la autorización de acceder al secreto de las comuniones, careciendo así el caso de información para poder seguir con la investigación, provocando su posterior archivo, teniendo como fundamento que el

investigado no ha sido posible de identificar o que no se tiene suficientes elementos de convicción.

C. Fundamentos de los archivos de las carpetas fiscales sobre los delitos informáticos

Mediante el estudio de los fundamentos utilizados para el archivo de dos denuncias, el Ministerio Público ha establecido los siguientes:

- Caso Fiscal N° Nº 3106064501-2019-1751: se dispuso mediante Disposición N° 03-2020, No procede formalizar ni continuar con la investigación preparatorio:

  "**7.2.** Si bien existe datos sobre las cuentas a las que dichas transferencias llegaron a parar, también lo es que esta información está protegida por el derecho del secreto bancario el cual solo puede ser restringido por orden judicial y en el modo y forma de ley, lo cual puede considerarse como una atribución activada en base al requerimiento fiscal que sobre el particular se pueda solicitar, no es menos cierto que la investigación preliminar no es un simple formalismo condenado de antemano a un resultado infructuoso, pues tiene este pedido tiene que ir a la par de los elementos de convicción que se van recabando en la investigación, en cuyo seno cobra validez la declaración que sobre los hechos pueda verter el denunciante-agraviado y en base a la misma los futuros actos de investigación que nacen sobre sus alegaciones. E incluso respecto al ***levantamiento del secreto a las telecomunicaciones, conforme lo establece el artículo 230º.1 de la norma procesal penal,*** *"(...) cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad (...)",* y ***estando a que el delito de Fraude Informático previsto en el artículo 8º de la Ley Nº 30096 establece en su extremo mínimo una pena privativa de libertad de tres años, sería bastante discutible requerir levantar la información respecto a dicho extremo.***"
- Caso Fiscal N° 3106064501-2021-2287-0: se dispuso mediante Disposición N° 01-2021, No procede formalizar ni continuar con la investigación preparatorio:

“7.2. Si bien existe datos sobre la empresa a la cual se realizaron los pagos de las compras online realizadas, también lo es que esta información está protegida por el derecho del secreto bancario, el cual solo puede ser restringido por orden judicial y en el modo y forma de ley, lo cual puede considerarse como una atribución activada en base al requerimiento fiscal que sobre el particular se pueda solicitar, no es menos cierto que la investigación preliminar no es un simple formalismo condenado de antemano a un resultado infructuoso, pues este pedido tiene que ir a la par de los elementos de convicción que se van recabando en la investigación, en cuyo seno cobra validez la declaración que sobre los hechos pueda verter el denunciante-agraviado y en base a la misma los futuros actos de investigación que nacen sobre sus alegaciones. ***E incluso respecto al levantamiento del secreto a las telecomunicaciones, conforme lo establece el artículo 230º.1 de la norma procesal penal,*** *“(...) cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad (...)”,* y estando a que el delito de ***Fraude Informático previsto en el artículo 8º de la Ley Nº 30096 establece en su extremo mínimo una pena privativa de libertad de tres años, sería bastante discutible requerir levantar la información respecto a dicho extremo***.”

Es por ello que, según los fundamentos utilizados en las carpetas antes mencionadas, podemos concluir que uno de los principales argumentos de los fiscales se basa en que los delitos informáticos tienen un extremo de pena mínimo de tres años de libertad, no cumpliendo con el presupuesto material del LSC, el cual es que el delito sea sancionado con una pena superior de cuatros años, por lo cual sería infructuoso el solicitar dicha medida limitativa debido a que no contarían con suficientes fundamentos que le permitan lograr la autorización para poder solicitar información a las empresas de telecomunicaciones.

Por lo tanto, se hace una imperiosa necesidad el incorporar a los delitos informáticos como supuesto especial del LSC ya que, de los datos y fundamentos recabados en la presente investigación, en conjunto con lo referido por los entrevistados, concluimos que las dificultades que atraviesa la investigación de los

delitos informáticos al momento de solicitar el LSC, gira en torno al no cumplir con los presupuestos ya preestablecidos.

4.2. Los delitos informáticos como supuesto especial en la legislación española

La hipótesis planteada en la presente investigación está referida a que con la incorporación de los delitos informáticos como supuesto especial para el LSC, facilitará la investigación realizada por el Ministerio Público a este tipo de ilícitos, y para poder desarrollar esta, se ha tenido especial consideración la legislación española.

Es así, que tomamos como ejemplo a la Legislación Española, la cual determinó a los delitos informáticos como un presupuesto especial dentro del LSC debido a la trascendencias de este tipo de ilícitos, es así que en el artículo 588 ter a de la Ley Orgánica 13/2015 (2015), que modifica la LECrim, establece como presupuestos del LSC a los delitos cometidos a través de instrumentos informáticos, tecnología de la información o comunicación, para los cuales se puede solicitar autorización judicial de dicho levantamiento; debido a que la norma procesal pena peruana no ha considerado a los delitos informáticos como complejos y que requieren de mecanismos de investigación que se adecuen a estos, si bien es cierto existe en nuestra norma el LSC esta no se puede solicitar en el caso de los delitos informáticos, ya que no cumplen con los presupuestos materiales de la norma.

Asimismo, tenemos La Ley Orgánica 13/2015 (2015), incorpora nuevas medidas de investigación tecnológicas, con la finalidad de lograr una mayor protección a un conjunto de prácticas que faciliten la investigación y persecución de los ciberdelitos, debido a que las diligencias que antes se realizan vulneraban los derechos fundamentales y podían utilizarse como prueba, entre las novedades incorporadas a esta ley son figuras de investigación tecnológicas.

Teniendo en cuenta la legislación española sobre la intercepción de las comunicaciones telefónicas y telemáticas, la cual permite solicitar la autorización el LSC cuando se traten de delitos informático, en ese sentido se busca modificar mediante la incorporación el artículo 230 del C.P.P., en ese sentido el presente trabajo de investigación busca incorporar a los delitos informáticos como supuesto especial del LSC, con la finalidad de que el representante del Ministerio Público no

tenga dificultades en las investigaciones de estos delitos debido a su alta complejidad y trascendencia en la actualidad, por lo que dicha incorporación permitirá solicitar el levantamiento debido a que este resulte necesario para identificar al autor y recaudar elementos de convicción.

CAPITULO V: ASPECTOS METODOLÓGICOS

5.1. Tipo y diseño de investigación

El enfoque que se empleó en la presente tesis, es de enfoque cualitativo, según Cadena et al (2017), señalaron que este enfoque busca determinar la naturaleza de la realidad que se investiga a través de un estudio de los fenómenos obtenidos bajo técnicas como es la observación o las entrevistas para obtener mayor información y compresión de los resultados obtenidos; es decir que, la investigación cualitativa estudia los contextos situacionales o estructurales buscando conocer cuál es la naturaleza profunda de la realidad, su estructura dinámica o circular, en conclusión la investigación cualitativa se basa en la lógica y el proceso inductivo. Sobre el tipo de investigación, es necesario precisar que es de tipo aplicada, como se propuso en la CONCYTEC (2017) señalando que la investigación aplicada va a estar dirigida a resolver, por medio de un conocimiento científico, dichos medios por los que se puede cubrir una necesidad reconocida y específica; debido a que, utilizaremos la técnica de recolección de información a través de una guía de entrevista. Se utilizó el diseño fenomenológico, refiere que es un método de investigación sistemática en la que se busca obtener el conocimiento a partir de las experiencias de los individuos de manera que luego de esto pasa por un proceso de interpretación de la gente que define su exterior y actúa según esto por lo que el fenomenólogo va a mirar las cosas desde una perspectiva o punto de vista de otras personas de manera que va a describir, comprender e interpretar.

5.2. Categoría, subcategoría y matriz de categorización

Respecto a este punto tenemos que son apriorísticas, ya que, se fabricaron antes de la recolección de información, y nacieron a raíz de la propia investigación en el desarrollo de la presente investigación; la matriz de categorización se encuentra en el Anexo N° 01.

5.3. Escenario de estudio

Corresponde al lugar en el cual se realizó la investigación de la realidad problemática presentada en la presente investigación sobre el levantamiento de las comunicaciones en los delitos informáticos, con el fin de lograr obtener información relevante para absolver la interrogante planteada en esta investigación, siendo el escenario de estudio la 1°FPPCNCH, ya que los fiscales son los encargados de la investigación de los DI y de presentar el requerimiento del LSC

5.4. Participantes

Con respecto a las características de los participantes, Hernández et al. (2014), señaló que en algunas investigaciones de enfoque cualitativa es necesaria la postura u opinión de sujetos especializados en el tema a tratar para obtener datos precisos; se contó con la participación de:

- Cuatro Fiscales de la 1°FPPCNCH, su participación en la entrevista se debe a la cualidad específica al dirigir las investigaciones y experiencia adquirida a lo largo de su labor.
- Dos Asistentes de Función Fiscal de la 1°FPPCNCH, su participación en las entrevistas se debe a las funciones desarrolladas en su labor, como la de proyección de requerimiento.

5.5. Técnicas e instrumentos de recolección de datos

Con el fin de obtener resultados a favor y satisfactorios para la investigación se han utilizado las entrevistas a profundidad, siendo que los entrevistadores guiarán la conversación y el entrevistado manifestará sus diversas ideas u opiniones que serán relevantes para el desarrollo del tema de investigación.

5.6. Procedimiento

La recolección de información se realizó mediante el estudio teórico de los DI y el LSC, posteriormente se realizó la categorización y subcategorización del tema mediante el análisis de los objetivos que se plantearon, en esta investigación se recolecto los datos mediante la técnica de entrevista a profundidad, que se aplicó a los fiscales y asistentes de función fiscal de la 1°FPPCNCH, empleando la guía a profundidad, mediante videoconferencias de Google Meet; manteniendo una comunicación continua con los participantes; estas entrevistas quedaron grabadas

los cuales nos transmitirán sus conocimientos y sus puntos de vista respecto al tema de investigación. Así también se utilizará el análisis documental a la doctrina y jurisprudencia extranjera, para poder realizar el segundo objetivo específico de la presente investigación.

5.7. Rigor científico

La investigación debe cumplir con la calidad de investigación solicitada, por lo cual se desarrollaron los siguientes criterios:

- Credibilidad: las entrevistas se realizarán a fiscales y jueces especialistas en Derecho Penal, Derecho Procesal Penal. Los participantes mencionados tienen una reputación intachable.
- Confirmabilidad: se va a investigar de manera que encontraremos criterios que van a favorecer al desarrollo del mismo.
- Transferibilidad: los resultados que se logren adquirir van a servir a futuro como base para futuras investigaciones, que se puedan realizar respecto al tema, estos resultados adquiridos por la presente investigación se van a poder comparar con las investigaciones futuras, ya que los participantes con la misma condición de jueces o fiscales se pueden encontrar en cualquier parte del país por ende los resultados son transferibles independientemente del escenario de estudio.
- Consistencia: reside en que todos los datos que se obtengan, sean datos fijos, ya que siempre existirán jueces o fiscales especializados en Derecho Penal y Derecho Procesal Penal. Además, la figura jurídica de los ciberdelitos o el LSC siempre van a estar presentes en el ordenamiento jurídico peruano.

5.8. Método de análisis de datos

Para analizar los datos obtenidos tendremos en cuenta el siguiente esquema a llevar a cabo de manera ordenada y secuencial:

- Transcripción de las entrevistas a profundidad que se han de realizar.
- Análisis, visualización y reproducción del audio/vídeo de las entrevistas.
- Sistematización de los datos.
- Selección de las respuestas obtenidas por los participantes en relación a las categorías y subcategorías.

- Comparación de los datos obtenidos con los antecedentes y las teorías recabadas en el marco teórico.
- Instaurar posturas, fundamentos y conclusiones.

5.9. Aspectos éticos

La presente investigación se realizó conforme a los lineamientos del Código de Ética en Investigación de nuestra casa de Estudios, teniendo los siguientes criterios de transparencia y credibilidad:

- Principio de Autonomía: La selección de los sujetos de estudios fueron designado por el valor de la información que puedan aportar al estudio y no por cuestiones personales, son personas neutrales y de esta forma las respuestas u opiniones respetan a la ética del estudio. Además, no existe un conflicto de intereses y se estaría respetando el aspecto ético del estudio.
- Respeto a los sujetos: Existió un consentimiento informado y respeto hacia los participantes.
- Respeto a la información: La información brindada no se manipulo, por lo cual las respuestas brindadas fueron trascritas tal cual ha respondido el participante.

CAPITULO VI: Resultados y discusión

En este apartado se describió los resultados obtenidos mediante los instrumentos de recolección de datos de la guía de entrevista, teniendo en consideración los objetivos de la presente investigación.

6.1. Resultados

En primer lugar, se describirá los resultados de la guía de entrevista, ordenando la información de acuerdo a cada pregunta planteada.

Con respecto a la primera pregunta: ¿Qué entiende por ciberdelitos o delitos informáticos?

Los entrevistados E1, E2, E3 y E4 señalan que entienden por delitos informáticos, aquel comportamiento activo que busca introducirse en un sistema protegido por la informática con la finalidad de poder obtener una ventaja económica indebida, para lo cual se valen del empleo de sistemas y/o programas informáticos especializados, así como el ardid, el engaño, o el abuso de la confianza del titular del bien con contenido patrimonial. Por otro lado, los entrevistados E5 y E6, señalan que los delitos informáticos son aquellos que se realizan mediante el uso de TIC con el fin de causar un perjuicio a los datos o sistemas informáticos u otros bienes jurídicos tradicionales.

Asimismo, en la segunda pregunta, ¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?

Todos los entrevistados, indicaron que no existe una tutela efectiva de los bienes jurídicos protegidos en la presente ley, precisando que la tutela efectiva de los bienes jurídicos, proviene de una adecuada legislación punitiva que, antes de regularla, la proteja de conductas que tengan la idoneidad suficiente para vulnerarlas, pero dicha tutela, debe contar con herramientas jurídicas que permitan su investigación y persecución, o de ser el caso la prevención; en ese sentido si bien la ley ampara los bienes jurídicos vulnerados, esta no brinda herramientas o mecanismos que permitan realizar una adecuada investigación, de igual forma el legislador en su intento de regular nuevas conductas ilícitas no tomo en consideración regular herramientas que permitan esclarecer los hechos.

Continuando con la siguiente pregunta, ¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los delitos informáticos?

Los entrevistados E2, E3, E4, E5 y E6, señalaron que las penas establecidas en dicha norma no son las adecuadas debido que no resultan beneficiosas y que no están de acorde al daño causado en la victima; mientras que el entrevistado E1, refiere que si lo que se busca es eficiencia, antes que efectividad, en combatir este nuevo fenómeno, se debe verificar la idoneidad de los mecanismos o herramientas jurídicas existentes para su investigación, y es que, con una adecuada legislación procesal se puede llegar a la finalidad de la investigación y seguidamente circunstanciar debidamente una imputación, garantizando de una correcta pretensión punitiva estatal.

Con respecto a la cuarta pregunta, ¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los delitos informáticos?

Por unanimidad los entrevistados, concuerdan en que el LSC es de vital importancia, debido a que puede obtenerse la información sobre la identidad de los titulares de los números, en el caso hayan establecido comunicación con la víctima, desencadenándose así el actuar delictivo.

Con respecto a la pregunta número cinco, ¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación de los delitos informáticos?

La mayoría de los entrevistados E2, E3, E4, E5 y E6, señalan que los requisitos no facilitan la investigación de estos tipos penales, debido a que estos no cumplen con uno de los presupuestos, al tener penas menores de cuatro años, descartando la opción de poder solicitar el levantamiento, debido a que ya tienen conocimientos que este no será autorizado. Por otra parte, el entrevistado E1, refiere que el problema no radica en los requisitos y menos los presupuestos que establece el artículo 230° de la norma procesal penal, sino que radica en la técnica utilizada por el legislador, así como en las conductas descritas en la Ley N° 30096, esto es, los requisitos del art. 230° del CPP se encuentra en armonía con todo el sistema jurídico, pues el requisito de los 4 años de PPL constituye el barómetro que

garantiza una intervención estatal en la esfera de un derecho fundamental, además, que una adecuada investigación no está solo en función de un acto único como lo puede ser un LSC, sino por todo el conjunto de actos de investigación recopilados en la carpeta fiscal, señalando que lo que se debe procurar, es legislar con una mejor técnica narrativa los supuestos de hecho de las conductas que deben estar comprendidas como delitos informáticos y en ese sentido los agravantes constitutivos del tipo penal en específico, que finalmente podrán ser subsumidas en las conductas cuya sanción se presenta como superior a los 4 años de pena privativa de la libertad; de tal manera que muy bien podrá configurarse en el requisito que exige el art. 230° de la norma procesal.

Con respecto a la pregunta número seis, ¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?

Los entrevistados E2. E3, E4, E5 y E6, indican que la investigación de los delitos informáticos si se ve limitada, debido a que el levantamiento es uno de las principales de herramientas de investigación de estos delitos, pero debido a que estos ilícitos no cumplen con los presupuestos, optan por archivarlos; sin embargo, el entrevistados E1, considera que la investigación de los delitos informáticos no se ve limitada, debido a que existen otras técnicas y estrategias que deben ser repotenciadas.

Con respecto a la pregunta número siete, ¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los delitos informáticos, al ser estos complejos?

Los entrevistados E2. E3, E4, E5 y E6, manifestaron que si debería haber una modificatorio al artículo 230 del C.P.P., con la finalidad de facilitar la investigación y persecución de los delitos informáticos debido a su complejidad; mientras que, el entrevistado E1, señala que no debería existir una modificación, ni en los requisitos ni en los presupuestos, del art. 230° del CPP, sino que dicha modificación debería darse en los supuestos de hechos de la norma especial que regula los delitos informáticos, sin embargo, al compartirle la finalidad del presente trabajo de

investigación, manifestó estar de acuerdo en un modificatoria que consista en incorporar los delitos informáticos como un supuesto especial.

Con respecto a la pregunta número ocho, ¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los delitos informáticos por su complejidad?

En respuesta a este ITEM todos los entrevistados, manifestaron que sí, debido a que el LSC es una de las principales herramientas de investigación que podría aplicarse a este tipo de delitos, por lo cual la incorporación facilitaría la investigación de los delitos informáticos.

Con respecto a la pregunta número nueve, ¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP? Por unanimidad todos los entrevistados, manifestaron que una de las principales ventajas sería tener más facilidades para llegar a la identificación de los autores en esta clase de delitos y poder recabar suficientes elementos de convicción que permitan su posterior juzgamiento.

Con respecto a la penúltima pregunta: ¿Conoce usted legislaciones extranjeras en las cuales se permite el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad? La mayoría de los entrevistados E2, E3, E4, E5 y E6, indicaron que no conocen legislaciones extranjeras que regulen el LSC en el caso de los delitos informáticos. Por otra parte, uno de los entrevistados E1, señala que no conoce legislación extranjera, sin embargo, refiere que, al margen de las legislaciones, tendría que definirse antes que nada cuál es la razón para afirmar que estos delitos son complejos y sobre todo cuál es la causal que alberga dicha premisa fáctica.

Finalmente, ante la última pregunta: Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?, todos los entrevistados señalaron que en la legislación española, se tienen más avance en la parte procesal del derecho penal, por cual creen conveniente que esta norma como puede ser tomada como

referencia para que el legislador incorpore al artículo 230 los delitos informáticos, para garantizar una mejor investigación de este tipo delictivo.

6.2. Discusión

En esta sección se realizará la discusión de resultados obtenidos de los instrumentos de recolección de datos para corroborar si nuestra hipótesis:

Respecto al primer objetivo específico: **Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones**

En torno a las dificultades que presenta la investigación de los delitos informáticos, hemos considerado pertinente saber si los entrevistados tienen conocimiento de los delitos informáticos, definiéndolo como aquel comportamiento activo que busca vulnerar un sistema protegido por la informática, con el fin de poder obtener un provecho económico, valiéndose del uso de sistemas o programas informáticos, sin embargo, estas conductas causar un daño a los datos o sistemas informáticos u otros bienes jurídicos tradicionales; en ese sentido, podemos definir a los delitos informáticos como aquel comportamiento que se realiza mediante el uso de las TIC, buscando ocasionar un perjuicio a los datos, red o sistemas informáticos, u otros bienes jurídicos. Asimismo, se cuestionó si la Ley N° 30096 brinda una tutela efectiva de los bienes jurídicos, señalando que, si bien el legislador cumplió con regular estas nuevas conductas ilícitas para proteger a la sociedad, este no conto con implementar herramientas jurídicas especializadas que permitan la investigación y persecución de estos ilícitos, como lo señala el entrevistado E1, debe existir funcionalidad entre la norma sustantiva con la norma procesal; en este sentido, podemos señalar que no existe una efectiva tutela de esto bienes jurídicos. Es por ello, que se cuestionó si las penas aplicadas para sancionar este tipo de delitos son adecuadas, sosteniendo la mayoría entrevistados que las penas establecidas en estos ilícitos no son las más adecuada para sancionar este tipo de delitos, debido a que resultan beneficiosas para el delincuente, y no justifican el daño causado al agraviado, por otra parte, tenemos que el problema no radica en las penas sino que radican en que el legislador no ha previsto implementar un adecuada legislación procesal, como ya se ha señalado anteriormente, no existen

mecanismos o herramientas idóneos que contribuyan a la investigación de estos delitos.

Por consiguiente, es pertinente tratar si el LSC es de vital importancia en la investigación de los ciberdelitos, obteniéndose de los resultados que esta medida es muy importante, debido a que mediante esta se puede obtener información relevante para la continuación de la investigación y posterior enjuiciamiento, tales como la identidad del sujeto activo, lugar desde donde se generó el delito; por lo que podemos colegir que el LSC, es un instrumento de vital importancia en la investigación de los delitos informáticos, ya que este se podría utilizarse para recabar elementos de convicción que ayuden identificar al autor de este tipo de delitos; sin embargo, estos no cumplen con los presupuestos materiales establecidos en la norma procesal, es así que el levantamiento no se utiliza en las investigaciones de estos delitos. A lo referido en el párrafo anterior, tenemos que los requisitos o presupuestos establecidos en el primer inciso del artículo 230 del C.P.P., según la mayoría de los entrevistados, los requisitos de esta norma procesal no permiten que el representante del Ministerio Público pueda solicitar el levantamiento, porque como ya lo hemos mencionado anteriormente los delitos informáticos no cumplen con el requisito de la pena sea mayor a los cuatros años, por lo cual la investigación se un ve un tanto limitado, dificultando al fiscal que otras diligencias podría realizar para continuar con la investigación de estos hechos delictivos.

Con respecto a lo principalmente referido en el presente objetivo, podemos arribar a que, si existen dificultades en la investigación de los delitos informáticos, principalmente ante la denegatoria de la autorización del LSC, debido a que toda medida limitativa de derecho requiere que se cumplan presupuesto materiales y sustanciales para poder otorgarlo, siendo uno de los presupuestos materiales que el delito sancionado tenga como pena mayor de cuatro años de pena privativa de libertad, en este caso los delitos informáticos no cumplen con los parámetros referidos a la pena en la norma procesal.

Con respecto a la hipótesis planteada ***“La incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las***

comunicaciones, facilitaría la investigación realizada por el Ministerio Público".

Podemos señalar que la hipótesis planteada se ve fielmente respaldada, por los resultados obtenidos en el presente proyecto, al quedar demostrado que la principal dificultad en la investigación de los delitos informáticos radica en las denegatorias del levantamiento, originando que no exista una tutela efectiva de estos bienes jurídicos, en este sentido señalaron que el levantamiento es de vital importancia para la investigación de estos delitos, por lo cual se requiere de una mejor regulación en el ámbito procesal, es por eso, que la incorporación de los delitos informáticos como supuesto especial en el levantamiento del secreto de las comunicaciones, resultaría beneficioso para facilitar la investigación realizada por el Ministerio Público, para este tipo de hechos delictivos; apoyando lo planteado tenemos que los entrevistados manifestaron que debe existir una modificación al artículo 230 C.P.P., siendo esta la incorporación de los delitos informáticos como supuesto especial en el levantamiento, con la finalidad de poder facilitar la investigación y persecución.

Respecto al segundo objetivo específico: **Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones**

Con respecto al presente objetivo se obtuvo que los entrevistados no conocen legislaciones extranjeras referentes a los delitos informáticos y el levantamiento de secreto de las comunicaciones, e incluso desconocen cómo se desarrolla la investigación de este tipo de delito, por lo cual no tenían sustento para referir si es que en alguna legislación se concede la autorización del levantamiento en la investigación de los delitos informáticos.

Es así que se le planteo que en la legislación española se permite solicitar la autorización de esta medida, planteándose como un presupuesto, que se encuentra establecido en el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal, especificando que dichos presupuestos se incorporaron ante la necesidad de implementar nuevas medidas de investigación tecnológicas debido al gran avance de la cibercriminalidad, de esta manera, al plantearles cómo opera la legislación española, señalaron que sería adecuado tomar como ejemplo dicha norma para

que el legislador pueda evaluar e incorporar los delitos informáticos como un supuesto especial, atendiendo a las dificultades que presentan la investigación de estos delitos y la carecían en normativa procesal respecto a los avances tecnológicos en la sociedad.

Con respecto a la hipótesis planteada ***"La incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones, facilitaría la investigación realizada por el Ministerio Público".***

Podemos indicar que nuestra hipótesis se ve respaldada por los resultados obtenidos, pues señalan que están a favor de poder incorporar una norma procesal más adecuada para garantizar y facilitar la investigación de este tipo penal, como se ha venido dando en España durante los últimos años con respecto a la investigación de los delitos informáticos, y al adaptar su norma procesal a las nuevas tecnologías; es así que podemos corroborar que resulta necesario incorporar los delitos informáticos como supuesto especial para poder solicitar la autorización del levantamiento del secreto de las comunicaciones, lo que facilitara la investigación realizada por el Ministerio Público a este tipo de ilícitos.

CONCLUSIONES

1. En relación al desarrollo del presente trabajo de investigación, llegamos a concluir que se debe incorporar los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones, para facilitar la investigación de este tipo de ilícito; porque se demostrado que existen dificultades en la investigación de los delitos informáticos, siendo la principal dificultad el obtener la autorización del levantamiento del secreto de las comunicaciones, dado que este tipo de delitos no cumple con uno de los presupuesto materiales requeridos en el numeral 1 del artículo 230 del Código Procesal Penal, esta dificultad repercute en la investigación, ya que esta medida permite poder identificar al titular de la acción o recabar elementos de convicción que permitían tener indicias del autor de los hechos, sin embargo al no realizarse esta medida, diversos casos son archivados o incluso se puede usar como fundamento para archivar las denuncias, el no poder solicitar el levantamiento como se ha señalado en los dos casos estudiados en la investigación; esta situación en España aun no teniendo una ley especial de delitos informáticos, considera que es de vital importancia esta medida por lo que en su normativa procesal ampara el levantamiento en este tipo de delito, al considerarlos transcendentes y complejos; a diferencia de nuestra legislación que no la regula, generando dificultades en la investigación de este ilícito.

2. Se concluyó que los delitos informáticos presentan dificultades durante su investigación y persecución, lo que demuestra que no existe una tutela efectiva de los bienes jurídicos protegidos por la ley de delitos informáticos, debido a que las penas impuestas en dicha norma legal no cumplen con los presupuestos del levantamiento del secreto de las comunicaciones, por lo cual se requiere un adecuado estudio de la política-criminal para que la norma sustancial encuentre funcionalidad en la norma procesal, y poder garantizar una adecuada investigación.

3. Se concluye que, la legislación penal española garantiza una efectiva tutela de los bienes jurídicos amparados en los delitos informáticos aun sin contar con una ley especial, sin embargo, debido a que cuentan con una norma procesal penal más adecuada para realizar la investigación de este tipo de delitos, basándose en la gravedad del hecho.

RECOMENDACIONES

PRIMERO: Se recomienda modificar el artículo 230 del Código Procesal Penal, incorporando los delitos informáticos como supuesto especial por su nivel de complejidad y trascendencia, para poder solicitar y obtener la autorización judicial del levantamiento del secreto de las comunicaciones, para facilitar la investigación de los ciberdelitos, para dicha incorporación debe tenerse en consideración el Proyecto de Ley (Anexo N° 06), que se encuentra en los anexos de la presente investigación, teniendo presente el artículo 107 de la Carta Magna, con respecto a la iniciativa legislativa que gozan el presidente, los congresistas, el Colegio de abogados y la población; el objetivo del presente trabajo es que las autoridades tomen conocimiento sobre el proyecto de ley y se presente con el objetivo de modificar una norma procesal para garantizar la investigación de delitos complejos como lo son los ciberdelitos.

SEGUNDO: Implementar medidas destinadas a combatir los delitos informáticos por ser un sector vulnerable ante el crecimiento y desenvolvimiento de las nuevas tecnologías, una de esas medidas que podría proponerse sería: Tener una adecuada capacitación constante a los diversos usuarios de algún tipo de tecnología sea desde la más mínima hasta el máximo conocimiento de ella.

TERCERO: Adecuar las normas procesales penales al incipiente avance de las tecnologías, con la finalidad de poder implementar nuevas medidas de investigación tecnológicas en la legislación penal peruana.

REFERENCIAS BIBLIOGRAFICAS

Abushihab, A. (2016). *Cibercrimen: una aproximación a la delincuencia informática*. [Tesis de Maestría, Universidad Santo Tomás]. https://repository.usta.edu.co/bitstream/handle/11634/1995/Abushihabamir2016.pdf?sequence=1&isAllowed=y

Acurio, S. (2016). *Delitos informáticos: generalidades.* [Archivo PDF] http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Amazon Web Services (2021). *¿Qué es un ataque DDOS?* https://aws.amazon.com/es/shield/ddos-attack-protection/

Arifi, D. y Arifi, B. (2021). *Cybercrime: A Challenge to Law Enforcement.* SEEU Review,15*(2)* 42-55. https://doi.org/10.2478/seeur-2020-0016

Basu, S. & Jones, R. (2007). *Regulating cyberstalking*, en JILT, (vol. 22) https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.8224&rep=rep1&type=pdf

Cabrera, M. (2020). *Fundamentos jurídicos considerados por los fiscales del Cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el período 2010 – 2018.* [Tesis para optar el título de abogado, Universidad Privada del Norte] https://repositorio.upn.edu.pe/bitstream/handle/11537/24533/Cabrera%20Quiroz%2c%20Marycarmen.pdf?sequence=1&isAllowed=y

Cadena, P., Rendón, R., Aguilar, J., Salinas, E., De la Cruz, F. y Sangerman, D. (2017). *Métodos cuantitativos, métodos cualitativos o su combinación en la investigación: un acercamiento en las ciencias sociales.* Revista Mexicana de Ciencias Agrícolas, 8(7),1603-1617. ISSN: 2007-0934. https://www.redalyc.org/pdf/2631/263153520009.pdf

Cano, Q. (11 de mayo del 2020). *Fenomenología de la ciberdelincuencia*. [Mensaje en un blog]. https://cibercrim.com/fenomenologia-de-la-ciberdelincuencia/

Castellanos, C. (2020). *Modalidades de Cibercrimen en tiempos de Pandemia Covid-19 en Bogotá, Colombia.* [Ensayo, Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/37304

Chamarro, S. (2019). *Las nuevas medidas de investigación tecnológica limitativas del derecho al secreto de las comunicaciones en el proceso penal.* [Tesis de maestría, Universidad de Alcalá]. https://ebuah.uah.es/dspace/handle/10017/40857

Chavarría, E., Jirón, M. y Miranda, F. (2016). *La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, El Salvador y Nicaragua*. [Tesis de licenciatura, Universidad Nacional Autónoma de Nicaragua]. http://repositorio.cnu.edu.ni/Record/RepoUNANL5316

Chiluisa, D. (2021). *Los delitos informáticos y los vacíos legales que afectan a los ciudadanos.* [Tesis para obtener el título de abogado, Universidad Católica de Santiago de Guayaquil]. http://repositorio.ucsg.edu.ec/bitstream/3317/16501/1/T-UCSG-PRE-JUR-DER-MD-334.pdf

Chua, C. & Wareham, J. (2004). *Fighting Internet Auction Fraud: An Assessment and Proposal Computer*, en IEEE Computer, núm. 10

Código Penal. Ley N° 26.388, 24 de junio de 2008. (Argentina) https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

Código Procesal Penal. Decreto Legislativo 957, 22 de Julio del 2004. (Perú). https://lpderecho.pe/nuevo-codigo-procesal-penal-peruano-actualizado/

Código Procesal Penal. Ley N° 23.984, 09 de septiembre de 1991. (Argentina). http://spij.minjus.gob.pe/Graficos/Legcomp/sudamerica/Argentina/CODIGO_PROCESAL_PENAL.pdf

Congreso de la República de Argentina. (1972, 22 de agosto). Ley N° 19.788. *Por la cual se expide la Ley Nacional de Telecomunicaciones.* Ministerio de Justicia y Derechos Humanos Presidencia de la Nación. http://servicios.infoleg.gob.ar/infolegInternet/anexos/30000-34999/31922/texact.htm

Congreso de la República de Argentina. (2001, 03 de diciembre). Ley N° 25.520. *Por la cual se expide la Ley de Inteligencia Nacional*. Ministerio de Justicia y Derechos Humanos Presidencia de la Nación.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/7000074999/70496/texact.htm

Congreso de la República de Bolivariana de Venezuela. (2001, 30 de octubre). Ley N° 37.313. *Por la cual se expide la Ley Especial Contra los Delitos Informáticos.* Gaceta Oficial. https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Congreso de la Republica de Chilena. (1993, 07 de junio). *Ley N° 19223. Por la cual se expide la Ley que tipifica figuras penales relativas a la informática.* Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=30590

Constitución Política de Argentina. (1853). *Casa Rosada Presidencia.* https://www.casarosada.gob.ar/nuestro-pais/constitucion-nacional#:~:text=El%201%C2%BA%20de%20mayo%20de,tras%20la%20Revoluci%C3%B3n%20de%20Mayo

Constitución Política del Perú. (1993). *Diario Oficial El Peruano.* *http://www.pcm.gob.pe/wp-content/uploads/2013/09/Constitucion-Pol%C3%ADtica-del-Peru-1993.pdf*

Coronado, R. y Segura, L. (2018). *La actuación del representante del Ministerio Público frente al levantamiento del secreto de las comunicaciones.* [Tesis para optar el título de abogado]. https://repositorio.uss.edu.pe/handle/20.500.12802/6051

Cristiano, K. y Moyarga, M. (2015). *Análisis Criminológico del Cibercrimen.* [Proyecto de Investigación, Universidad la Gran Colombia]. https://repository.ugc.edu.co/bitstream/handle/11396/4239/An%C3%A1lisis_criminol%C3%B3gico_cibercrimen.pdf?sequence=1&isAllowed=y

Díaz, C. (2019). *La aplicación de la ley N° 30096 – Ley de delitos informáticos respecto a su regulación en el derecho penal peruano.* [Tesis para optar el título de abogado, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/51569/D%c3%adaz_BCZ-SD.pdf?sequence=1&isAllowed=y

Elias, R. (2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú. Revista Hiperderecho* (01). https://hiperderecho.org/2014/07/luces-y-sombras-de-la-delincuencia-informatica-en-peru/

Fernández Teruelo, J. G. (2019). *Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red. Revista De Derecho Penal Y Criminología*, (19), 217–243. http://revistas.uned.es/index.php/RDPC/article/view/24951

Fernandez, P. (2020). *Análisis del artículo 5º de la Ley Nº 30096 en la prevención de los delitos informáticos contra la indemnidad sexual.* [Tesis para optar el título de abogada, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/46921?show=full

Gallardo, A. (2020). *Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019.* [Tesis para optar el título de abogado, Universidad Científica del Perú]. http://repositorio.ucp.edu.pe/bitstream/handle/UCP/984/GALLARDO_DER_TESIS_TITULO_2020.pdf?sequence=1

Gómez, J. (2020). *El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019.* [Tesis para optar el título de abogada, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/53071/G%c3%b3mez_VJC-SD.pdf?sequence=1&isAllowed=y

Henson, B. (2010). *Cyberstalking* en Fisher, B. s., y Lab, s. P. (eds.). *Encyclopedia of Victimology and Crime Prevention,* Thousand Oaks, CA, Sage.

Hernández, L. (2009). *El Delito Informático.* Cuaderno del Instituto Vasco de Criminología Núm. 23 Pág. 227-243. https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Hernández, R; Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación*. (6.a ed.) Mg. Graw-Hill Interamericana. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Herrera, J. (2017). *La investigación cualitativa.* http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/1167

Hong, J. (2012). *The State of Phishing Attacks*, en Communications of the ACM, (vol. 55, núm. 1).

Jaishankar, K. (2008). *Identity related Crime in the Cyberspace: Examining Phishing and its impact*, en IJCC, (vol. 2).

Jakobsson, M. (2005). *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft, John Willey & Sons*.

Keats, D., y Norton, H. (2011). *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, en Boston University Law Review, (vol. 91)

López, L. y otros (2010). *Manuales Derecho Constitucional*, Editorial Tirant Lo Blanch, Volumen I, España. https://dialnet.unirioja.es/servlet/libro?codigo=676411

Lusthaus, J. (2016). *Cybercrime: The Industry of Anonymity.* [Tesis doctoral, Universidad de Oxford, Estados Unidos de América]. https://ora.ox.ac.uk/objects/uuid:80d9d881-586d-42ef-b56e-7c140d396a73/download_file?file_format=pdf&safe_filename=Cybercrime%2520-%2520Library%2520Submission.pdf&type_of_work=Thesis

Manson, M. *Legislación sobre delitos informáticos,* en https://dl.dropbox.com/u//dl.legislacioncomparada.pdf [visto el 01 de diciembre 2021].

Marco, A. (2010). *La intervención de las Comunicaciones telefónicas: grabación de las conversaciones propias, hallazgos casuales y consecuencias jurídicas derivadas de la ilicitud de la de la injerencia.* [Tesis doctoral, Universidad Autónoma de Barcelona]. https://www.tesisenred.net/bitstream/handle/10803/32087/amu1de1.pdf?sequence=1

Martínez, B., y Abreu, V. (2015). *Análisis del fenómeno de los ciberdelitos en el Municipio de Moca enero – abril 2015.* [Monografía para optar el título de

licenciados en Derecho, Universidad Tecnológica de Santiago, República Dominicana].

Matusan, C. (2013). *La Acción Penal Privada y la afectación de derechos fundamentales. Revista VIA IURIS*, (14),187-197. ISSN: 1909-5759. https://www.redalyc.org/pdf/2739/273929754011.pdf

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos. Revista Chilena de Derecho*, 44(1), 261-285. ISSN: 0718-3437. http://dx.doi.org/10.4067/s0718-34372017000100011

Mesia, C. (2010). *Derechos de la Persona Dogmática Constitucional*. Fondo Editorial del Congreso de la República, Lima-Perú.

Miró, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Marcial Pons.

Montiel, I. (2016). *Cibercriminalidad social juvenil: la cifra negra.* Revista de Internet, Derecho y Política, (22),108-120. ISSN:1699-8154. https://www.redalyc.org/pdf/788/78846481008.pdf

Moscoso, R. (2014). *La Ley 19.223 en general y el delito de hacking en particular.* En Revista Chilena de Derecho y Tecnología, 3 *(1)* pág. 11 – 78. Universidad de Chile (Santiago). DOI 10.5354/0719-2584.2014.32220

Neyra, M. y Tresierra, A. (2017). *El procedimiento de intervención, grabación o registro de comunicaciones telefónicas sin las garantías previstas en el Código Procesal Penal de 2004 y su vulneración al derecho fundamental al secreto y la inviolabilidad de las comunicaciones.* [Tesis para optar el título de abogado, Universidad Nacional de la Amazonia Peruana]. https://repositorio.unapiquitos.edu.pe/handle/20.500.12737/4717

Núñez, R. y Correa, C. (2017). *La prueba ilícita en las diligencias limitativas de derechos fundamentales en el proceso penal chileno.* Revista Ius et Praxis, 23(1), 195-246. ISSN: 0718-0012. http://dx.doi.org/10.4067/S0718-00122017000100007

OECD, Malicious Software (Junio 2008): *A Security Threat to the Internet Economy*, OECD.

https://www.oecd.org/sti/consumer/computerviruesandothermalicioussoftwareathreattotheinterneteconomy.htm

Paredes, J. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009 – 2010.* [Tesis para maestría, Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Pons, V. (2018). *Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional. [T*esis de doctorado, Universidad Nacional de Educación a Distancia]. http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf

Posada, R. (2017). *Los cibercrímenes: un nuevo paradigma de criminalidad*. Un estudio del Título VII bis del Código Penal colombiano (1ª ed.). Editorial Ibáñez. https://dialnet.unirioja.es/servlet/libro?codigo=719813

Rayón, M. y Gómez, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Revista de Anuario Jurídico y Económico Escurialense*, XLVII 209-234/ ISSN:1133-3677. https://dialnet.unirioja.es/servlet/articulo?codigo=4639646

Reglamento de calificación y registro de investigadores en ciencia y tecnología del sistema nacional de ciencia, tecnología e innovación tecnológica - SINACYT. (30 de diciembre de 2017). Diario El Peruano. https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-de-calificacion-y-registro-de-invest-resolucion-n-198-2017-concytec-p-1602543-1/

Reyna, L. (2001). *El bien jurídico en el delito informático.* Revista electrónica de derecho informático, (33).

Romeo, C. (2006). *El cibercrimen: nuevos retos jurídico-penales, nuevas perspectivas político criminales.* Editorial Comares. https://dialnet.unirioja.es/servlet/libro?codigo=571090

Rubio, M. (2008). *La interpretación de la Constitución según el Tribunal Constitucional.* Editorial PUCP, Tomo I, Lima-Perú.

Salinas, R. (2013). *Derecho Penal: Parte especia*l. (5ª ed.) Editorial Grijley,

San Martín, C. (2017). *Derecho Procesal Penal Peruano Estudios.* Gaceta Jurídica.

Şcheau, M. y Pop, S. (2018). *Cybercrime Evolution.* International conference KNOWLEDGE-BASED ORGANIZATION, 24*(1)* 225-229. https://doi.org/10.1515/kbo-2018-0034

Serrano, A. (2009). Oportunidad y Delito. Introducción a la criminología (6 ª ed.). Editorial Dykinson. https://www.marcialpons.es/libros/oportunidad-y-delito/9788498496925/

Shadel, D (2012). *Outsmarting the Scam Artist: How to Protect Yourself From the most Clever Cons*, Wiley.

Staddler, W. (2010). *Internet Fraud*. Fisher, B. s., y Lab, s. P., Encyclopedia of Victimology and Crime Prevention, (vol. 1), California/London, Sage Publications.

Toledo, E. (2019). *Levantamiento del secreto de las comunicaciones a agraviados y testigos y el debido proceso en Trujillo durante 2017*. [Tesis para optar el título de abogado, Universidad Nacional de Trujillo]. https://dspace.unitru.edu.pe/handle/UNITRU/13073

Tribunal Constitucional. (2014, 17 de julio). Sentencia Exp. N° 00867-2011-PA/TC APURIMAC (Alan Siasmany Quintano Saravia). https://tc.gob.pe/jurisprudencia/2015/00867-2011-AA.pdf

Varsi, E. (2014). *Tratado de Derecho de las Personas*, Editorial Gaceta Jurídica S.A. (1ª ed.).

Vega, J. (201). *Los delitos informáticos en el Código Penal*. [Tesis para optar el grado de magister, Universidad Católica de Santa María]. https://alicia.concytec.gob.pe/vufind/Record/UCSM_fa158dffcd96c62de133b3499aa2a814/Details

Villavicencio, F. (2014). *Delitos Informáticos.* Revista IUS ET veritas, 24*(49)*, 284-304. http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Vivila, B. (2016). *Falta de motivación e indebida afectación del secreto de las comunicaciones Telefónicas.* [Tesis para optar el título de abogada, Universidad Andina Néstor Cáceres Velásquez]. http://repositorio.uancv.edu.pe/handle/UANCV/547

Yar, M. (2005). *The novelty of cybercrimo: an assessment in light of routine activity theory,* en EJC, (núm. 2).

Yeargain, J.; Settoon, R. & McKay, S. (2004). Can-Spam act of 2003: How to spam legally, en JSeC, (vol. 2, núm. 1)

ANEXOS

Anexo N° 1. Matriz de Categorización Apriorística

ÁMBITO TEMÁTICO	PREGUNTA DE INVESTIGACIÓN	OBJETIVO GENERAL	OBJETIVOS ESPECIFICOS	CATEGORIAS	SUBCATEGORÍAS
DERECHO PROCESAL PENAL	¿En qué medida la modificación del código procesal penal en torno al levantamiento secreto de las comunicaciones facilitaría una investigación efectiva de los delitos de cibercrimen?	Proponer la modificación del art. 230 del Código Procesal Penal de modo a incorporar un párrafo relativo a los cibercrímenes	Establecer los requisitos de procedencia del levantamiento del secreto de las comunicaciones para facilitar la investigación de los ciberdelitos	Criminalidad Informática	Delitos informáticos Ley N° 30096
				Levantamiento del secreto de las comunicaciones	Importancia de la medida Dificultades de la medida Incorporación de un supuesto especial en la medida
			Comparar las legislaciones extranjeras referentes al levamiento del secreto de las comunicaciones	Legislación Internacional	Legislación Argentina Legislación Venezolana Legislación Colombiana Legislación Chilena Legislación Española

Anexo N° 2

ENTREVISTA A LOS OPERADORES JURIDICOS

Buenos días/tardes/noches, Dr. ……..., actual …….. de la ……., la presente entrevista tiene como propósito el conversar y conocer sus puntos de vista respecto a una eventual reforma del art. 230 del Código Procesal Penal respecto al levantamiento del secreto de las comunicaciones para los delitos informáticos, vale decir que estos se puedan incorporar como presupuesto especial al levantamiento del secreto de las comunicaciones, en razón a que son delitos de alta complejidad para individualizar al autor, siendo este requerimiento de vital importancia para poder recabar suficientes indicios o elementos de convicción los cuales servirán para la continuación de la investigación respecto a los delitos informáticos. De antemano le agradezco por su tiempo brindado y por la desinteresada colaboración que tiene, siendo este tema de vital importancia para un mayor alcance al momento de investigar los delitos informáticos. El alcance que se pretende obtener es su perspectiva respecto al tema materia de investigación, cabe mencionar además que se salvaguardan los datos personales hacia su persona teniendo como prioridad la confidencialidad.

CIBERDELITOS

¿Qué entiende por ciberdelitos o delitos informáticos?

¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?

¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los delitos informáticos?

LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES

¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los delitos informáticos?

¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?

¿Considera usted que la investigación de los delitos informáticos se ve limitada por los presupuestos establecidos el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?

¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los delitos informáticos, al ser estos complejos?

¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los delitos informáticos por su complejidad?

¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?

¿Conoce usted legislaciones extranjeras en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?

Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?

Se le agradece por su tiempo brindado y por su participación en la encuesta, la cual servirá para el desarrollo de la presente investigación.

UNIVERSIDAD CÉSAR VALLEJO

Anexo N° 3

MATRIZ DE VALIDACIÓN A JUICIO DE EXPERTO DE LAS VARIABLES *CIBERDELITOS* Y *LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES*.

TÍTULO: Levantamiento del secreto de las comunicaciones en los delitos informáticos.
AUTORES: Lunarejo Guevara Erick Bryan y Rodríguez Gil Karla Olinda.

VARIABLE	DIMENSIONES	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN								OBSERVACIONES Y RECOMENDACIONES
				Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítems		Relación entre el ítems y la opción de respuesta		
				Si	No	Si	No	Si	No	Si	No	
Ciberdelitos	Criminalidad Informática	**Delitos informáticos**	**¿Qué entiende por ciberdelitos o delitos informáticos?**	X								
		Bien jurídico protegido	**¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?**	X								
		Ley N° 30096 (Ley de delitos informáticos)	**¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los ciberdelitos?**	X								

Levantamiento del secreto de las comunicaciones	**Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**	**Importancia de la medida**	**¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los ciberdelitos?**	X								
		Requisitos de la medida	**¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?**	X								
		Limitaciones de la medida	**¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?**	X								
		Modificación al art. 230 del Código Procesal Penal para las diligencias preliminares de delitos informáticos	**¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los ciberdelitos, al ser estos complejos?**	X								
			¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los ciberdelitos por su complejidad?	X								
			¿Cree usted que una modificación al art. 230 del Código Procesal Penal podría llevarse a cabo con la finalidad de facilitar las investigaciones en etapa de diligencias preliminares para una adecuada y exhaustiva búsqueda de información para los ciberdelitos?	X								
			¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?	X								
		Legislaciones Internacionales	**¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?**	X								
			Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?									

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: “Guía de entrevista a profundidad para recabar opiniones acerca del levantamiento del secreto de las comunicaciones en los delitos informáticos”

OBJETIVOS:

- **Objetivo General:**
  - Proponer la incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones el cual facilitaría la investigación del Ministerio Publico
- **Objetivos específicos:**
  - Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones
  - Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones

DIRIGIDO A:

- Fiscales y Asistentes Función Fiscal de la Primera Fiscalía Provincial Penal Corporativa de Nuevo Chimbote.

……
……..

APELLIDOS Y NOMBRES DEL EVALUADOR: Marin Chung Pedro Cesar

GRADO ACADÉMICO DEL EVALUADOR: Magister en Gestión Pública

VALORACIÓN:

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

FIRMA DEL EVALUADOR

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN A JUICIO DE EXPERTO DE LAS VARIABLES *CIBERDELITOS* Y *LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES*.

TÍTULO: Levantamiento del secreto de las comunicaciones en los delitos informáticos.
AUTORES: Lunarejo Guevara Erick Bryan y Rodríguez Gil Karla Olinda.

VARIABLE	DIMENSIONES	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN								OBSERVACIONES Y RECOMENDACIONES
				Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítems		Relación entre el ítems y la opción de respuesta		
				Si	No	Si	No	Si	No	Si	No	
Ciberdelitos	Criminalidad Informática	**Delitos informáticos**	**¿Qué entiende por ciberdelitos o delitos informáticos?**	X								
		Bien jurídico protegido	**¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?**	X								
		Ley N° 30096 (Ley de delitos informáticos)	**¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los ciberdelitos?**	X								

Levantamiento del secreto de las comunicaciones	**Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**	**Importancia de la medida**	**¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los ciberdelitos?**	X								
		Requisitos de la medida	**¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?**	X								
		Limitaciones de la medida	**¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?**	X								
		Modificación al art. 230 del Código Procesal Penal para las diligencias preliminares de delitos informáticos	**¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los ciberdelitos, al ser estos complejos?**	X								
			¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los ciberdelitos por su complejidad?	X								
			¿Cree usted que una modificación al art. 230 del Código Procesal Penal podría llevarse a cabo con la finalidad de facilitar las investigaciones en etapa de diligencias preliminares para una adecuada y exhaustiva búsqueda de información para los ciberdelitos?	X								
			¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?	X								
		Legislaciones Internacionales	**¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?**	X								
			Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?									

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: “Guía de entrevista a profundidad para recabar opiniones acerca del levantamiento del secreto de las comunicaciones en los delitos informáticos”

OBJETIVOS:

- **Objetivo General:**
  - Proponer la incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones el cual facilitaría la investigación del Ministerio Publico
- **Objetivos específicos:**
  - Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones
  - Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones

DIRIGIDO A:

- Fiscales y Asistentes Función Fiscal de la Primera Fiscalía Provincial Penal Corporativa de Nuevo Chimbote.

……
……..

APELLIDOS Y NOMBRES DEL EVALUADOR: Alba Callacna Rafael Arturo

GRADO ACADÉMICO DEL EVALUADOR: Doctor en Educación

VALORACIÓN:

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

FIRMA DEL EVALUADOR

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN A JUICIO DE EXPERTO DE LAS VARIABLES *CIBERDELITOS* Y *LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES*.

TÍTULO: Levantamiento del secreto de las comunicaciones en los delitos informáticos.
AUTORES: Lunarejo Guevara Erick Bryan y Rodríguez Gil Karla Olinda.

VARIABLE	DIMENSIONES	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN								OBSERVACIONES Y RECOMENDACIONES
				Relación entre la variable y la dimensión		Relación entre la dimensión y el indicador		Relación entre el indicador y el ítems		Relación entre el ítems y la opción de respuesta		
				Si	No	Si	No	Si	No	Si	No	
Ciberdelitos	Criminalidad Informática	**Delitos informáticos**	**¿Qué entiende por ciberdelitos o delitos informáticos?**	X								
		Bien jurídico protegido	**¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?**	X								
		Ley N° 30096 (Ley de delitos informáticos)	**¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los ciberdelitos?**	X								

Levantamiento del secreto de las comunicaciones	**Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**	**Importancia de la medida**	**¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los ciberdelitos?**	X								
		Requisitos de la medida	**¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?**	X								
		Limitaciones de la medida	**¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?**	X								
		Modificación al art. 230 del Código Procesal Penal para las diligencias preliminares de delitos informáticos	**¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los ciberdelitos, al ser estos complejos?**	X								
			¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los ciberdelitos por su complejidad?	X								
			¿Cree usted que una modificación al art. 230 del Código Procesal Penal podría llevarse a cabo con la finalidad de facilitar las investigaciones en etapa de diligencias preliminares para una adecuada y exhaustiva búsqueda de información para los ciberdelitos?	X								
			¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?	X								
		Legislaciones Internacionales	**¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?**	X								
			Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?									

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: “Guía de entrevista a profundidad para recabar opiniones acerca del levantamiento del secreto de las comunicaciones en los delitos informáticos”

OBJETIVOS:

- **Objetivo General:**
  - Proponer la incorporación de los delitos informáticos como supuesto especial para el levantamiento del secreto de las comunicaciones el cual facilitaría la investigación del Ministerio Publico
- **Objetivos específicos:**
  - Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones
  - Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones

DIRIGIDO A:

- Fiscales y Asistentes Función Fiscal de la Primera Fiscalía Provincial Penal Corporativa de Nuevo Chimbote.

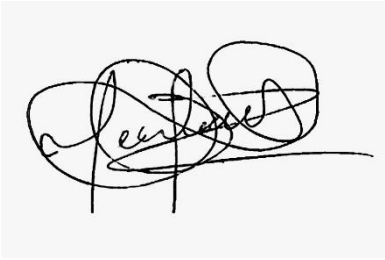
……..

APELLIDOS Y NOMBRES DEL EVALUADOR: Natividad Teatino Mendoza

GRADO ACADÉMICO DEL EVALUADOR: Maestro en Derecho

VALORACIÓN:

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo



FIRMA DEL EVALUADOR

Anexo N° 4. Cuadro de categorización de resultados

OBJETIVO	CATEGORIAS	SUBCATEGORÍAS	PREGUNTAS	ENTREVISTADO N° 1	ENTREVISTADO N° 2	ENTREVISTADO N° 3	ENTREVISTADO N° 4	ENTREVISTADO N° 5	ENTREVISTADO N° 6
Determinar que la investigación de los delitos informáticos presenta dificultades debido a la denegatoria del levantamiento del secreto de las comunicaciones	Criminalidad Informática	Delitos informáticos	¿Qué entiende por ciberdelitos o delitos informáticos?	Es la conducta activa que busca penetrar un sistema protegido por la **informática** con el fin de poder alcanzar una ventaja económica indebida. La **tutela positiva de los bienes jurídicos**, viene acompañada de una idónea legislación punitiva que, previo a regularla, la salvaguarde de conductas que tengan la idoneidad suficiente para vulnerarlas. En impacto, dialogar de tutela positiva conlleva a poder asegurar que las conductas ocurridas en el seno de la sociedad encuentren subsunción en la redacción del supuesto por cierto de la regla penal, como fiel reflejo de correspondencia entre lo legislado y el fenómeno criminológico ocurrido, que paralelamente sirve	Es una nueva forma de criminalidad en estos tiempos, son delitos complejos que se realizan a través de la internet pretendiendo dañar sistemas informáticos. Considero que no hay una efectiva tutela ya que hay ciertos delitos que suelen terminar quedando impunes debido a la carencia normativa.	Los delitos informáticos son ocupaciones ilícitas o antijurídicas que: poseen por objeto provocar perjuicios, ocasionar pérdidas o impedir la utilización de sistemas informáticos. Considero que si, puesto que se sanciona las conductas ilícitas que están afectando los sistemas y datos informáticos, cometidas por medio de la implementación de tecnologías de la información o de la comunicación.	Los delincuentes actualmente han buscado su campo de acción y es de esta forma que nacen además dichos delitos informáticos y buscan amenazar a la estabilidad informática; buscan afectar sistemas de información con una secuencia de ocupaciones ilícitas. Considero que para que se tenga una tutela positiva y adecuada de los bienes jurídicos mediante esta Ley se debe profundizar en las penas ya que si se hace un	Esos delitos en los cuales se aplican medios tecnológicos para entrar a información bancaria, de una persona natural o jurídica, así como entrar a información privada de los agentes. Considero que no, pues varios de dichos delitos no prosperan gracias a la carencia de medios jurídico y tecnológicos para averiguar. Para que este tipo de investigaciones tengan resultado,	Los delitos son acciones penadas que se realizan a través del internet, estos delitos se dan forma rápida y sistemática, dañan los ordenadores a través de medios eléctricos. Considero que si debido a que sanciona delitos informáticos que acostumbran ser de alta dificultad y que van a dañar sistemas y datos informáticos realizados por medio de las tecnologías que se fueron desarrollando y construyendo por medio del tiempo. Considero que no debido a que sus penas acostumbran ser bajas para dichos tipos de delitos que son de alta dificultad, por esto es que las penas en su
		Ley N° 30096	¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?						
			¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los delitos informáticos?						

				como garantía de una correcta acusación elemental. De forma que si lo cual se desea es hallar eficiencia, previamente que efectividad, en combatir este nuevo fenómeno, es comprobar en la idoneidad de los mecanismos o herramientas jurídicas existentes para su averiguación, y es que, con una correcta legislación procesal se puede llegar a el objetivo de la indagación y posteriormente circunstanciar debidamente una acusación, cual garantía de una adecuada pretensión punitiva estatal.			estudio de esta normatividad se podrá comprobar que, aunque hay penas para los delitos de dicha regla, estas sanciones penales tienden a ser bastante bajas por lo que no se da garantías adecuadas para las conductas que se realizan a los agraviados por estos delitos estipulados en dicha regla; solo así se contará con herramientas jurídicas efectivas para combatir estos delitos y se debe regular de manera correcta. Toda pena tiene funcionalidad preventiva, protectora y resocializadora, sin embargo, esto no implica que las penas van a ser dadas con base a esto, sino que sin embargo al expandir la pena se podrá llevar a cabo con la funcionalidad preventiva ya que las personas que deseen cometer ilícitos de delitos informáticos van	la pena debería ser mayor a los cuatros años, ya que para muchos casos necesita que se levanten las comunicaciones y puedan hallar a los responsables de los delitos, los cuales van aumentando.	medida deberían incrementarse.

							a tomar en consideración que las penas son mayores y se tiene que ir de la mano con la regla procesal.		
	Levantamiento del secreto de las comunicaciones	Importancia de la medida	¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los delitos informáticos?	Obviamente que sí, en tanto que logre obtenerse la información acerca de la identidad de los titulares de los números de abonados que, en la situación concreto, hayan predeterminado cualquier tipo de comunicación con el agraviado, y de ser la situación el flujo de denominadas y mensajes de escrito existentes, así como la localización geográfica de las celdas de comunicación A partir de donde salieron las mismas.	Si.	Definitivamente si, con ello se desencadena todo el actuar delictivo.	Sí, claro, ya que con esta figura procesal se podrá obtener información para una investigación completa, en la que se pueda constatar que realmente se ha cometido un delito a través del delito informático.	Sí, como mencioné anteriormente, desvelar las comunicaciones es un factor extremadamente importante para desentrañar la verdad y encontrar a los responsables; Sin embargo, el sistema legal actual no permite la eliminación de comunicaciones confidenciales para estos delincuentes.	Eso sí, dado que estos delitos suelen ser cometidos por telecomunicaciones y la investigación debe realizarse en la etapa preliminar del proceso para que el fiscal pueda llevar a cabo una investigación completa y justificada cuando solicite cualquier acción si la realización de una medida preventiva impide o en última instancia busca la reeducación.
		Dificultades de la medida	¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias	A partir de mi vivencia general considero que el problema no radica en los requisitos y menos los presupuestos que instituye el artículo 230° de la regla procesal penal, sino		No, pues en dicha etapa no se consigue recabar todos los elementos de convicción	Por tanto, debería crearse otro requisito como causa especial para retirar el secreto de las comunicaciones por delitos muy complejos como	No facilitan, porque existe un obstáculo que no permite el desarrollo de una buena investigación,	No, porque muchas veces durante esta etapa preliminar no es posible reunir suficientes convictos porque no se levanta la

			preliminares de los delitos informáticos?	en la técnica usada por el legislador, así como en las conductas descritas en la Ley N° 30096. 230° del CPP está en armonía con todo el sistema jurídico, puesto que el requisito de los 4 años de PPL constituye el barómetro que asegura una participación estatal en la esfera de un derecho importante. Si verificamos en este límite en nuestro sistema, como requisito anteriormente que presupuesto, lo hallaremos en diferentes estamentos, solo por nombrar uno de ellos en el artículo 57° del CP está establecido como un requisito para suspender la efectividad de una pena, que esta no supere los 4 años, y dicha es la proporción que usa nuestro sistema por la simple razón que resulta ponderable para lograr restringir derechos primordiales y más que nada asegurar la efectividad del sistema. Lo cual se debería intentar, a partir de mi criterio, es cambiar o			los delitos informáticos. Considero que además de los requisitos para facilitar una investigación completa en el proceso preliminar, se debe hacer un inciso como causa especial para los delitos informáticos por estos delitos. Es en gran medida demasiado complicado para permitir una mayor confidencialidad de las comunicaciones. estos delitos. Si bien es cierto que el secreto de las comunicaciones se aplica principalmente a la mayoría de los delitos, en el caso de los delitos tipificados en el Código No. 30096 esto tiende a convertirse en un obstáculo porque, debido a los requisitos establecidos en el procedimiento estándar, es que no se puede realizar una investigación adecuada.	uno de ellos es digno de este cargo, por ello, pida que se cumpla una solicitud de remoción de la confidencialidad de la comunicación.	confidencialidad de la comunicación.

				modular con mejor técnica narrativa los supuestos por cierto de las conductas que tienen que estar comprendidas como ciberdelitos y de esa forma los agravantes constitutivos del tipo penal en concreto, que al final van a poder ser subsumidas en las conductas cuya sanción se muestra como mayor a los 4 años de PPL; de tal forma que realmente bien va a poder configurarse en el requisito que pide el artículo.					
			¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?	No creo que se deba a que la persona correspondiente deba volver a empoderar algunas habilidades y estrategias, pero la clave del éxito radica en la inclusión original de hechos específicos, por ejemplo, si la conducta puede incluirse inicialmente en algún agravante constitutivo. factores. En ciertos tipos, es probable que sea necesario eliminar el secreto de las telecomunicaciones, pero el problema radica en la tecnología que	Definitivamente si.	Si.	Creo que sí, porque en la práctica se ha observado que muchas veces durante el proceso preliminar no se aprueba la remoción de la confidencialidad de las comunicaciones solicitadas por la Fiscalía, lo que interfiere para la continuación de	Sí, porque como repito, este delito no cumple con todos elos requisitos que establece el código para reclamar el reclamo correspondiente	Sí, debido a los requisitos de procedimiento del articulo. 230, determinó que el delito cometido era punible con más de cuatro años.

				utilizan los legisladores para establecer el tipo de supuestos fácticos (comportamiento relacionado con el delito) en cada caso.			la investigación de delitos informáticos.		
		Incorporación de un supuesto especial en la medida	¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los delitos informáticos, al ser estos complejos?	No debería existir una modificación, ni en los requisitos ni en los presupuestos, del art. 230° del CPP. La modificación debe darse en los supuestos de hechos de la norma especial que regula los ciberdelitos.	Si se hace una modificación al art. 230 CPP más que una modificación sería una incorporación en el que el levantamiento del secreto de las comunicaciones sea una herramienta contra los delitos informáticos.	Si.	Creo que se debe incorporar una razón en particular para permitir el levantamiento del secreto de las comunicaciones, ya que estos delitos son en su mayor parte delitos muy complejos y esa es la forma en que, con una combinación de causas en particular, la fiscalía podrá realizar investigaciones. y acomodar los crímenes en cuestión; También es posible que con esta modificación sea posible estudiar cada caso en particular ede una mejor manera.	Lo que debería existir es una combinación de un artículo en el que los delitos informáticos se aborden de una manera particular y una divulgación aceptable del secreto; o fallar, aumentar la pena para que coincida con los requisitos del art. 230	Creo que con la modificación del citado artículo se debe conjugar una causa específica para que se otorgue el levantamiento del secreto de las comunicaciones frente al delito informático.
			¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los delitos	Si, debido a que esto facilitaría la investigación fiscal para poder obtener un buen resultado.	Si.	Si.	Como mencione en la pregunta anterior creo que debería incluirse una causa especial para los	Sí, eso ayudará con el desarrollo de la investigación y permitirá un mejor desenlace, porque muchos de estos casos aún se encuentran en	Sí, ayuda a asegurar que en estas investigaciones se asegure la protección de un

			informáticos por su complejidad?				delitos informáticos dentro del levantamiento del secreto de las comunicaciones.	investigación preliminar porque no cuentan con las armas adecuadas para ayudar con la investigación.	derecho legal actualmente violado.
			¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?	Las ventajas al realizar la investigación de la manera más eficaz se dan frecuentemente ya que en estos tiempos actuales la tecnología va avanzando cada día más.	Se tendría una mejor regulación para que se puedan intervenir las comunicaciones en delitos de alta complejidad como lo son los delitos informáticos.	Se pueden tomar medidas más adecuadas para los delitos informáticos, que son muy complejos y han evolucionado con el tiempo.	Se podría hacer un tratamiento más adecuado a los delitos informáticos que son delitos de alta complejidad y que han ido avanzando con el paso del tiempo.	Para poder encontrar a los responsables de estos delitos, y así ayudar a reducir estos delitos, ya que actualmente están en aumento; y los perdedores son los ciudadanos.	Las ventajas serían que la fiscalía podría llevar a cabo una investigación más efectiva de estos delitos y la investigación no se vería obstaculizada; Además, se puede identificar al culpable mucho más rápido.

OBJETIVO	CATEGORIAS	SUBCATEGORÍAS	PREGUNTA	E. N° 1	E. N° 2	E. N° 3	E. N° 4	E. N° 5	E. N° 6
Analizar el ordenamiento penal extranjero sobre los delitos informáticos y el levantamiento del secreto de las comunicaciones	Legislación Internacional	Legislación Argentina	¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia; sin embargo, al margen de las legislaciones, se tiene que definir la razón para afirmar que estos delitos son complejos y sobre todo cuál es la causal que alberga dicha premisa fáctica; asimismo, refiere que se debe tomar como ejemplo la legislación española.	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia, y que se debe toma como ejemplo la legislación española.	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia, y que se debe tomar como ejemplo la legislación española.	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia, y que se debe tomar como ejemplo la legislación española.	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia, y que se debe tomar como ejemplo la legislación española.	Indica que no conoce alguna legislación extranjera que regule el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a su trascendencia, y que se debe tomar como ejemplo la legislación española.
		Legislación Venezolana							
		Legislación Colombiana							
		Legislación Chilena							
		Legislación Española	Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?						

Anexo N° 5: Cuadro de transcripción de entrevistas

PREGUNTAS	ENTREVISTADO N° 1 FISCAL ADJUNTO DE LA 1°FPPCNCH	ENTREVISTADO N° 2 FISCAL ADJUNTO DE LA 1°FPPCNCH	ENTREVISTADO N° 3 FISCAL ADJUNTO DE LA 1°FPPCNCH"	ENTREVISTADO N° 4 "FISCAL PROVINCIAL DE LA 1°FPPCNCH"
¿Qué entiende por ciberdelitos o delitos informáticos?	Es todo comportamiento activo que busca introducirse en un sistema protegido por la informática con la finalidad de poder obtener una ventaja económica indebida, tanto para sí como para un tercero, para los cual se vale del empleo de sistemas y/o programas informáticos especializados, así como el ardid, el engaño, o el abuso de la confianza del titular del bien con contenido patrimonial.	Se entiende a todo comportamiento que busca desapoderar económicamente al titular de un bien con contenido patrimonial, cuya guarda se encuentra protegida por algún mecanismo de la informática en general, utilizando para ello algún sistema informático especializad.	Los delitos informáticos son actividades ilícitas o antijurídicas que: tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos	Son conductas ilícitas o ilegales realizado por personas dentro de un espacio digital a través de redes informáticas o mediante dispositivos en red, se va a considerar así que es una acción antijurídica con el uso de la Internet, con el uso de las nuevas tecnologías. Los delincuentes en la actualidad han buscado su campo de acción y es así que nacen también estos delitos informáticos y buscan amenazar a la seguridad informática; buscan dañar sistemas de información con una serie de actividades ilícitas.
¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?	La tutela efectiva de los bienes jurídicos, viene acompañada de una adecuada legislación punitiva que, antes de regularla, la proteja de conductas que tengan la idoneidad suficiente para vulnerarlas**.** En efecto, hablar de tutela efectiva conlleva a poder garantizar que las conductas ocurridas en el seno de la sociedad encuentren subsunción en la redacción del supuesto de hecho de la norma penal, como fiel reflejo de correspondencia entre lo legislado y el fenómeno criminológico ocurrido, que a su vez sirve como garantía de una adecuada imputación necesaria. Pero la efectividad de su tutela, pasa además por contar con las herramientas jurídicas que permitan, en aras de esclarecer los hechos, investigar debidamente lo ocurrido, y de ser el caso combatir este flagelo siempre desde una perspectiva de prevención especial positiva; para lo cual debe contarse con un marco que regule de manera adecuada, per se, el procedimiento de investigación propiamente dicho, puesto que la	Considero que no, pero dicha tutela podría mejorar al realizarse una adecuada investigación, si bien es cierto se sancionan conductas que han ido surgiendo con el pasar de los años pues también es cierto que para frenar estas conductas debía existir una adecuada norma procesal.	Considero que no, a pesar de que se sanciona las conductas ilícitas que afectan los sistemas y datos informáticos, cometidas mediante la utilización de tecnologías de la información o de la comunicación.	Considero que para que se tenga una tutela efectiva y adecuada de los bienes jurídicos mediante esta Ley se debe profundizar en las penas ya que si se hace un estudio de esta normatividad se podrá verificar que, aunque hay penas para los delitos de dicha norma, estas sanciones penales tienden a ser muy bajas por lo que no se brinda garantías adecuadas para las conductas que se realizan a los agraviados por estos delitos estipulados en dicha norma; solo así se contará con herramientas jurídicas efectivas para combatir estos delitos y se debe regular de manera adecuada.

	norma sustantiva encuentra funcionalidad con la norma procesal. Campo en el cual se requiere algunos ajustes para satisfacer la garantía de efectividad en la tutela de estos bienes jurídicos.			
¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los delitos informáticos?	Hablar de la sanción penal es referirnos al extremo final de todo un procedimiento pretensivo por parte del Estado, es decir, cuando el funcionario autorizado para ello (fiscal penal), una vez presentada tu teoría imputativa (pretensión punitiva estatal), y sometida a las garantías del contradictorio, publicidad, oralidad e inmediación, ha sido aceptada (sanción penal) y por tanto declarada judicialmente la culpabilidad de un ciudadano por un hecho concreto. En ese mismo sentido, las penas como tal, cuya función es preventiva, protectora y resocializadora, no están en relación directa con una política –al menos adecuada- de combatir las conductas reguladas como punibles. Pues la sanción penal no debe ser entendida como una retribución por el hecho cometido, sino debe ser entendida desde su enfoque de prevención especial positiva. De manera que si lo que se quiere es encontrar eficiencia, antes que efectividad, en combatir este nuevo fenómeno, es verificar en la idoneidad de los mecanismos o herramientas jurídicas existentes para su investigación, y es que, con una adecuada legislación procesal se puede llegar a la finalidad de la investigación y seguidamente circunstanciar debidamente una imputación, cual garantía de una correcta pretensión punitiva estatal (acusación fiscal).	Considero que, si pero que podría mejorar esta tutela efectiva de derechos, si bien es cierto se sancionan conductas que han ido surgiendo con el pasar de los años pues también es cierto que para frenar estas conductas deberían incrementarse las penas. Considero que no, deberían incrementarse en la medida y teniendo en cuenta que para la realización de estas conductas ilícitas se debe tener conocimientos especializados, es así que toda aquella persona que cometa un acto de estos es porque lo realiza sabiendo que cometerá un gran perjuicio ya que son delitos complejos.	Considero que no, son muy benéficas y no están acorde con el daño producido a la víctima.	Creo que las penas que se encuentran deberían reformarse, pero no se debe olvidar que la pena es de ultima ratio para privar la libertad de una persona, por ende, aun cuando se modifique las penas de dicha Ley el fiscal a cargo de la investigación tiene que hacer un estudio a profundidad de cada caso en concreto para que el juez pueda declarar la culpabilidad. Toda pena tiene función preventiva, protectora y resocializadora, pero esto no significa que las penas van a ser dadas en base a esto, sino que por el contrario al ampliar la pena se podrá cumplir con la función preventiva ya que las personas que deseen cometer ilícitos de delitos informáticos tendrán en cuenta que las penas son mayores y se tiene que ir de la mano con la norma procesal.
¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los delitos informáticos?	Desde luego que sí, en tanto que pueda obtenerse la información sobre la identidad de los titulares de los números de abonados que, en el caso concreto, hayan establecido algún tipo de comunicación con el agraviado, y de ser el caso el flujo de llamadas y mensajes de texto existentes, así como la ubicación geográfica de las celdas de comunicación desde donde salieron las mismas. De esta forma, podrá cruzarse la información para verificar, de ser el caso, la participación de los	Definitivamente si, es de vital importancia para poder hallar elementos suficientes para una investigación preparatoria	Definitivamente si, con ello se desencadena todo el actuar delictivo.	Claro que sí, ya que con esta figura procesal se va a poder obtener información para una adecuada investigación, se va a poder verificar que efectivamente a través de delitos informáticos se ha cometido ilícitos penales.

	titulares de estos abonados en el caso concreto, así como la participación de alguna otra persona, toda vez que pueda darse que el titular de la línea telefónica desconoce por completo la actividad criminal realizada desde una línea telefónica registrada a su nombre.			
¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?	Desde mi experiencia general considero que el problema no radica en los requisitos y menos los presupuestos que establece el artículo 230° de la norma procesal penal, sino en la técnica utilizada por el legislador, así como en las conductas descritas en la Ley N° 30096. Esto es, los requisitos del art. 230° del CPP se encuentra en armonía con todo el sistema jurídico, pues el requisito de los 4 años de PPL constituye el barómetro que garantiza una intervención estatal en la esfera de un derecho fundamental. Si verificamos en este límite en nuestro sistema, como requisito antes que presupuesto, lo hallaremos en diferentes estamentos, solo por mencionar uno de ellos en el artículo 57° del CP se establece como un requisito para suspender la efectividad de una pena, que esta no supere los 4 años, y esa es la proporción que utiliza nuestro sistema por la sencilla razón que resulta ponderable para poder restringir derechos fundamentales y sobre todo garantizar la efectividad del sistema. Y además porque una adecuada investigación no está solo en función de un acto único como lo puede ser un levantamiento del secreto a las telecomunicaciones, sino por todo el conjunto de actos de investigación recopilados en la carpeta fiscal. Lo que se debe procurar, desde mi punto de vista, es modificar o modular con mejor técnica narrativa los supuestos de hecho de las conductas que deben estar comprendidas como ciberdelitos y en ese sentido los agravantes constitutivos del tipo penal en específico, que finalmente podrán ser subsumidas en las conductas cuya sanción se presenta como superior a los 4 años de PPL; de tal manera que muy bien podrá configurarse en el	Considera que no, debido a que durante esta etapa no se puede obtener suficientes elementos de convicción.	No, pues en dicha etapa no se consigue recabar todos los elementos de convicción.	Considero que más allá que los requisitos faciliten una adecuada investigación en las diligencias preliminares se tiene que hacer un inciso como causa especial para los delitos informáticos ya que estos delitos en su mayoría son de alta complejidad de manera que se necesita que el levantamiento del secreto de las comunicaciones se permita para estos hechos delictivos. Si bien es cierto el levantamiento del secreto de las comunicaciones en su mayoría concuerda para la mayoría de delitos, en el caso de los delitos de la ley N° 30096 tiende a ser un impedimento ya que por los requisitos establecidos en la norma procesal es que no se puede hacer una investigación idónea. Por ende, se debe crear como causa especial un requisito más al levantamiento del secreto de las comunicaciones para los delitos de alta complejidad como son los delitos informáticos.

	requisito que exige el art. 230° de la norma procesal.			
¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?	Considero que no, dado que existen técnicas y estrategias que deben sr repotenciadas por quien corresponde, pero la clave del éxito está en la subsunción primigenia que se pueda realizar del hecho concreto, por ejemplo, si la conducta primigeniamente puede ser subsumida en algún agravante constitutivo del tipo específico, muy bien podría requerirse el levantamiento del secreto a las telecomunicaciones, empero, la problemática radica en la técnica utilizada por el legislador para establecer los supuestos de hecho (conductas con relevancia penal) en cada uno de los tipos.	Si.	Si	Considero que si ya que en la práctica se ve que muchas veces en las diligencias preliminares no se otorga el levantamiento del secreto de las comunicaciones solicitado por el fiscal haciendo que esto resulte un impedimento para la continuación con la investigación de los delitos informáticos.
¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los delitos informáticos, al ser estos complejos?	Afirmar ello implicaría dar por sentado que todo ciberdelito es, per se, complejo. La complejidad de la investigación y procesamiento de un hecho punible, no pasa por su naturaleza jurídica ni muchos menos por su configuración narrativa, sino por los alcances de sus efectos en el caso concreto, pero atendiendo a las particulares circunstancias o presupuestos habilitantes previstos en la norma procesal para su configuración. Y atendiendo a la interrogante, considero que no debería existir una modificación, ni en los requisitos ni en los presupuestos, del art. 230° del CPP. La modificación debe darse en los supuestos de hechos de la norma especial que regula los ciberdelitos.	Si.	Si	Considero que debería incorporarse una causa especial para otorgar el levantamiento del secreto de las comunicaciones por ser estos delitos en su mayoría, delitos de alta complejidad y es así que con la incorporación de esta causa especial hará que el Ministerio Público pueda realizar una investigación adecuada e idónea para los delitos en mención; se tiene además que con esta modificación se va a poder estudiar de mejor manera cada caso en concreto.
¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los delitos informáticos por su complejidad?	Considera que si, debido a que esto facilitaría la investigación fiscal para poder obtener un buen resultado.	Definitivamente si ya que son delitos complejos que ameritan lo más factible para su investigación.	Si	Como mencione en la pregunta anterior creo que debería incluirse una causa especial para los delitos informáticos dentro del levantamiento del secreto de las comunicaciones.
¿Cuáles serían las ventajas en la investigación al realizarse una	Las ventajas serían que podría investigarse de una manera más eficaz los delitos informáticos, que en la actualidad son muy frecuentes en estos tiempos donde la tecnología ha avanzado.	Se podría dar trámite más rápido en este tipo de delitos, de forma que el representante del	Considero que habría más eficacia al momento de tratar contra los delitos	Se podría hacer un tratamiento más adecuado a los delitos informáticos que son delitos de alta complejidad y que han ido avanzando con el paso del tiempo.

modificación al art. 230 del CPP?		Ministerio Pública podrá recabar mucha más información que será usada en juicio.	informáticos.	
¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?	No, sin embargo Al margen de las legislaciones, tendría que definirse antes que nada cuál es la razón para afirmar que estos delitos son complejos y sobre todo cuál es la causal que alberga dicha premisa fáctica (complejidad legal	No.	No.	No.
Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?	Si	Si	Si	Si

PREGUNTAS	ENTREVISTADO N° 1 “ASISTENTE FUNCION FISCAL DE LA 1°FPPCNCH”	ENTREVISTADO N° 1 “ASISTENTE FUNCION FISCAL DE LA 1°FPPCNCH”
¿Qué entiende por ciberdelitos o delitos informáticos?	Aquellos delitos en los que se utilizan medios tecnológicos para acceder a información bancaria, de una persona natural o jurídica, así como acceder a información privada de los agentes.	Los delitos informáticos son aquellas acciones antijurídicas que se van a realizar a través del internet, usualmente estos delitos se realizan de forma sistemática y rápida; tienden a la destrucción o daño de ordenadores valiéndose de medios electrónicos disponibles.
¿Considera que en la Ley N° 30096 existe una tutela efectiva de los bienes jurídicos vulnerados por las modalidades de comisión de estos ilícitos?	Considero que no, puesto que muchos de estos delitos no prosperan debido a la falta de medios jurídico y tecnológicos para investigar	Considero que si ya que sanciona delitos informáticos que suelen ser de alta complejidad y que van a afectar sistemas y datos informáticos cometidos mediante las tecnologías que se han ido desarrollando y creando a través del tiempo
¿Usted cree que las penas estipuladas en la Ley N° 30096 son adecuadas para sancionar la comisión de los delitos informáticos?	Pienso que para que estas investigaciones tengan resultado la pena debería ser superior a los cuatro años, debido a que muchos necesitan que se realicen el levantamiento de las comunicaciones, toda vez que ese sería un elemento fundamental que ayude a encontrar a los responsables de estos delitos, que hoy en día van en aumento.	Considero que no ya que sus penas suelen ser bajas para estos tipos de delitos que son de alta complejidad, por ello es que las penas en su medida deberían incrementarse.
¿Considera usted que el levantamiento del secreto de las comunicaciones es de vital importancia para la investigación de los delitos informáticos?	Sí, como lo mencioné líneas arriba, el levantamiento del secreto de las comunicaciones es un elemento de vital importancia para esclarecer los hechos y encontrar a los responsables; sin embargo el actual ordenamiento jurídico no permite que en esos delitos se realice el levantamiento del secreto de las comunicaciones	Claro que si ya que estos delitos suelen hacerse a través de las telecomunicaciones y se debe hacer el levantamiento en la etapa de diligencias preliminares para que el fiscal pueda hacer una investigación adecuada y pueda fundamentar al momento de solicitar alguna medida sea medida de prisión preventiva o solicitar en definitiva la pena privativa de la libertad.

¿Considera usted que los requisitos estipulados en el artículo 230 del C.P.P. facilitan una adecuada investigación en la etapa de diligencias preliminares de los delitos informáticos?	No facilitan, pues existen trabas que no permiten el desarrollo de una buena investigación, una de ellas la pena que tiene este delito, ya que por ese motivo no se cumple el requisito para solicitar el levantamiento del secreto de las comunicaciones	No, pues muchas veces en esta etapa preliminar no se logra recabar suficientes elementos de convicción debido a que no se da el levantamiento del secreto de las comunicaciones.
¿Considera usted que la investigación preliminar en los delitos informáticos se ve limitada por los requisitos que contiene el artículo 230 del C.P.P. que regula el levantamiento del secreto de las comunicaciones?	Sí, debido a que como repito, este delito no cumple con todos los requisitos que establece el código para solicitar el requerimiento respectivo.	Si, debido a los requisitos procesal del art. 230, establecen que el delito cometido tenga una pena mayor de cuatro años.
¿Considera usted que debe existir una modificación al artículo 230 del Código Procesal Penal, para que facilite el otorgamiento del levantamiento del secreto de las comunicaciones para los delitos informáticos, al ser estos complejos?	Lo que debería existir es la incorporación de un artículo en el que los delitos informáticos sean tratados de manera especial, y se pueda otorgar el levantamiento del secreto de las comunicaciones; o caso contrario el incremento de la pena para que se cumpla con los requisitos del art. 230	Considero que una modificación a dicho artículo, se debe incorporar una causa especial para que se otorgue el levantamiento del secreto de las comunicaciones ante los delitos informáticos.
¿Considera usted que debe incluirse en el artículo 230 del C.P.P. el levantamiento del secreto de las comunicaciones en los delitos informáticos por su complejidad?	Sí, esto ayudaría en el desarrollo de la investigación y sí lograr un mejor resultado, debido a que muchos de estos casos quedan en investigación preliminar por no tener las armas jurídicas que ayuden a la investigación	Sí, ayudaría a que en estas investigaciones se logre la tutela del bien jurídico que se ve vulnerada actualmente
¿Cuáles serían las ventajas en la investigación al realizarse una modificación al art. 230 del CPP?	Poder encontrar a los responsables de estos delitos, y así ayudar a que estos delitos disminuyan, ya que en la actualidad van en aumento; y los perjudicados somos los ciudadanos	Las ventajas serían que podría darse una investigación más efectiva por parte del Ministerio Público a estos delitos y no se entorpecerían las investigaciones; además que se podría identificar de forma muchas más rápida a los autores de los delitos.
¿Conoce usted legislación en las cuales se permitido el acceso al secreto de las comunicaciones en los delitos informáticos por su complejidad?	No.	No.

Según el artículo 588 ter-a de la Ley de Enjuiciamiento Criminal – España, señala que se podrá concebir la autorización del levantamiento del secreto de las comunicaciones cuando se trate de un delito informático, estableciendo esto como un presupuesto, ¿Considera usted que esta legislación garantiza una adecuada investigación de los delitos informáticos?	Si	Si

Anexo N° 06

Proyecto de ley

Presentación:

Los estudiantes de la Escuela Profesional de Derecho, de la Universidad César Vallejo – Filial Chimbote; Erick Bryan Lunarejo Guevara y Karla Olinda Rodriguez Gil, proponen lo siguiente:

"PROYECTO DE LEY QUE INCORPORA LOS DELITOS INFORMATICOS COMO SUPUESTO ESPECIAL EN EL LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES Y MODIFICA EL NUMERAL 1 DEL ARTÍCULO 230 DEL CÓDIGO PROCESAL PENAL PERUANO"

FÓRMULA LEGAL:

El Congreso de la República

Ha dado la siguiente ley:

LEY QUE INCORPORA LOS DELITOS INFORMATICOS COMO SUPUESTO ESPECIAL EN EL LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES Y MODIFICA EL NUMERAL 1 DEL ARTÍCULO 230 DEL CÓDIGO PROCESAL PENAL PERUANO

Artículo 1°. Modificación del numeral 1 artículo 230 del Código Procesal Penal Peruano.

Modifíquese el numeral 1 del artículo 230 del Código Procesal Penal, en los siguientes términos:

1. El Fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, **o cuando se trate de delitos informáticos,** podrá solicitar al Juez

de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4) del artículo 226.

2. La orden judicial puede dirigirse contra el investigado o contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación.

3. El requerimiento del Fiscal y, en su caso, la resolución judicial que la autorice, deberá indicar el nombre y dirección del afectado por la medida si se conociera, así como, de ser posible, la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar. También indicará la forma de la interceptación, su alcance y su duración, al igual que la dependencia policial o Fiscalía que se encargará de la diligencia de intervención y grabación o registro.

El Juez comunicará al Fiscal que solicitó la medida el mandato judicial de levantamiento del secreto de las comunicaciones. La comunicación a los concesionarios de servicios públicos de telecomunicaciones, a efectos de cautelar la reserva del caso, será mediante oficio y en dicho documento se transcribirá la parte concerniente

4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.

5. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.

6. La interceptación no puede durar más de sesenta días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal y decisión motivada del Juez de la Investigación Preparatoria.

EXPOSICIÓN DE MOTIVOS:

Conforme el artículo dos de la Constitución Política del Perú establece que “Toda persona tiene derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados”, generando una protección para la intimidad de las comunicaciones de cualquier sujeto de derecho; sin embargo, en la citada norma precisa que “las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley”, lo que muestra que en casos especiales se podrá limitar este derecho solamente cuando el Juez asi lo disponga con argumentos debidamente motivados.

En el mismo orden tenemos lo descrito en el artículo 230 del Código Procesal Penal, en el cual describen que se puede interrumpir el derecho al secreto y la inviolabilidad de las comunicaciones solo cuando fuese necesario para continuar con la investigación de un hecho delictivo, teniendo, así como objetivo que es el obtener la verdad, obtener pruebas por parte del Ministerio Público para poder continuar con la investigación y persecución; sin embargo dicha prerrogativa establece determinados presupuestos para poder solicitar dicha autorización.

Ahora, según el Boletín Estadístico (2019) emitió un informe estadístico donde se observa que de marzo de 2018 a marzo del 2019 han existido un total de 1536 casos registrados en fiscalías provinciales penales y mixtas, de marzo de 2017 a marzo del 2018 existieron 769 delitos informáticos, por lo que tenemos que hubo un incremento de 767 casos más entre 2018 a 2019; por otro lado, según el informe de análisis N° 04 realizado por la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público (2021), se tiene que la DIVINDAT desde el 2013 hasta el 2020, ha recibido 12169 denuncias vinculadas a los delitos informáticos, teniendo su mayor incidencia en el año 2020, producto de la pandemia Covid-19. Mientras que, el Ministerio Publico es quien tiene un mayor índice de denuncias siendo estas 21687, que comprenden desde el año 2013 hasta el 2020, teniendo mayor incidencia de denuncias en la provincia de Lima Metropolitana con un total de 10 340, información que fue registrada en el SGF y SIATF. Esto evidencia, que en los últimos años se ha venido teniendo un incremento en la criminalidad entorno a la comisión de delitos informáticos, debido al constante avance de las TIC,

poniendo en mayor peligro a la sociedad peruana al desconocer estas nuevas formas delictivas, y su escaso conocimiento sobre la seguridad informática, encontrándose cada vez más expuestas a estas, debido a la digitalización de la información y la facilidad de poder acceder a estas mediante las tecnologías.

Por otra parte, tenemos que existen hasta la fecha 12608 denuncias archivadas, 8842 en proceso de investigación y juzgamiento, 125 con sobreseimiento, 108 con sentencias y 4 con terminación anticipad, comprendiendo estas estadísticas desde el 2013 hasta el 2020 (OFAEC, 2021, p. 26); estas estadísticas evidencian que no existe una adecuada tutela efectiva de los bienes jurídicos establecidos en la Ley N° 30096, demostrado mediante el alto porcentaje de denuncias que han sido archivadas.

Asimismo, se tiene que la OFAEC (2021), obtuvo de las entrevistas a los fiscales con mayor incidencia de delitos informáticos, a fin de determinar cuáles son las principales dificultes de investigación y enjuiciamiento, es así que señalan que uno de las principales dificultades en la investigación, es debido a que los jueces niegan el Levantamiento del secreto de las Comunicaciones, debido a que los delitos informáticos no cumplen con los presupuestos materiales del artículo 230 del C.P.P.; asimismo, precisaron que los principales motivos de archivamiento o sobreseimiento es debido a que no se logra identificar al autor de los hechos, falta de capacitación, investigación deficiente, desconocimiento de la obtención y tratamiento de la prueba digital, falta de capacitación a fiscales y personal policial, y la falta de información.

Por lo tanto, ante esta situación existe la necesidad de investigar y dar una solución a la limitación en la investigación de los delitos informáticos, con el objetivo de que se autorice el levantamiento del secreto de las comunicaciones para la adecuada investigación de los delitos informáticos.

En ese sentido, precisamos que, conforme a las disposiciones establecidas sobre el LSC, se establece que para los delitos informáticos será una medida ineficaz por los presupuestos de sus requisitos establecidos en la norma procesal.

Entonces, si se pretende luchar contra los delitos informáticos que son una nueva forma de criminalidad y que además son delitos de alta complejidad ya que se necesita una preparación o estudios para cometer estos ilícitos, entonces se debe

tomar medidas que sean más efectivas para la lucha con ellos, por ende es que resulta un impedimento el que no se pueda levantar el secreto de las comunicaciones ya que en su mayoría las penas dadas para los delitos informáticos son penas menos de 4 años haciendo que no se puedan dar el LSC y la investigación no prospere.

Ahora bien, luego de exponer los primeros puntos, corresponde detallar que nuestro ordenamiento jurídico ha reconocido medidas limitativas de derechos, pero estas solo se podrán solicitar en casos especiales y cumpliendo los presupuestos de la norma, pero dichos presupuestos no se acoplan a todos los delitos.

Entonces, si en Perú se encuentra regulado los delitos informáticos como delitos complejos que tienen una Ley Especial la Ley N° 30096 y el Levantamiento se encuentra en el art. 230 de CPP, como una medida que se podrá utilizar para obtener información relevante para una investigación, ¿por qué no utilizar el levamiento como método de investigación de este tipo de ilícitos, debido a que son complejos? ¿acaso no debe buscarse la tutela efectiva de los bienes jurídicos protegidos en la mencionada ley?, si notamos que ello no afectará a nadie, sino más bien será un beneficio para la investigación y persecución de estos delitos.

Además, en la legislación extranjera ya ha aceptado el levantamiento del secreto de las comunicaciones en los delitos informáticos debido a la trascendencia y complejidad de estos delitos, adaptando sus normas procesales a los avances de la tecnología, para facilitar la investigación y persecución de los delitos informáticos, considerando los criterios antes referidos, más bien, corresponde considerar lo referido por ellos, es así que:

> España: Regula a el Levantamiento del Secreto de las Comunicaciones de los delitos informáticos, en la Ley de Enjuiciamiento Criminal, la misma que fue incorporada mediante la Ley Organica N° 13/2015, refiriendo que:
>
> > “Artículo 588 ter a. Presupuestos.
> >
> > La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o **delitos cometidos a través de instrumentos informáticos o de cualquier**

<u>otra tecnología de la información o la comunicación o servicio de comunicación</u>."

De ello, precisaremos que, la norma permite el levantamiento del secreto de las comunicaciones en caso de delitos informáticos, debido a que estos son delitos de alta transcendencia y complejidad como antes hemos referido, es por eso que el legislador español se vio en la necesidad de adaptar sus normas existentes al constante avance de las tecnologías, con la finalidad de poder afrontar la criminalidad, justificando que no importa la naturaleza grave del delito, si no la gravedad del hecho y lo reprochable que es para la sociedad. Uno de los fundamentos a considerar por los legisladores de esta época es la cantidad de casos archivados debido a que no existe una adecuada investigación de estas nuevas modalidades, siendo estas una gran dificultad, además porque el legislador debe adoptar normas que permitan la investigación y persecución de estos ilícitos, y no solamente regular las modalidades y dejar a la deriva los métodos de investigación que se podrán utilizar en estos casos. La idea de esta norma es generar una respuesta a las dificultades existentes en la investigación de este tipo penal, generando un sistema procesal más adecuado que garantice una tutela efectiva de los bienes jurídicos protegidos en la Ley N° 30096.

EFECTO DE LA NORMA:

Con la presentación de la modificatoria se agrega un supuesto más como causa especial para la figura jurídica del levantamiento del secreto de las comunicaciones ante los delitos informáticos.

Se adiciona también, que el presente proyecto no tiene algún efecto contrario con lo que menciona la Constitución, más bien cumple con la exigencia referida por ella, tampoco afecta alguna otra norma como tratado, sino esta se vincula con la necesidad de tener una lucha idónea contra los delitos informáticos y que el representante del Ministerio Público por falta de información o evidencias permita que la investigación se archive en etapa de diligencias preliminares.

ANÁLISIS COSTO BENEFICIO:

El proyecto referido tiene como beneficiarios a los representantes del Ministerio Público (fiscales) de nuestro país y de forma indirecta a las personas afectadas por cualquier tipo de delito informático que se les haya cometido, lo cual resumiremos de la siguiente manera:

ACTORES	COSTO	BENEFICIO
ESTADO	Ninguno	Garantiza una tutela efectiva de los bienes jurídicos protegidos en la Ley N° 30096
POBLACIÓN	Ninguno	Sus denuncias sobre delitos informáticos no quedaran archivadas debido a la falta de elementos de convicción e identificación del autor del hecho.
MINISTERIO PÚBLICO	Ninguno	Facilitará la investigación realizada en los delitos informáticos, pudiendo recabar elementos de convicción de permitan identificar al autor de los hechos. Podrán garantizar la efectividad del proceso penal, logrando la tutela efectiva de los bienes jurídicos.