UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FACULTAD DE DERECHO

# El TRATAMIENTO DE LOS BIENES JURÍDICOS COLECTIVOS EN LOS DELITOS INFORMÁTICOS


Tesis presentada por:
Ccasa Zavala, Veronica
Coila Mamani, Rosmery


Para optar el Título Profesional de:
Abogadas


Asesor:
Mag. Teran Dianderas, Helder Uriel.


Arequipa – Perú

2021

*¨Creo que los virus informáticos deberían contar como vida. Creo que dice bastante sobre nosotros el hecho de que la única forma de vida que hemos logrado crear sea puramente destructiva. Hemos creado vida basada en nuestra imagen. ¨*

**Stephen Hawking**

## DEDICATORIA

A Dios, mis padres Juan y Alejandrina, mis amigas lady´s y socias en Punto Legal, en especial a toda mi familia Ccasa Zavala, porque ellos son mi fuente de inspiración, mis ganas de salir adelante y porque con ellos aprendí que no sirve de nada ser profesional sino estas dispuesto a compartir tus conocimientos con aquellos olvidados por el sistema.

**Verónica**

Principalmente a Dios. A mis padres, Isaac y Silvia por darme la vida, su amor y apoyo incondicional, porque son mi principal motor para alcanzar mis objetivos. Todo esto es por y para ustedes, con amor.

**Rosmery**

A los caídos en la contención del poder punitivo, en especial a todas aquellas personas inocentes, que han sido privadas de su libertad injustamente y olvidadas por el verdadero fin del derecho penal.

## AGRADECIMIENTO

Nuestra inmensa gratitud a nuestra querida Universidad Nacional de San Agustín por albergarnos por seis años en sus aulas y enseñarnos la misión de un verdadero profesional agustino.

A nuestro asesor, Uriel Terán Dianderas por su disposición, apoyo y voluntad que tuvo desde el primer momento en acompañarnos a lo largo de este recorrido desconocido, frustrante pero gratificante tarea.

A nuestros amigos por motivarnos a cumplir nuestra meta, en especial a Ignacio, quien con su sabiduría y enseñanza hizo más llevadero este camino.

A nuestros profesores por brindarnos sus conocimientos a lo largo de nuestra carrera universitaria.

## RESUMEN

En esta era digital nuestras identidades virtuales son elementos esenciales de la vida cotidiana, utilizamos sistemas informáticos para adquirir bienes y servicios, celebramos contratos, expresamos nuestras opiniones, revisamos nuestras finanzas, etc. En este contexto los delitos informáticos se están constituyendo rápidamente en los delitos que más rápidamente afectan los bienes jurídicos de las personas y empresas; aunque en un inicio los delitos informáticos tutelaban principalmente bienes jurídicos patrimoniales, el rango de alcance del derecho penal informático se ha extendido a conductas en los sistemas informáticos que no solo afectan el patrimonio de las personas y/o empresas, sino también, comprende bienes jurídicos penalmente protegidos como la integridad de las personas, de los datos, la fe pública, la seguridad y otros de similar relevancia. Los delitos informáticos son ataques a la información de las personas, las empresas o los gobiernos, es decir al conjunto de atributos informativos que definen a las personas e instituciones en Internet.

Los regímenes legales están desarrollando diversas estrategias destinadas a reducir el riesgo que representan los delitos informáticos, y la legislación es una parte indispensable de su estrategia. Sin embargo, nuestra investigación ha identificado la eficacia limitada de las legislaciones y las políticas penales cuando aborda la protección de bienes jurídicos colectivos en los delitos informáticos, este trabajo busca aportar al debate sobre la naturaleza de los bienes jurídicos protegidos en los delitos informáticos, especialmente cuando se trata de delimitar un bien jurídico colectivo propiamente informático denominado funcionalidad informática o seguridad informática.



***Palabras clave***: Delito, Delitos Informáticos, bien Jurídico, bienes jurídicos colectivos, bienes jurídicos informáticos, funcionalidad informática.

## ABSTRACT

In this digital age our virtual identities are essential elements of everyday life, we use computer systems to acquire goods and services, we enter into contracts, we express our opinions, we review our finances, etc. In this context, cybercrime is rapidly becoming the crimes that most rapidly affect the legal assets of individuals and companies; although in the beginning computer crimes mainly protected patrimonial legal assets, the range of scope of computer criminal law has been extended to behaviors in computer systems that not only affect the assets of individuals and / or companies, but also includes criminally protected legal assets such as the integrity of people, data, public faith, security and others of similar relevance. Computer crimes are attacks on the information of people, companies or governments, that is, the set of informative attributes that define people and institutions on the Internet.

Legal regimes are developing various strategies aimed at reducing the risk posed by cybercrime, and legislation is an indispensable part of their strategy. However, our research has identified the limited effectiveness of criminal laws and policies when it addresses the protection of collective legal assets in computer crimes, this work seeks to contribute to the debate on the nature of legal assets protected in computer crimes, especially when it comes to delimiting a collective legal good properly computer called computer functionality or computer security.



***Key words:*** Crime, Computer Crimes, Legal Good, Collective Legal Assets, Computer Legal Assets, Computer Functionality.

# ÍNDICE

# CAPÍTULO I

# PLANTEAMIENTO DEL PROBLEMA

## 1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Los delitos informáticos son una forma de delito que aprovecha las fallas en sistemas de información complejos e infraestructuras de información. La rápida expansión del comercio electrónico y la dependencia generalizada de los servicios en línea para las transacciones financieras y las interacciones sociales han creado oportunidades sin precedentes para muchos tipos de actividades delictivas. Los delitos informáticos se están convirtiendo rápidamente en uno de los delitos más lesivos del mundo. Disuadir la actividad delictiva en la era digital requiere sistemas más seguros, educación de los usuarios, nueva legislación y nuevos métodos de aplicación de acuerdos internacionales que aborden la naturaleza compleja del delito informático.

Es necesario entender que hay muchas personas involucradas en cada delito informático. Este nuevo fenómeno implica un entorno colaborativo que incluye desarrolladores de malware, comerciantes que intercambian datos robados de víctimas, técnicos que construyen y mantienen infraestructuras de servidores y bases de datos, etc. Ahora bien, para enfrentar la ciberdelincuencia, las autoridades han hecho esfuerzos intensivos en seguridad y políticas criminales con el objetivo de proteger las tecnologías digitales de las que cada vez más personas dependen. Por esta razón, es importante abrir espacios de reflexión en la doctrina penal sobre la naturaleza compleja de los delitos informáticos.

La promulgación de la Ley N° 30096, Ley de Delitos Informáticos y modificatorias; ha significado un avance legislativo en el marco de la adecuación de nuestra legislación al convenio de Budapest. Sin embargo cuando se trata de delitos informáticos, los operadores jurídicos han encontrado dificultades tanto en la adecuada tipificación como en la persecución de dichos delitos, ya sea por la poca información y el poco desarrollo en la normativa nacional o por las dificultades que representa la investigación de estos delitos. En ese sentido es necesario contar con un criterio de uniformidad respecto al bien jurídico protegido, es decir, indicar si este delito es de

naturaleza pluriofensivo que afecta bienes no solo individuales sino que también bienes jurídicos colectivos de gran importancia social.

En cuanto al bien jurídico, se entiende que se protege en general la información, pero está es considerada de diferentes formas, ya sea como un valor económico, como un valor intrínseco a la persona, por su tráfico jurídico y finalmente por la naturaleza de los sistemas que la procesan o automatizan; en otras palabras, además de proteger los bienes jurídicos tradicionales afectados como son: el patrimonio, la identidad o la indemnidad sexual; se protegen bienes jurídicos de naturaleza colectiva como la fe pública, la salud pública, la seguridad vial, la seguridad del sistema financiero o la administración pública. Por esta razón compartimos la opinión de diversos autores que afirman que se trata de un delito pluriofensivo, pues afecta varios bienes jurídicos protegidos y que también afecta un bien jurídico que podría conceptualizarse como informático.

El presente trabajo se ocupará de definir el bien jurídico de los delitos informáticos en sentido estricto (en adelante, delitos informáticos), El estudio considerará, principalmente, los tres ejes sobre los que (con más o menos matices) se estructuran los delitos informáticos: aquellas conductas que implican destrucción o inutilización de datos o programas de sistemas informáticos, que suelen ligarse con el sabotaje informático; las que suponen acceso u obtención indebidos de datos o programas de sistemas informáticos, que suelen vincularse con el espionaje informático; y las que implican alteración o manipulación de datos o programas de sistemas informáticos, que suelen ligarse con el fraude informático. Entre las aproximaciones doctrinales al bien jurídico de los delitos informáticos es posible distinguir dos teorías, estrechamente vinculadas con la forma que adopta (o debería adoptar) la tipificación de dichos delitos. Por una parte, está la tesis que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales; por otra parte están las que consideran a los delitos informáticos solamente como una modalidad, por ejemplo, al respecto el jurista peruano Bramont Arias Torres, considera que con los delitos informáticos en realidad no se protege ningún bien jurídico, porque no hay, como tal un “delito” informático. Y que los delitos informáticos son modalidades de comisión de conductas delictivas ya tipificadas.

## 1.2 FORMULACIÓN DEL PROBLEMA

### 1.2.1 PROBLEMA PRINCIPAL

1.2.1.1 ¿Qué criterios justifican o justificarían la tutela de un bien jurídico colectivo específico, propiamente informático?

### 1.2.2 PROBLEMAS SECUNDARIOS

1.2.2.1 ¿Cómo afecta la tipificación de los delitos informáticos a los operadores jurídicos a la hora de formalizar las denuncias?

1.2.2.2 ¿Qué beneficios se pueden obtener con la conceptualización de los delitos informáticos como un ilícito pluriofensivo que afecta bienes jurídicos colectivos?

## 1.3 OBJETIVOS

### 1.3.1 OBJETIVO GENERAL

1.3.1.1 Identificar los criterios que justifican la tutela de un bien jurídico específico, es decir un jurídico colectivo referido a la funcionalidad e integridad de los sistemas informáticos.

### 1.3.2 OBJETIVOS ESPECÍFICOS

1.3.1.2 Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

1.3.1.3 Identificar los problemas que tienen los operadores de justicia en la persecución de los delitos informáticos.

## 1.4 JUSTIFICACIÓN DEL PROBLEMA

La presente investigación es necesaria para profundizar el análisis teórico, doctrinal que en los últimos años ha tomado fuerza y que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático. Sin embargo, ella no ha logrado imponerse, en parte por los reproches de los que ha sido objeto. En la presente tesis se efectuará un análisis crítico de las opiniones que pueden incluirse dentro de esta tesis. Sobre esa base, se planteará que reconocer un bien jurídico

específico, propiamente informático, se justifica si los delitos informáticos, fuera de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. A fin de delimitar su objeto de tutela, se reflexionará sobre las funciones que cumplen los sistemas informáticos para el libre desarrollo de la persona, así como para las instituciones que están a su servicio en un Estado democrático de derecho.

## 1.5 DELIMITACIÓN DE LA INVESTIGACIÓN

### 1.5.1 ESPACIAL

El presente trabajo de investigación tendrá un escenario de estudio a nivel nacional, donde se va a realizar con los Artículos del Código Penal, Ley de Delitos Informáticos LEY Nº 30096 y a la Constitución Política del Perú, así como con las normas internacionales donde se regulan los delitos informáticos.

### 1.5.2 TEMPORAL

La presente investigación es longitudinal, pues se toma como análisis la información encontrada en los últimos cinco años.

### 1.5.3 LIMITACIONES

La principal dificultad que encontramos al desarrollar la tesis es la poca información sobre el tema en la doctrina nacional. La mayoría de textos especializados son de doctrina internacional, lo cual ha hecho que su adquisición sea costosa y de difícil acceso. Así mismo por ser un tema que se encuentra en desarrollo y debate, las posiciones doctrinarias son en muchos casos disonantes, lo cual ha implicado un mayor tiempo de análisis.

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1 ANTECEDENTES DE INVESTIGACIÓN

### 2.1.1 A NIVEL INTERNACIONAL

Carolin Anabel Ruiz Cruz (2016). Realizó un trabajo titulado: *"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"* (Universidad Nacional de Loja, Ecuador). La cual tiene como objeto dar una visión clara sobre los delitos informáticos, en especial sobre la violación de los derechos constitucionales de los ciudadanos, que se generan por la utilización de las tecnologías de la información y de la comunicación, como el correo electrónico, transacciones financieras, comercio electrónico y la utilización de las redes sociales; se analiza y conceptualiza la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales y se establecen alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

María Gloria Barrera (2014). Realizó una tesis para obtener el grado académico de abogado, titulada: *"Determinar los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana* (Facultad de Derecho de la Universidad Central del Ecuador). Este trabajo trata sobre Determinar los Delitos de Estafa Informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana contiene 5 Capítulos:

Dar a conocer los Delitos Informáticos en el Ecuador, su regulación, iniciativas de investigación, tecnología formación de los especialistas que investigan dicho delito, identificar los retos y brechas que deben ser superadas en nuestro país, para el tratamiento de los mismos.

CAPITULO I.- La investigación se inicia con una retrospectiva histórica, continúa con una aproximación teórica de lo que es la delincuencia informática, así como sus particularidades específicas.

CAPÍTULO II.- Aquí se investiga los sujetos que intervienen en este delito y los bienes jurídicos que se lesionan, se realiza un análisis de los diferentes tipos de delitos informáticos.

CAPÍTULO III.- En este capítulo se analizan los tipos de delitos informáticos que existen y si constan o no en el catálogo de Delitos del Código Penal, se estudia la persecución y la forma de probar los delitos cometidos, se analizan los delitos informáticos en las legislaciones extranjeras.

CAPÍTULO IV.- Encuestas y entrevistas para conocer resultados de la investigación.

CAPITULO V.- Se exponen las conclusiones a que se arribó luego de realizada la investigación, se establece las recomendaciones que desde nuestro punto de vista académico-profesional; son las más adecuadas para solucionar el problema y finalmente se realiza la propuesta de estructuración de un proyecto de Ley que tipifique el fraude financiero.

Gabriela Cristina Chauca Acero (2014). Realizó una tesis de título: *EL PRINCIPIO DE PROPORCIONALIDAD EN LA PREVENCION DE LOS DELITOS INFORMATICOS* (Universidad Regional Autónoma de los andes, Bolivia). Esta tesis elabora un análisis jurídico sobre la aplicación del principio de proporcionalidad para la prevención de los delitos informáticos. Esta investigación pretende identificar que en la realidad no se aplica el principio de proporcionalidad para este tipo de delito, ya que una vez concluida la investigación podemos poner en práctica el Principio de Proporcionalidad en la prevención de los delitos informáticos, tenemos hoy en día varios delitos como: el fraude, el robo, chantaje, el cual determina las causas, consecuencias que produce el mal uso de las redes sociales, las faltas contravenciones administrativas que se realizan con el ánimo de causar daño de perjudicar y aprovecharse de bienes y servicios ilícitamente el cual incurre en la infracción penal, como consecuencia de la no aplicación del Principio de Proporcionalidad en la Prevención de los Delitos Informáticos.

### 2.1.2. A NIVEL NACIONAL

Carlos Orlando Yupanqui Homareda (2015). Realizó una tesis titulada: *"IMPACTO DEL DECRETO LEGISLATIVO Nº 1182 EN EL CONTENIDO ESENCIAL DE LOS DERECHOS A LA INFORMACIÓN Y LIBERTAD DE EXPRESIÓN"* (Facultad de Derecho y Humanidades de la Universidad Autónoma del Perú). La investigación sobre la propuesta de elaboración del Nuevo Marco Teórico de los Delitos Informáticos en el Perú y los aspectos que involucra su uso como apoyo teórico-científico para los operadores de justicia que actúan sobre los delitos informáticos (Policías, Fiscales y Jueces) y de otras instituciones y organizaciones comprometidos en la lucha contra dicha problemática.

El gobierno promulgó el Decreto Legislativo 1182 que determina incorrectamente que la información sobre la ubicación de un usuario, obtenida mediante la geolocalización de su teléfono móvil, no forma parte del contenido constitucionalmente protegido del secreto y la inviolabilidad de las comunicaciones. No obstante, como se desprende de la Constitución, de sus leyes de desarrollo y de la jurisprudencia existente, dicha información sí se encuentra igualmente protegida que el contenido mismo de la comunicación. Siguiendo este razonamiento, la norma propone que el acceso a dicha información puede ser ejecutado por la policía sin la necesidad de contar con una autorización judicial previa, estableciendo un mecanismo de aprobación judicial posterior para legitimar esta acción. El artículo 10 de la Constitución contradice esto, al establecer que cualquier procedimiento que involucre el acceso a esta información por parte de un tercero debe de ser autorizado y motivado por un juez.

Además de la inconstitucionalidad de sus medidas, el Decreto Legislativo 1182 interfiere también con la implementación del Nuevo Código Procesal Penal en la medida que resta atribuciones al Ministerio Público de forma ilegítima e invalida de facto normas penales que ya disponían cómo debía ser la solicitud y el acceso a los datos de geolocalización. Todas estas medidas buscan ampararse en la interpretación de que la policía puede actuar de esta

manera cuando esté frente a un delito flagrante. Por supuesto, esta interpretación está llena de deficiencias y no tiene sustento en la jurisprudencia nacional.

El Decreto Legislativo 1182 también obliga a las empresas de telecomunicaciones a registrar y conservar los datos relacionados con las comunicaciones de sus usuarios, incluyendo registros de llamadas, navegación por Internet y ubicación geográfica. De esta forma, nuestros datos privados estarán a disposición del escrutinio policial durante el plazo de tres (3) años. Esto no es más que la legalización de la vigilancia masiva e indiscriminada, cuya implementación en estas condiciones no resulta necesaria, idónea ni proporcional a los fines que persigue. En otros países existen actualmente normativas similares que ya fueron derogadas, archivadas o enfrentan procesos para que se evalúe su constitucionalidad.

Alejo Pardo Vargas (2018). Realizó un trabajo de investigación titulado *"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018"*. (Facultad de Derecho y Ciencias Políticas de la Universidad Cesar Vallejo). Tuvo como objetivo general Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Para el cual se utilizó serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptivo explicativo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, nacionales y extranjeros, llegándose a conclusiones precisas.

En tal sentido, se concluyó que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Finalmente se recomienda que el Congreso de la República formule iniciativa legislativa de para la adhesión del Perú al convenio de Budapest, así

como debe legislar en forma expresa y tipificar los delitos informáticos contra el patrimonio, diferenciando las modalidades, sean éstos delitos de fraude, estafa, sabotaje o hurto informático, se debe crear fiscalías especializadas en delitos informáticos, la Corte Penal internacional debe asumir competencia para conocer delitos informáticos de carácter trasnacional y en todas las Universidades se debe incluir un curso obligatorio de derecho informático, así como a nivel de la formación primaria y secundaria se debe incluir en la malla curricular el curso de informática, con énfasis en la prevención de todo tipo de delitos informáticos.

Jorge Martin Paredes Pérez (2013). Realizó una tesis titulada: *"De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010"* (Facultad de Derecho de la Universidad Mayor de San Marcos). El estudio desarrolla el problema principal referido a los problemas que se presentan al momento de la calificación del tipo penal de delito Informático, ya sea al formalizar la denuncia fiscal o al calificar dicha denuncia por el órgano jurisdiccional y su impunidad.

Igualmente, este trabajo se propone como objetivo principal demostrar que las conductas que emplean, utilizan o se basan en sistemas informáticos se encuentran deficiente e insuficientemente tipificadas y el ordenamiento jurídico resulta inadecuado para abarcar las principales manifestaciones que afectan importantes bienes jurídicos. Entre sus objetivos secundarios tenemos: *i)* determinar si existe una conducta a la que se pueda denominar en sentido estricto como "delito informático"; *ii)* Identificar cuáles son las limitaciones que existen en la tipificación del delito Informático al momento de formalizar la denuncia fiscal y/o en su calificación judicial; *iii)* demostrar que el delito informático se confunde en su calificación con otros tipos penales, de tal forma que se estaría afectando el principio de legalidad y seguridad jurídica; *iv)* identificar cuáles son las manifestaciones de la criminalidad informática que no se encuentran tipificadas; *vi)* demostrar que la Ley 27309 no tipifica correctamente las afectaciones del patrimonio individual con el uso de sistemas informáticos, pues éste se encuentra tipificado en el artículo 183.3 del Código Penal, entre otros.

Como hipótesis general se ha planteado la siguiente: La inadecuada tipificación del delito informático y de las conductas que utilizan los sistemas informáticos, la existencia de conductas vinculadas a las nuevas tecnologías que teniendo relevancia penal no se encuentran tipificadas, y el uso de nueva tecnología en la comisión de los tipos penales tradicionales, son los factores que afectan la subsunción, formalización, procesamiento y eventual sanción –generando sensación de impunidad- de conductas que hacen uso de medios informáticos en la comisión de delitos en el Distrito Judicial de Lima, durante el período 2009-2010.

Karina Joselin Zorrilla Tocto (2018). Realizó una tesis titulada: *" INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO"* (Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ancash, Santiago Antúnez de Mayolo). El estudio analiza los delitos informáticos Ley N° 30096 y sus modificatorias que son normativas que se acoplan a los nuevos cambios en el mundo, el avance tecnológico ha revolucionado las formas de celebrar contratos, transacciones, buscar información, difundir ideas, etc. todos estos cambian y a su vez posibilitan medios para delinquir, en ese sentido la Ley de delitos informáticos busca frenar esos medios o formas de delinquir, que si bien la presente ley no encuadra adecuadamente los tipos penales, pero es un intento de regularlos.

Ese intento de regularlos ha conllevado que el legislador incurra en inconsistencias y ambigüedades.

Elvis Yoseff Hancco Zapana (2018). Realizó una tesis titulada: *"La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú - 2017"* (Facultad de Derecho de la Universidad Nacional de San Agustín). El estudio analiza la tipificación del bien jurídico que la ley delitos informáticos que ha realizado el legislador al momento de estructurar el tipo penal del delito informático que regula la ley 30096, la investigación tiene como conclusión que nuestros representantes en el Congreso de la Republica muchas veces incurre en

problemas sobre técnica y sistematización legislativa, uno por exceso de regulación y otro por defecto, si el legislador considera más grave la comisión de un delito por el solo uso de tecnologías de la información debieron haberse subsumido en otras figuras más generales y, en todo caso excepcional, modificar las penas o agravantes de dichos delitos . Asimismo ha tenido una errónea y equivocada concepción del bien jurídico, porque los bienes jurídicos protegidos no son los sistemas y datos informáticos. Por otro lado, debe indicarse que la investigación es de naturaleza mixta, es decir de enfoque cualitativo y cuantitativo, con una mayor preeminencia del cualitativo, a través de la metodología de la interpretación hermenéutica.

## 2.2 BASES TEÓRICAS

### 2.2.1. Marco Doctrinario:

2.2.1.1. Derecho informático.

La palabra informática es un neologismo que deriva de vocablos información y automatización, el cual fue históricamente sugerido por Phillipe Dreyfus en 1962, quien la define como "la ciencia del procesamiento electrónico de la información como un cimiento del conocimiento". Trata de la concepción, realización y utilización de los sistemas para procesamiento de la información.

Sistema de información, se entiende como un conjunto integrado de componentes para recopilar, almacenar, procesar datos, además de proporcionar información, conocimiento, productos y servicios digitales. En tal sentido, el derecho informático conforme señala ZICCARDI, (2000) es el conjunto de normas jurídica que regulan la utilización de los bienes y servicios informáticos en la sociedad" (p.13)

La tesis que abordamos se enmarca en primer lugar dentro del derecho informático, específicamente en la rama del derecho penal informático, en tanto y en cuantos sistemas jurídicos que regulan las relaciones sociales a través de sistemas de información.

2.2.1.2. El derecho penal informático.

El derecho penal informático viene a ser una rama del derecho que regula y sanciona conductas penalmente relevantes que son efectuadas por medio de las tecnologías informáticas, es decir, el derecho penal informático se encarga de la prevención y sanción de la comisión de delitos informáticos.

Nosotros sostenemos al igual que Chaparro que actualmente la información de las empresas y las personas cada vez más tiende a ser almacenada en bases de datos electrónicas, esto ha provocado la aparición de diferentes formas de delitos informáticos derivados de la utilización de la

información con fines lucrativos o maliciosos o la alteración de la misma. (Chaparro, 2014, p. 32).

El derecho penal informático, aparece principalmente como una institución del derecho penal, que tiene la finalidad de sancionar conductas informáticas que afectaban al patrimonio de las personas y empresas, sin embargo, debido a la necesidad y por el avance de las nuevas tecnologías y las formas de comisión de actos socialmente reprochables, el rango de alcance del derecho penal informático se ha extendido a conductas en los sistemas informáticos que no afectan solo el patrimonio de las personas y/o empresas, sino también, comprende bienes jurídicos penalmente protegidos como la integridad de las personas, de los datos del mismo sistema, la fe pública, la seguridad y otros de similar relevancia.

Este punto es importante para la tesis que sostenemos, actualmente nuestro ordenamiento ya protege bienes jurídicos de naturaleza colectiva, por ejemplo, los delitos contra la administración de justicia o la administración pública, los delitos contra el orden económico o los delitos medio ambientales. En ese orden de ideas, sostenemos que los delitos informáticos afectan bienes jurídicos de naturaleza colectiva cuando vulneran sistemas informáticos que posibilitan el libre intercambio de bienes y servicios, el libre intercambio de información o el funcionamiento mismo del estado.

#### 2.2.1.3 La ciberdelincuencia

La evolución de la tecnología de la información dio a luz al espacio cibernético donde en Internet ofrece igualdad de oportunidades a todas las personas a acceder a cualquier información. Debido al aumento en el número de internautas, el mal uso de la tecnología es cada vez mayor, que conduce a los delitos cibernéticos. La ciberdelincuencia se refiere a los actos ilegales en qué parte del equipo es o bien una herramienta o de destino o ambos (Aggarwal, Arora, Ghai y Poonam, 2014, p.48).

Al respecto, (Das y Nayak, 2013, p. 142) señalan que la ciberdelincuencia es un término usado para describir en términos generales la actividad criminal en la que los ordenadores o redes de ordenadores son una

herramienta, un objetivo, o un lugar de actividad criminal e incluyen todo, desde el agrietamiento electrónico a ataques de denegación de servicio. También se utiliza para concretar delitos tradicionales en las que se utilizan los ordenadores o redes para realizar actividades ilícitas. El criminal cibernético puede detener cualquier vía ferroviaria, puede confundir a los aviones en su vuelo al confundirlo con señales incorrectas, puede hacer que cualquier dato militar importante caiga en manos de países extranjeros, puede detener los medios electrónicos y hacer que el sistema colapse en fracción de segundos.

Se puede, entonces, señalar que la ciberdelincuencia es cualquier conducta o actividad con el uso de la internet, sea éste de carácter privada o pública, o sistema informático cualquiera con la finalidad de lograr un objetivo ilícito que puede consistir en líneas generales en la destrucción o daño de ordenadores, base de datos, medios electrónicos, interceptaciones, así como sacar provecho indebido de los bienes, el cual se traduce en delitos informáticos o ciberdelitos.

Al respecto nosotras consideramos que es importante esta distinción, adoptada en nuestra legislación en concordancia con el convenio de Budapest; la conceptualización de ciberdelincuencia como un ilícito que se comete no solo por medios informáticos, sino que tiene como objetivo sistemas informáticos.

#### 2.2.1.4 Delito informático y evolución

Para definir cualquier tipo de delito, previamente debemos preguntarnos cuando es que un hecho constituye delito, esto es, en qué momento de la conducta humana pasamos de cualquier hecho a catalogar como delito, al respecto, (Lamperti. 2017), señala que un hecho constituye delito cuando es relevante jurídicamente, el cual implica que un hecho cualquiera para que sea delito debe estar regulado penalmente; entonces se podrá decir que el hecho encuadra en un tipo penal, es a ésta la que se le conoce como principio de legalidad, y el juez tiene la prohibición de sancionar otras conductas que no estén estrictamente tipificadas en la ley penal.

Al decir de (Levin y Ilkina, 2013) el Ciberdelito (o delitos informáticos) es cualquier crimen donde la tecnología de la información y la comunicación es:

1) utilizado como una herramienta en la comisión de un delito; 2) el objetivo de un delito; 3) un dispositivo de almacenamiento en la comisión de un delito (p. 14).

Por otro lado, (Villavicencio, 2014) considera que se entiende por criminalidad informática a aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. (p. 286). Con el cual coinciden (Laredo y Ramírez, 2013) al decir que el "Delito informático es el uso de cualquier sistema informático como medio o fin de un delito" (p. 45).

En este sentido, se puede establecer que una de las características fundamentales de los delitos informáticos es que, para la configuración de dichos ilícitos, el sujeto activo de la conducta delictiva, necesariamente debe emplear o usar un sistema o dispositivo informático.

Al respecto, Ramírez y Castro (2018) sostienen que el "(…) delito informático es todo aquel acto antijurídico y de carácter culpable que se da por medios informáticos o que pretende manipular o dañar computadoras, redes de internet o medios electrónicos" (p. 57). El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha provocado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. (Imbaquingo, *et. al*, 2016, p. 130).

Finalmente, (Besares, 2015, p. 53) señala que el "delito informático es la conducta típica antijurídica y culpable que afecta la seguridad informática y el derecho humano de la intimidad de las personas, mediante el tratamiento doloso de los datos, que se distinguen de los demás supuestos de los llamados delitos computacionales o electrónicos". En consecuencia, se puede afirmar que el delito informático es aquella conducta típica, antijurídica y culpable que se comete empleando los medios informáticos, con fines lucrativos o no.

Para acércanos a una conceptualización de Delitos Informativos, debemos tomar en cuenta lo señalado por (PEÑA CABRERA F., 2011):

"El hombre a fin de satisfacer sus necesidades más elementales y en su afán de obtención de lucro, no solo hace uso de medios lícitos, sino también se sirve de ciertos instrumentos que de forma ilegítima importa un ataque a ciertos bienes jurídicos merecedores de tutela penal. Instrumentos que en la actualidad adquieren ribetes en suma sofisticados, en ventaja al gran desarrollo alcanzando por la ciencia y tecnología, poniendo en vitrina un sistema plenamente informatizado en el funcionamiento de la información en lo cual respeta a datos y otros semejantes."

El delito informático se define como cualquier actividad delictiva que tenga lugar en o a través de computadoras o Internet u otra tecnología.

Tomando una interpretación más amplia, se puede decir que, el delito informático incluye cualquier actividad ilegal donde la computadora o Internet es un instrumento para cometer estos ilícitos.

Ciertamente el avance de la tecnología, permite conocer nuevas conductas cuyas características se particularizan por el uso de medios digitales y que para su investigación requieren técnicas especiales, que en nuestro país cuenta desde 2005 con la Unidad de Investigación de Alta Tecnología (DIVINDAT). Sin embargo, no todas las ciudades tienen una unidad especializada similar, la DIVINDAT no cuenta con suficiente soporte técnico, logístico y humano para responder, a tiempo, todos los pedidos formulados por el Ministerio Público. Ahora bien, esto no significa que toda investigación que involucre un caso de ciberdelincuencia es derivada a la DIVINDAT. Así, es facultad de la fiscalía remitir el caso a una unidad especializada distinta: Estafas o Robos, por ejemplo. Esto genera que policías no especializados en ciberdelito, investiguen este fenómeno delictivo.

Cabe resaltar que, en el caso del Ministerio Público, el 15 de febrero del 2021, la Unidad Fiscal Especializada en Ciberdelincuencia inició sus labores. La finalidad de esta unidad no es de investigación, sino de acompañamiento, coordinación, gestión y administración. El camino escogido es el adecuado

pues, de un lado, el fiscal penal adquirirá conocimientos especializados y, de otro, la red y la unidad se nutrirán de casuística y metodología de investigación, pero se necesita que está Unidad no sea solo de acompañamiento, sino la misma pueda brindarla atención necesaria a estos delitos.

Por su parte, DAVARA RODRÍGUEZ, citado por (MOISÉS BARRIOS, 2017, p. 26) afirma:

La denominación de delito informático, representa una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Como se advierte, el delito informático está referido a cualquier conducta de carácter ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de los mismos.

Desde sus términos iniciales como "delito informático", "delito relacionado con la informática" y "delito por ordenador", hasta conceptos más digitales, como "delito de alta tecnología", "delito habilitado tecnológicamente", "delito virtual" y "delito digital", se han utilizado una docena de términos.

Aparte de estos términos, para enfatizar la participación de Internet, también se han desplegado "ciberdelincuencia" (o "ciberdelincuencia"/«ciberdelincuencia») y «delincuencia en red».

En nuestro país el delito informático ha sido objeto de cambios, siendo que en nuestro ordenamiento jurídico estaba previsto en el artículo 182, segundo párrafo, inciso 3 del Código Penal Peruano, que fue tipificado como agravante del delito de hurto (hurto electrónico), el mismo que fue modificado por la ley 27309, expedido el 17 de julio del año 2009, ley que modificó el Título V del libro II del Código Penal, realizando la nueva inserción de un nuevo capítulo llamado “Delitos Informáticos”, que luego fue corregido y denominado “DELITOS INFORMATICOS PATRIMONIALES”, introduciéndose los delitos de: intrusismo, fraude informático, sabotaje informático y tráfico ilegal de datos, en ese contexto entra en vigencia la Ley N°30096, Ley de Delitos

Informáticos, publicado el 22 de octubre de 2013 y su modificatoria Ley N°30171, de fecha 10 de marzo de 2014, legislación que fue incorporada a nuestro sistema penal con el fin de adecuar nuestro ordenamiento jurídico interno, a las exigencias fijadas a partir del Convenio de Budapest.

2.2.1.5 Delitos de cuello blanco.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional. Son individuos con una gran especialización en informática, que conocen muy bien las particularidades de la programación de sistemas computarizados, de forma tal que logran un manejo muy solvente de las herramientas necesarias para violar la seguridad de un sistema automatizado (Pecoy, 2012). (Alcívar, Domenech y Ortiz, 2015, p. 46).

De manera general el sujeto activo que comete los ilícitos relacionados a delitos informáticos, son personas que poseen características particulares, esto es, que tienen conocimiento del manejo y uso de la informática que es el elemento diferenciador de los delincuentes convencionales.

DELITOS DE CIBERTERRORISMO: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

En el esquema de nuestra argumentación el ciberterrrorismo es la modalidad que más claramente contiene un bien jurídico colectivo de naturaleza informática, los ataques posteriores al 11 de setiembre y las nuevas modalidades del terrorismo internacional, han tenido como objetivos a los sistemas

informáticos que controlan servicios públicos, afectando bienes jurídicos colectivos.

2.2.1.6 Internacionalidad de los delitos informáticos.

A naturaleza de los delitos informáticos y la forma como se estructuran las organizaciones criminales, determina que se puedan cometer sin estar presente en el lugar donde se afectan los bienes jurídicos protegidos, es decir, no existe limitación espacial alguna para la comisión del ilícito penal.

En ese sentido (Temperini, 2014) precisa que, entre los diferentes desafíos inherentes o característicos de los delitos informáticos a nivel mundial, encontramos la posibilidad de que estos puedan ser cometidos sin respetar barreras geográficas o jurisdiccionales. Esto implica que cualquier delincuente informático puede ejecutar acciones desde un determinado lugar, conectándose a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. (p. 132).

Los delitos informáticos son cada vez más efectivos frente a la vulnerabilidad que muestran los sistemas y en especial los usuarios, puesto que "Los gobiernos en conjunto con millones de usuarios y empresas utilizan esta tecnología para el desarrollo de funciones que se desarrollan a diario. La seguridad en Internet se convierte en un trabajo crítico que causa estragos en la vida cotidiana. Cada día existen miles de ataques que se materializan principalmente por estados, naciones, gobiernos, y ciberdelincuentes". (López, López y Jerónimo, 2017, p. 2).

Por lo citado en los párrafos anteriores, consideramos que se debería tomar acciones que lleguen a una colaboración conjunta entre países y poder facilitar la sanción del ciberdelincuente, es decir, tenemos en claro que estos delitos no tienen parámetros de geografía por lo mismo una vez identificado el sujeto activo del delito, debe permitirse ser sancionado por las leyes que castiguen la comisión de delitos informáticos, en el país en el que se encuentre, no oponiéndose ni protegiendo al delincuente, sino colaborando y evitando los procesos largos de extradición.

Por otro lado, (García, 2017, p. 17) señala que la Internet, las redes y tecnologías similares se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones.

Al decir (Ibrahim, 2016, citando a Wall y otros), a diferencia de los delitos tradicionales, un plan criminal en el ámbito del ciberespacio puede implicar múltiples naciones y actores e incluso impacto en varios países al mismo tiempo. Así, mientras el crimen tradicional tiende a ser considerada a nivel local, los delitos informáticos se suelen considerar a escala global. Por ejemplo, supongamos que una persona en Rusia crea los "*virus / malware"*, mientras que otra persona en Nigeria lo alquila para enviar correos electrónicos para recopilar datos de las cuentas de crédito y un tercero en los Estados Unidos transfiere fondos usando los datos adquiridos ilegalmente, los tres individuos están implicados en diferentes fases (p. 45).

Nuestra tesis plantea, que sería beneficioso conceptualizar los delitos informáticos como delitos complejos, esto permitiría crear mejores estrategias, que articulen nuestro sistema penal, con los organismos internacionales y los demás gobiernos, en acciones colaborativas contra las organizaciones criminales multinacionales.

Es importante entonces que la internacionalidad de los delitos informáticos está determinada por la profunda innovación de las comunicaciones cuyo efecto jurídico se manifiestan en nuevas características, entre ellas merecen mencionarse la existencia de una red internacional descentralizada, desregulada que no conoce, tampoco reconoce, autoridad nacional visible, un ejemplo es la telefonía, que hasta no hace muchos años atrás era considerada un monopolio natural, con derechos concentrados en unos pocos, hoy la tecnología aplicada a la cibernética permite derrumbar el mito del monopolio natural, abriendo un campo nuevo a la competencia, donde la

conformación de una red universal permite transmitir, voces, imágenes, datos etc. (Rodríguez, 2013, p. 20).

Para entender el delito en una sociedad, es esencial y crucial entender todos los factores que influyen y contribuyen al crimen. La estructura socioeconómica y política de la sociedad necesita entender el crimen y el recurso que puede frenar el mismo. Las medidas preventivas y correctivas adoptadas por los mecanismos para controlar el delito y el comportamiento delictivo en la sociedad también se tienen en cuenta al estudiar la naturaleza y el alcance de un delito.

Según, (HERNÁNDEZ MENDOZA, 2003): Informática es la sistematización racional de la información. Consideramos que esta definición ubica a la informática en una actitud más próxima a una ciencia y en torno a la información, pero siempre tratada ésta en forma de sistema o sistemas. Es decir, sistematizar la información es la función básica de la informática, pero deberá hacerse racionalmente, de lo contrario el uso de herramientas que van desde el papel y el lápiz hasta las computadoras más sofisticadas, dependiendo del volumen de datos que se maneje para generar la información y los procedimientos que se establezcan para el procesamiento de los datos.

### 2.2.1.7 Sistema Operativo

El sistema operativo es un programa de control de la computadora, que proporciona herramientas o comandos que permiten la interacción con una computadora personal o PC. Según (HERNÁNDEZ MENDOZA, 2003, p. 45):

"El sistema operativo es el núcleo de toda actividad de software, monitores y controla toda la entrada y salida, así como la actividad de procesamiento dentro del sistema de computadora".

En palabras sencillas, podemos decir que es, un conjunto de programas, que controla la ejecución del Software de aplicación y actúa como una interfaz entre el usuario y el Hardware de la computadora.

Entendiéndose que el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una

computadora, es decir en la parte lógica e intangible del ordenador, en cambio el Hardware es la parte material que se puede tocar de la computadora, por ejemplo: mouse, teclado, CPU, etc. Es importante agregar que el DATO, es la unidad mínima que compone cualquier información, y en informática un dato es, una información breve y concreta proporcionada en un formato especifico y que puede ser procesada por un ordenador y por último una información es, "un conjunto organizado de datos que tiene un significado especifico más allá de cada uno de estos, de manera independiente" (IBAÑEZ, 2009, p.9).

2.2.1.8 Redes de Computadoras.

La red de computadoras, está referida a la interconexión que existe entre estas máquinas, en este sentido se expresa (HERNÁNDEZ MENDOZA, 2003, pp. 84-85) afirmando:

Conforme las PC se difundieron en los negocios y aparecieron los complejos multiusuarios de software, conectar las PC se convirtió en una meta de las organizaciones. La comunicación de datos, es decir, la comunicación electrónica de información entre computadoras se convirtió en el punto esencial para la industria de estas máquinas. El rápido crecimiento de la red mundial de computadoras conocida como internet hizo que la difusión de comunicación de datos se apresurara.

La primera red de computadoras se crea en 1969 y fue desarrollada por el Departamento de Defensa de los Estados Unidos y fue conocida como Arpanet, red de internet que estuvo vigente hasta 1990.

2.2.1.9 Sujetos Del Delito Informático.

2.2.1.9.1 Sujeto activo. - Desde nuestra perspectiva, puede ser cualquier persona que tenga la capacidad o condiciones técnicas suficientes para cometer algún delito informático ya que habrá sujetos que sí tengan grandes conocimientos (generales y específicos) en informática para cometer este delito informático, como también sujetos con mínimos conocimientos, ejemplo fraude informático y proposición a menores de edad con fines sexuales por medios

tecnológicos respectivamente. Nuestra doctrina, clasifica según el comportamiento y fin deseado de estos sujetos:

- HACKER.- Es aquella persona que ingresa vulnerando medidas de seguridad y sin autorización a una computadora y explora su interior, pudiendo acceder a todo tipo de ambientes como " noticias, servicios financieros, información financiera, correo electrónico, etc." (BLOSSIERS y CALDERON 2000, p. 56).

- CRACKER.- Es aquel que rompe con la seguridad de un sistema, con el fin de ingresar a ella y destruir información, es considerado un vandálico virtual.

- PREACKER.- Es una persona que investiga los sistemas telefónicos, teniendo como instrumento o medio el uso de la tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.

- VIRUCKER.- Se refiere al creador de un programa que, introduciendo en forma dolosa un "virus", destruye, altera o inutiliza una información contenida en un sistema de cómputo. Existen dos tipos de virus, los benignos, que molestan, pero no dañan y los malignos, que destruyen información o impiden trabajar.

- COPYHACKERS.- Son una nueva raza, no tienen los conocimientos de un Hacker, por ello extraen información de este, empleando la ingeniería social para convencer y entablar amistad con los verdaderos Hacker para así terminar su trabajo, copiándoles los métodos de ruptura para luego venderlos a los bucaneros (comerciantes de la red).

2.2.1.9.2 Sujeto pasivo.- Cualquier persona y dentro de este rango encontramos con mayor vulnerabilidad a las personas que no poseen conocimientos informáticos básicos, las mismas que pueden ser engañadas fácilmente para la comisión de estos delitos, que según Littejohn Shinder, 2003, pp. 181 – 184, existen categorías:

- Los Nuevos en la red: Los recién llegados no pueden darse cuenta de que sus sistemas, pueden infectarse con virus con solo abrir un mensaje de correo electrónico o visitando un sitio web equivocado.

- Inocentes por naturaleza: Por lo general están conformados por adultos mayores y niños o menores que por su inocencia, curiosidad no les permite entender que existe delitos en la red.

- Desesperados: Personas que pueden estar buscando amor, salvación, trabajo tienen necesidad de dinero lo que los hace vulnerables frente a estos cibercriminales.

- Pseudo Víctimas: Personas que informan crímenes que jamás se han cometido o se presentan ellas mismas como víctimas.

2.2.1.10 Tipos de Virus Informáticos.

Los antecedentes de los delitos informáticos van aparejados al desarrollo de las tecnologías informáticas y de comunicación en el ciberespacio, escenario en el que los delincuentes pueden cometer delitos desde cualquier parte del mundo, únicamente accediendo a una computadora, viéndose favorecidos por el anonimato que el ciberespacio le brinda y la gran cantidad de víctimas que se hallan expuestas.

Alguno de los antecedentes fácticos que posteriormente darían lugar a la comisión de los delitos en mención, se encuentran los virus informáticos, que son:

1) El CREEPER.

Fue el primer virus informático con carácter demostrativo en ordenadores de ARPANET (Red de computadoras utilizada como medio de comunicación, la primera comunicación con ARPANET se dio entre la Universidad UCLA de California y el instituto de investigación de Stanford el 29 de octubre de 1969), el CREEPER, fue un programa que podía recorrer una red saltando de un ordenador a otro mientras realizaba una tarea específica.

2) RABBIR

El primer virus informático con carácter dañino fue RABBIR, que se reproducía haciendo copias de sí mismo en un mismo ordenador hasta obstruir el sistema reduciendo su capacidad de rendimiento, esto provocaba que finalmente quede bloqueado.

2.2.1.11 Fraude Informático o Pharming.

Referido a: "(…), los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) La introducción, alteración, borrado o supresión de datos informáticos; b) Cualquier interferencia en el funcionamiento de un sistema informático" (artículo 8 del Convenio de Budapest).

El Pharming, asociado al phishing es:

Un tipo de fraude informático que ha aparecido desde mediados de la década pasada, cuya finalidad común es la de apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comercializarlos ilícitamente, o bien, conseguir claves de "e-banking" para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra, realizando una operación de transferencia de activos a un tercero que se denomina "mule". (OXMAN, 2013, pág. 216)

Según lo previsto por la Organización de Naciones Unidas que reconoce como delito al fraude cometido mediante manipulación de computadoras, el fraude puede ser cometido:

- Mediante manipulación de computadoras. Conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y fácil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. (HALL, s.f.)

- Manipulación de Programas: Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es del denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. (HALL, s.f.)
- Manipulación de datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipos y programas de computadoras especializadas para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y las tarjetas de crédito.

Por su parte, (KATERIN, 2019) agrega los delitos informáticos específicos, entre los que se tiene al sexting, consiste en enviar mensajes, fotos o videos de contenido erótico y sexual a través del dispositivo móvil mediante redes sociales o una aplicación de mensajería instantánea. El Grooming, delito que consiste en realizar acciones y conductas realizadas por un adulto, que actuando en anonimato busca a tomar videos o imágenes de un menor de edad.

Las Extorciones, Delito que consiste en obligar a una persona, utilizando la violencia, amenaza e intimidación, a realizar u omitir realizar un negocio jurídico con ánimo de lucro y generar perjuicio. El Pheraking, delito que consiste en acceder a redes sociales utilizando cuentas ajenas para realizar llamadas telefónicas.

Como ejemplo en legislación comparada, el profesor español (ACURIO DEL PINO, pág. 41) refiriéndose a la legislación ecuatoriana señala:

El nuevo Código Penal introduce el concepto de fraude informático, consistente en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia

de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. Los Arts. 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

2.2.1.12 Sabotaje informático.

El delito de daños informáticos o también denominado sabotaje informático persigue la sanción de quien perturba un procesador de datos que es de esencial importancia para una empresa ajena o para una autoridad, a través del menoscabo, destrucción, deterioro, inutilización, eliminación o transformación de un equipo de procesamiento de datos o un soporte de datos. La configuración de un tipo penal especial de daños se fundamentaría en la toma de conciencia acerca de la necesidad de un desarrollo del procesamiento de datos libre de perturbaciones, para la economía y la administración pública y, a su vez, en la comprobación de los elevados daños que conlleva esta especial forma peligrosa de sabotaje económico. (Krutisch, 2004).

La posición de Krutisch en el derecho penal alemán, aporta un punto importante a nuestra argumentación, ya que conceptualiza un tipo penal especial asociado a un derecho fundamental, es decir a un derecho constitucionalmente protegido, este es el derecho al desarrollo de un procesamiento de datos libre de perturbaciones, nos resulta claro que si bien es cierto la afectación finalmente es al orden económico, este resulta indesligable de los sistemas de procesamiento de datos que hacen posible su funcionamiento.

Para el profesor Simón Mayer, cuando los delitos informáticos stricto sensu son perpetrados a través de internet, ellos afectan, además, un bien jurídico común, denominado **funcionalidad informática** esto es, aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo (Mayer, 2017).

Uno de los casos más sonados del sabotaje informático ocurrió en EEUU, en la empresa Omega Engineering, donde un programador luego de ser despedido, decidió vengarse de la compañía borrando todo su software mediante

una bomba lógica activada diez días después del despido. Este sabotaje causo una pérdida patrimonial a la empresa, pero también causó daños a todos los usuarios que dependían del funcionamiento de la empresa en una cadena que afecta a sociedad como un colectivo, podemos apreciar entonces que la tesis del profesor Mayer, también aporta argumentos hacia una conceptualización de un bien jurídico colectivo de naturaleza informático presente en estos delitos.

2.2.1.12 Espionaje Informático.

La profesora chilena Laura Mayer, explica que el espionaje informático es un tipo penal que no está completamente delimitado, ya que dependiendo de la modalidad y el bien jurídico afectado, adquiere distintas conceptualizaciones, así refiere: En primer lugar, el sentido y alcance de aquello que denominamos «espionaje informático» no es evidente. En efecto, bajo dicho rótulo suelen incluirse conductas bastante disímiles en su forma de ejecución y gravedad, las que pueden abarcar el mero acceso indebido a datos o programas; pasando por el acceso indebido a sistemas informáticos que importa conocer, de alguna manera, la información en ellos contenida; hasta llegar al acceso a y obtención indebida de datos o programas. Al mismo tiempo, según la clase de información a la que indebidamente se acceda —y que en su caso se obtenga—, será también el bien jurídico afectado por el comportamiento (por ejemplo, el patrimonio, la intimidad, etcétera). (Mayer. L. 2020).

Sin embargo el consenso en la doctrina actual ha conceptualizado al delito de espionaje informático principalmente relacionado a las formas penales del espionaje, es decir de una conducta relacionada con el concepto de «violación de secretos», que puede expresarse ya sea mediante la introducción indebida en la esfera del secreto (intromisión), o bien, a través de la difusión indebida del secreto al que se ha tenido acceso legítimamente (revelación).

Cualquiera sea la definición que la legislación adopte, el espionaje informático como delito se enmarca dentro de nuestra argumentación como un delito evidentemente pluriofensivo.

2.2.1.13 Bien Jurídico Protegido en los delitos informáticos.

Empecemos por establecer la diferencia entre bien jurídico y bien jurídico penal. Para ello partimos de la noción de que en la sociedad el Derecho en general tiene como misión prevalente la defensa de intereses que, una vez asumidos por el ordenamiento jurídico, se denominan bienes jurídicos. En consecuencia, los intereses sociales o individuales son muchos, los bienes jurídicos solo aquellos (intereses sociales) tomados por el Derecho para su defensa; por lo que la protección de bienes jurídicos es una tarea que asumen todos los sectores del ordenamiento jurídico. (URQUIZO. O.1998. p. 809).

Mientras que un bien jurídico penal es aquel interés social que siendo recogido, para su protección, por el ordenamiento jurídico (ya sea la Constitución, el Derecho internacional o el resto de la legislación) además merece y necesita que esa tutela jurídica sea reforzada, por lo que se debe acudir al Derecho penal para lograr dicho cometido. Se puede ver que el concepto de bien jurídico-penal es uno más restrictivo que aquel de bien jurídico. A fin de identificar el Bien Jurídico Protegido en los Delitos Informáticos, tomaremos en cuenta lo descrito por (VILLAVICENCIO TERREROS, 2014):

El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera (…).

En este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal.

En efecto, los bienes jurídicos afectados son diversos por ser un delito de tipo pluriofensivo, lo que significa tener cuidado en la descripción de cada conducta ilícita señala en la normativa pertinente.

Para los delitos informáticos no se requiere de una cualidad especial para ser considerado sujeto activo; a decir de (PEÑA CABRERA FREYRE, 2011):

Basta con que se cuente con ciertos conocimientos propios de la informática para realizar la conducta prohibida. Resulta admisible apreciar una autoría mediata, cuando el hombre de atrás se aprovecha de la buena fe del hombre de adelante, del instrumento quien, sin dolo, desconociendo la naturaleza de los actos que está cometiendo, ingresa de forma indebida a una red o base de datos.

Cabe recalcar que no se puede considerar como sujeto activo a personas jurídicas solo naturales; pero que, sin embargo, si está implicado una persona jurídica esta puede ser pasible de consecuencias accesorias descritas en el Código Penal en el artículo 105°.

El sujeto pasivo puede considerarse cualquier persona, sea natural o jurídica, estatales o privados. A decir de (VILLAVICENCIO TERREROS, Delitos Informáticos, 2014), citando a Gutiérrez Francés señala que: “El sujeto pasivo por excelencia del ilícito informático es la persona jurídica, debido al tráfico económico en el que desarrollan sus actividades, por ello son los sectores más afectados por la criminalidad mediante computadoras. Y entre ellos están: la banca, las instituciones públicas, la industria de transformación, etcétera”.

2.2.1.14 Los bienes jurídicos colectivos.

Luego de haber expuesto nuestra posición respecto de la concepción de los delitos informáticos y su legitimidad en un Estado social y constitucional de Derecho, y de lo que entendemos por bien jurídico-penal protegido, ahora, es oportuno enfocar nuestro análisis en el objeto de protección de los llamados “delitos informáticos”. Para ello, creemos que es necesario abordar el análisis de los “bienes jurídicos colectivos”, que son la clase de bienes jurídicos que desde nuestro punto de vista están en juego en estos delitos. Al respecto, la

doctrina penal ha distinguido dos vertientes teóricas respecto del entendimiento de los bienes jurídicos colectivos: la "teoría monista" y la "teoría dualista".

a) Teoría monista, esta teoría propugna por una supresión de la bifurcación dogmática entre bienes jurídicos individuales y colectivos, puesto que únicamente los primeros serían bienes jurídicos penalmente protegibles (MAYO, B. 2005). Dentro de la teoría monista se han reconocido en doctrina dos posturas: la teoría monista personalista y la teoría monista social o estatal (SOTO, S. 2003). Según la teoría monista personalista, solamente los intereses y libertades individuales son merecedores de protección penal, mientras que los bienes colectivos pasarían a tener una jerarquía inferior a ellos debido a su carácter derivativo (SOTO, S. 2003). Partidario de dicha tesis es Hassemer, quien, como representante de la "escuela de Frankfurt", propuso crear un "Derecho de intervención" distinto al Derecho Penal -reservado para protección de bienes jurídicos individuales- para proteger a los bienes jurídicos de naturaleza colectiva(SOTO, S. 2003). Dentro de la teoría monista, también, se encuentra la teoría social estatal, según la cual el objeto de protección penal se relaciona directamente con la satisfacción de necesidades de la colectividad antes que las del individuo. Es decir, los bienes jurídicos colectivos al igual que los bienes jurídicos individuales, pretenden evitar lesiones a un orden social establecido (SOTO, S. 2003).

b) Teoría dualista Esta teoría, en contraposición a la teoría monista, distingue a los bienes jurídicos individuales de los bienes jurídicos colectivos. En esta media, se elimina entre estos dos tipos de bienes jurídicos toda relación derivativa u orden jerárquico (ABANTO, M. 2006). Esta teoría fue inicialmente formulada por Tiedemann, para quien los bienes jurídicos colectivos tienen su fundamento en la evolución del sistema de relaciones sociales, generando el surgimiento de diversos intereses no centrados en la persona individualmente considerada, sino en el colectivo social (economía, mercado, etc.) (SOTO, S. 2003). Los bienes colectivos, por tanto, buscarían proteger ya no relaciones sociales esenciales o básicas dentro del sistema, sino relaciones sociales referidas al propio funcionamiento del sistema social (SOTO, S. 2003). De acuerdo a los partidarios de esta teoría dualista, no es que se olvide la dimensión individual de la

protección penal, sino que la misma, en todo caso, pasará a ser una ratio legis de la punición. (SOTO, S. 2003). Sobre este punto, nos parece razonable la postura adoptada por Soto Navarro, quien sostiene que más que una relación de jerarquía o derivativa ente bienes jurídicos individuales y bienes jurídicos colectivos, lo que existe es una relación de dependencia recíproca entre ambos (SOTO, S. 2003).

Por otro lado, la crítica que se ha formulado a la teoría monista social o estatal es que, en principio, es una teoría que habría sido avalada por el nacionalsocialismo alemán de la "Escuela penal de Kiel" y que daría lugar a una instrumentalización del individuo al servicio de la colectividad (SOTO, S. 2003). En efecto, teniendo como referente el modelo de Estado Social y Constitucional de Derecho, no se debería caer en una concepción colectivista pura del bien jurídico que olvide la dimensión individual de la persona humana como fundamento del ordenamiento jurídico.

A nuestro juicio, la teoría dualista es la que propone un entendimiento del bien jurídico colectivo e individual adecuado. En nuestra opinión, la distinción entre bienes jurídicos individuales y colectivos responde a su distinta función social. En contraste con los bienes jurídicos individuales, los bienes jurídicos colectivos son aquellos que tienen la función primordial de ser aprovechados por la sociedad en su conjunto. Es decir, ninguna persona puede ser excluida del aprovechamiento del bien jurídico y su aprovechamiento individual no impide ni obstaculiza el aprovechamiento por parte de otros (SOTO, S. 2003).

Asimismo, los bienes jurídicos colectivos no pueden dividirse conceptual, fáctica o jurídicamente y atribuir individualmente en porciones (SOTO, S. 2003). Desde luego, no puede decirse por ejemplo que cada persona disfruta de una parte de la "correcta gestión del patrimonio público", sino que toda la sociedad en abstracto aprovecha de la totalidad de dicho bien jurídico.

Este es el sentido que en nuestra tesis le otorgamos al bien jurídico colectivo, protegido en los delitos informáticos, los delitos informáticos afectan bienes jurídicos individuales como el patrimonio, pero al vulnerar sistemas

informáticos, vulneran la capacidad social de hacer uso de estos para realizar transacciones.

2.2.1.15 Clasificación de los bienes jurídicos colectivos

La doctrina penal ha realizado una clasificación de los bienes jurídicos de naturaleza colectiva. Así, el Prof. Bustos Ramírez identifica dentro de esta categoría a los bienes jurídicos institucionales, los colectivos (propiamente dichos) y los de control (BUSTOS, J. 2004).

a) Los bienes jurídicos institucionales son aquellos referidos a la preservación de determinadas instituciones básicas (procedimientos de solución de conflictos) para el funcionamiento del sistema (administración de justicia, administración pública, los sistemas de información, etc.).
b) los bienes jurídicos colectivos propiamente dichos son aquellos que se refieren a la satisfacción de necesidades de carácter macro social y/o macro económico (salud pública p. ej.).
c) Los bienes jurídicos de control son aquellos referidos a la propia organización del aparato estatal, para que éste pueda cumplir con su función de control social (seguridad interior y exterior).

Los bienes jurídicos colectivos aseguran, mediante procedimientos formalizados (instituciones) el ejercicio efectivo de los derechos e interrelaciones de la personas (BUSTOS, J. 2004).

Somos de la idea que existen nuevas realidades o nuevas valoraciones de realidades preexistentes que ameritan una protección penal efectiva, por lo que resulta necesario una cierta y siempre racional expansión del Derecho penal, debido a las transformaciones que la sociedad va experimentando, ya que el Derecho penal no es estático, sino que es un fenómeno histórico cultural sujeto al devenir, por lo tanto, sujeto a las transformaciones del quehacer humano. Se debe entender que el Derecho en general (y por tanto también el Derecho penal) es variable y dinámico debido a factores externos de carácter social, político y cultural que van supeditar la presencia de un ordenamiento jurídico determinado. El Derecho acompaña la evolución de la sociedad, ofreciendo o buscando ofrecer respuestas a los problemas que surgen con las transformaciones

o cambios que suceden de manera incesante en la sociedad, de manera que esté listo para actuar cuando los demás medios de control social fallen.

### 2.2.2. Marco Jurídico

2.2.2.1. Ley de Delitos Informáticos

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley

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

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

## CAPÍTULO III

## DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

### Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

## CAPÍTULO IV

## DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

### Artículo 6. Tráfico ilegal de datos

*Derogado

### Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

## CAPÍTULO V

## DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

### Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

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

## CAPÍTULO VI

## DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

### Artículo 9. Suplantación de identidad

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

## CAPÍTULO VII

## DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley.

QUINTA. Capacitación

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas

El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a

las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente.

El objeto de esta ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, expresión que consideramos que es correcta, sin embargo consideramos que existe un bien jurídico propiamente informático que necesita ser reconocido y mencionado de forma literal en esta ley, puesto que el libre intercambio de la información hoy en día requiere una mínima seguridad, por lo que conllevaría a la protección de un bien jurídico colectivo, para la persecución efectiva de estos delitos.

Así mismo, consideramos que el convenio internacional sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría y entrada en vigor en nuestro país el 01 de diciembre de 2019, el cual no hace más que exhortar a los países miembros sobre la creación de normativas, medidas legislativas que resulten necesarias respecto a estos delitos.

#### 2.2.2.2 Legislación de Comparada

#### 2.2.2.2.1 Bolivia

En el año 1989, en este país se consideró el análisis y tratamiento sobre legislación informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato productivo nacional mediante la investigación científico tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de informática. (Jiménez, 2017, p.364)

Es así que el Código Penal Boliviano, texto ordenado según Ley 1768 del año 1997, realiza una reforma general al Código Penal. Incorporando en el título X, un capítulo destinado a los delitos informáticos, sin embargo esta Ley no está exenta de la problemática actual, al abordar en el capítulo XI la tipificación y penalización de delitos informáticos, pues no contempla la descripción de estas conductas.

#### 2.2.2.2.2 Chile

En relación a la situación de delitos informáticos en el país de Chile, consideramos el estudio realizado por (CARO MARTÍNEZ, 2010), quien señala:

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La Ley 19223, publicada en el Diario Oficial el 7 de junio de 1993, en un corto articulado tipifica y sanciona la destrucción o inutilización de un sistema de tratamiento de información.

Le Ley pretende proteger un nuevo bien jurídico surgido en el uso de las modernas tecnologías computacionales: calidad, la pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizando de tratamiento de ésta, y de los productos que de su operación se obtengan.

No obstante, no sólo se protege ese bien, sino que además concurren otros, tales como: el patrimonio, la privacidad, la intimidad y la confidencialidad; la seguridad y fiabilidad y tráfico jurídico y probatorio; el derecho de propiedad sobre la información y sobre los elementos físicos.

La Ley contempla cuatro artículos que, si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas: el sabotaje informático y el espionaje informático.

El sabotaje informático (artículo 1° y 3°) comprende aquellas conductas tipificadas atendiendo al objeto que se afecta o atenta con la acción delictual, y que puede ser un sistema de tratamiento de la información o a sus partes componentes, en funcionamiento de un sistema de tratamiento de la información, o los datos contenidos en un sistema automatizado de tratamiento de la información. El atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación. El espionaje informático (artículo 2° y 4°) comprende aquellas figuras delictivas que atienden al modo operativo ejecutable y pueden ser, en primer lugar, delitos de apoderamiento, uso o conocimientos indebidos de la información, cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos. Estas figuras corresponden a lo conocido comúnmente como hacking. En segundo lugar, comprende también delitos revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

#### 2.2.2.2.3 Colombia

Al respecto, (CARO MARTÍNEZ, 2010), señala:

En la década pasada se consideraba, tanto en el campo nacional como en el universal, que la inseguridad jurídica respecto del costo probatorio de los mensajes de datos era el primordial inconveniente para el desarrollo del negocio electrónico y que su regulación, por consiguiente, era un tema de suma trascendencia. La expedición de la ley 527 de 1999 obedeció a esta necesidad jurídica a las transacciones electrónicas.

En la regulación de los medios electrónicos para la ley 527 el legislador, con fines de adaptar el régimen jurídico existente a las nuevas realidades, creó el criterio del equivalente funcional. Dicho criterio puede ser enunciado como sigue:

Si un mensaje da datos cumple con los mismos objetivos y tiene las mismas funciones que un medio tradicional o físico de transmisión de información, dicho mensaje tendrá los mismos efectos jurídicos que dicho medio físico". En ese sentido, no pueden negarse efectos jurídicos, validez o fuerza a cierta información por el solo hecho de que esté en forma de mensaje de datos. (…).

El delito informático en Colombia no está tipificado expresamente como una categoría delictiva individual y autónoma. El Código Penal de Colombia cuenta con un exclusivo artículo, el 195, que bajo el epígrafe de "acceso abusivo de un sistema informático" (hanking

en otras legislaciones), instituye una sanción multa, sin especificar la cuantía, para quienes abusivamente se introduzcan en un sistema informático salvaguardado con medida de estabilidad o se mantenga contra la voluntad de quien tiene derecho a excluirlo.

Es fundamental considerar que, sin perjuicio de existir o no una definición de qué es o qué no es un delito informático, el Código Penal trae definidos, delimitados y regulados muchísimos delitos propensos de ser realizados en un ámbito informático. Y, es allí precisamente, donde el juzgador y los investigadores deben encontrar relación, con fines de evitar la impunidad en cuanto a la ciberdelincuencia.

#### 2.2.2.2.4. Argentina

El 4 de junio de 2008 mediante Ley 26388 se modificó el Código Penal Argentino para incluir delitos informáticos sus respectivas penas, teniendo en su contenido temas como: Distribución y tenencia con fines de distribución de pornografía infantil; violación de correos electrónicos; acceso ilegítimo a sistemas informáticos; daño informático y distribución de códigos maliciosos; interrupción de comunicaciones o DoS.

Posteriormente, el 4 de diciembre de 2013 se publicó la Ley Grooming, Ley N° 26904, que responde a una necesidad de proteger a menores de edad en la comunicación cibernética; siendo así, se incorporó en el Código Penal el artículo 131, que sanciona a personas que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacta a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

En atención a éste manual, la Organización de Naciones Unidas estableció que los Estados asuman mecanismos de control social y de poder a fin de prevenir, disminuir la criminalidad asociada a delitos informáticos.

Según refiere el profesor chileno (OXMAN, 2013):

En el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones.

Como era de esperar, la palabra “Internet” aparecía solo una vez en el Manual y la palabra “ciberdelincuencia” no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro.

Agrega el autor citado, “Si bien el Manual centró su atención en el concepto de “delito informático”, es bien sabido que hoy en día la “ciberdelincuencia” recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional”

En el Manual en mención se advierte que desde 1994 la Organización de las Naciones Unidas preveía algunos tipos de delitos informáticos que el Internet traía consigo; a la postre aparecerían además otros tipos de delitos informáticos, dando surgimiento a la denominación de “ciberdelincuencias”, que sin ser propiamente jurídica ha permitido comprender a los diferentes tipos de delitos informáticos.

2.2.2.2.4. Brasil

La ley 12.737 promulgada en el año 2012, dispone la tipificación criminal de los delitos informáticos y otras providencias. Por su parte, la Ley 11.829 regula es Estatuto de la Niñez y la adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil y así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia e internet. (Jiménez, 2017, p. 365)

2.2.2.2.5. Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en qué difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que

intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten solo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

#### 2.2.2.3 El convenio de Budapest en el Perú

Ante el panorama de cibercriminalidad la comunidad internacional reaccionó con una serie de conferencias, convenciones, congresos y eventos internacionales, que derivaron en acuerdos, criterios, principios y medidas a fin de dar solución a los problemas generados por las nuevas conductas delictivas, ya que por el carácter transnacional de estos delitos y la posibilidad de cometerlos desde cualquier parte del mundo, ya sea porque son cometidos por personas que operan en diferentes países, porque las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación lo que provoca una serie de problemas como son los de la legislación y la jurisdicción aplicable al caso.

A su vez, esto dio impulso a que hayan surgido iniciativas de regulación por parte de organismos internacionales. En este sentido, la idea se remonta a 1989, una vez que el Consejo del continente Europeo divulgó una secuencia de sugerencias sobre la necesidad de que el derecho penal sustantivo para penalizar las conductas dañinas realizados por medio de redes informáticas. En 1997 el Consejo del continente Europeo conformó un Comité de Profesionales sobre la delincuencia en el ciberespacio para escribir una convención para facilitar la cooperación de los Estados en la indagación y persecución de los delitos informáticos y para conceder una solución a los inconvenientes de la delincuencia cibernética por medio de la adopción de una herramienta jurídica mundial.

Ya en su 109ava cumbre, la junta de Ministros del Consejo del continente Europeo, determinaron aprobar el 23 de noviembre del año 2001 el “Convenio de Budapest” la cual se promovió con miras a la prevención de la cibercriminalidad en el ciberespacio, en especial mediante una legislación idónea y uniforme, de manera tal que las conductas sancionables sean pasibles de ser investigadas por cualquier persona de los Estados integrante, y el 1 de marzo de 2006 entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético. Los estados que lo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobos cometidos mediante medios informáticos.

Es así que, por medios del reconocimiento de la necesidad de cooperación entre Estados para la lucha contra la cibercriminalidad, a fin de proteger los intereses de la sociedad ligado al desarrollo de las tecnologías de información se planteó como objetivo en el convenio la introducción de las conductas pasibles de sanción penal como ilícitas, así como adoptar procedimientos idóneos para la investigación y sanción de dichos ilícitos.

En conclusión, La Convención de Budapest, es actualmente el único instrumento internacional que aborda de manera específica el tema de cibercrimen y hace frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones para procesar a los delincuentes cibernéticos y representa un importante intento de regular el ciberespacio.

La penetración de las redes informáticas trajo consigo los ciberataques que hoy, de acuerdo con el Informe de Riesgos Mundiales 2019, se encuentran entre las amenazas globales más graves del planeta (Banco Interamericano de Desarrollo, 2016).

De ahí que el concepto de ciberdelincuencia se convirtiera en una preocupación para los gobiernos de todo el mundo, Cabe señalar que el convenio no define explícitamente el concepto de ciberdelincuencia, pero sí establece los tipos de cibercrimen que los países deben tipificar en sus legislaciones.

Falsificación informática: hace referencia a la introducción, alteración, borrado o supresión, deliberada y de forma ilegítima, de datos informáticos que dé lugar a datos no auténticos, "con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos".

Fraude informático: son los actos deliberados e ilegítimos que causen perjuicio patrimonial a otro mediante la introducción, alteración, borrado o supresión de datos; o causándole interferencias en el funcionamiento de sus sistemas informáticos.

Los delitos informáticos mencionados líneas arriba son de gran importancia, sin embargo, de alguna manera ya han sido tratados en la legislación peruana, por otro lado, hay temas novedosos para nuestra legislación como la estandarización de procesos penales y la cooperación internacional.

El Convenio de Budapest sobre la Ciberdelincuencia trae una secuencia de relevantes beneficios para los Estados Parte que hicieron constancia mundial de su consentimiento a

obligarse por esta herramienta mundial. Con base a lo estipulado en el Pacto, se rescata los primordiales beneficios para los Estados Parte del Acuerdo son los próximos.

▪ Ejercer una política penal común con objeto de defender a la sociedad ante la ciberdelincuencia, por medio de la adopción de una legislación correcta.

▪ Utilizar herramientas establecidas en el mismo Acuerdo para prevenir delitos que pongan en peligro o abusen de sistemas y datos informáticos.

▪ Conseguir cooperación en materia penal instantánea y fiable, lo cual fortalecerá las habilidades de detección, averiguación y sanción de los Estados Parte para la contienda positiva contra los delitos previstos en los artículos del capítulo II del Acuerdo.

Ahora que el Perú ha ratificado el acuerdo Budapest, se iniciaría con el proceso de utilización del Pacto, como ha ocurrido ya en otros territorios, por esto resulta fundamental desarrollar el efecto que esta van a tener en el cumplimiento de sus fines, y cabe preguntarnos de qué forma o forma el acuerdo perjudicara en la ley de los delitos informáticos del Perú, y si ello mejorará el procedimiento de los delitos informáticos.

Para eso nos centraremos en desarrollar las metas que tiene el acuerdo de Budapest; (1) el implantar una política penal común para defender a la sociedad mundial ante la cibercriminalidad, (2) conseguir una legislación específica, (3) la construcción de nuevos mecanismos de cooperación multinacional ante los delitos cibernéticos.

En todos los casos en los cuales el Pacto de Budapest ha elaborado propuestas de tipificación, se han desarrollado o modificado reglas en el territorio en relación con el mismo objetivo. Por lo general, las reglas peruanas poseen una redacción parecida, incluyendo puntos clave como la necesidad de que los delitos sean realizados “deliberada e ilegítimamente” e inclusive usando los mismos verbos rectores (infringir, generar, dar a conocer, alterar, suprimir, etcétera.). En realidad, lo que se observa es más bien una ampliación de términos pues en varios delitos se agregan acciones más allá de lo sugerido por el Convenio (introducir, clonar, etc.).

Además, la Ley N° 30096 introduce en la categoría de delitos informáticos otras conductas que no estuvieron contempladas en el texto final de Budapest, pero que han sido desarrolladas posteriormente a través de sus protocolos. Este es la situación de: Proposiciones a chicos, chicas y jóvenes con objetivos sexuales por medios tecnológicos (grooming), tráfico ilegal de datos individuales y la modificación de los artículos 162 (Interferencia telefónica) y

323 (Discriminación e incitación a la discriminación) del Código Penal para que incluyan como agravante la utilización de medios informáticos o Internet.

Esto último no está exento de determinada disputa, sin embargo en términos prácticos no perjudica en nada la futura utilización del Acuerdo, toda vez que entre los recientes adherentes se discuten protocolos para tipificar nuevos delitos como el discurso de odio y la xenofobia por medio de medios informáticos.

Podría decirse entonces que la creación de un marco común de derecho penal sustantivo es una tarea bastante avanzada en el Perú, pero haber llegado a dicha situación ha requerido superar varios obstáculos. Al menos a partir de 2010, el interés por regular las situaciones en relación a los delitos informáticos produjo diversas iniciativas legislativas que fueron materia de enormes debates entre los actores del ecosistema digital. La definición misma de "delitos informáticos" es problemática en tanto que no existe acuerdo en si esta debe comprender solo a los delitos en donde el bien jurídico es la información o bien informático o integrar además a los delitos habituales realizados por medio de medios informáticos. Ejemplificando, no en todos los casos se había cuidado la redacción y se castigaba conductas usuales en Internet como la construcción de bases de datos o actividades inofensivas y potencialmente beneficiosas como el ethical hacking. Diferentes expertos criticaron estos problemas en su momento y señalaron la distancia que existía en perjuicio del país entre dicha norma y el estándar propuesto por el Convenio de Budapest. Recién con las modificaciones introducidas por la Ley N° 30171 publicada en 2014 se mejoró la redacción.

Sin embargo consideramos que el grado de aplicación efectivo de parte de los operadores del sistema de justicia es incierto. En comienzo, no existe información pública disponible sobre la ocurrencia de esta clase de delitos, salvo por la continua y constante confirmación de actores privados de existente un riesgo inminente y que buscan dar productos de estabilidad. Consecuentemente tampoco se sabe el número de razones que sobrepasan la averiguación policial y se formalizan en un proceso penal, llegan a juicio y reciben una sentencia. Al no existir cifras públicas ni otros medios para conocer el escenario presente, existe la sensación de que los diferentes actores interesados trabajan a ciegas o de manera descoordinada, a pesar de disponer de una legislación adaptada al uso universal. Prueba de ello son las diferentes iniciativas sectoriales que son impulsadas actualmente y que, en la mayoría de los casos, son contradictorias entre sí. Peor todavía, hay otras que ya han reclamado la

vulneración de diferentes derechos con el objetivo de facilitar la labor de sus operadores ignorando procesos anteriores largamente consensuados.

# CAPÍTULO III

# METODOLOGÍA

## 3.1 MÉTODO DE ANÁLISIS

### 3.1.1 Tipo

La presente investigación es del tipo Jurídico-Doctrinal, dado que se busca profundizar las teorías, leyes y antecedentes.

### 3.1.2 Nivel

El nivel de investigación corresponde al nivel explicativo, dado que en la presente investigación se explica qué criterios justifican o justificarían la tutela de un bien jurídico especifico, propiamente informático.

### 3.1.3 Diseño

Esta investigación se ha enfocado en el estudio de delitos informáticos y los bienes jurídicos protegidos, utilizando un método deductivo.

### 3.1.4 Enfoque

El enfoque de la presente investigación es un enfoque cualitativo, ya que se tiene una relación directa con el campo de estudio, puesto que, se han recogido percepciones y de esta manera se tiene como punto de partida la realidad.

## 3.2 Población y Muestra

En la presente investigación, por la naturaleza de la problemática, no corresponde asignar datos estadísticos en esta sección de la investigación; puesto que los datos que van a ser analizados son percepciones recogidas de diversas investigaciones.

## 3.3 Técnica

Esta investigación utilizó las técnicas de recolección de datos para las investigaciones de derecho, las cuales fueron:

3.3.2 Análisis de Registro Documental.

La misma que se dio por medio del análisis jurisprudencial así como doctrinal, esto con el fin de reforzar los conocimientos sobre delitos informáticos y los bienes jurídicos protegidos por los mismos.

3.3.3 Técnica de Encuesta.

Adicionalmente se usó la técnica de encuesta con el fin que se pueda formular preguntas a personas especialistas en el tema que puedan aportar datos, y así ayudar a la resolución de los problemas de investigación.

## 3.4 Instrumento

Los instrumentos de recolección de datos utilizados en la presente investigación son:

3.4.1 Guía de Análisis de Registro Documental.

Este análisis de registro documental sirve para construir un marco teórico, que se requiere para revelar aspectos contextuales, históricos, normativos, jurisprudencial, doctrinal, entre otros que estén afines al tema de investigación que venimos realizando.

3.4.2 Guía de Preguntas de Encuesta.

Es una serie de preguntas (cuestionario) con las cuales se busca establecer una serie de respuestas sobre el tema de investigación, tiene por objeto recabar, procesar y analizar información acerca de la conceptualización y tipificación de los delitos informáticos.

3.4.3 Ficha de Análisis de Carpetas Fiscales.

Esta ficha de análisis documental sirve para identificar en la carpeta fiscal los criterios de aplicación y adecuación del tipo delitos informáticos que los operadores jurídicos vienen aplicando.

## 3.5 ESTRATEGIA DE RECOLECCIÓN Y REVISIÓN DE DATOS

Se revisará y seleccionará el material para la elección del tema, se plantean diferentes problemáticas, se propone algunas interrogantes, se formulan objetivos, se selecciona el método, nuestra técnica e instrumentos (encuestas y análisis de documentos) se describe los resultados, posteriormente la discusión de los resultados, para que al final terminemos estableciendo las conclusiones y recomendaciones.

## 3.6 MÉTODO DE PROCESAMIENTO DE DATOS.

### 3.6.1 Método de Interpretación Jurídica

La presente investigación utiliza este método porque se interpretaron la Constitución Política del Perú, normas del Código Penal y la Ley 30096.

### 3.6.2 Método Deductivo

La presente investigación utiliza el método deductivo para el análisis de los datos; donde iremos desde La doctrina, normativa nacional, derecho comparado, artículos jurídicos, es decir conocimientos pre-existentes de manera muy general para llegar hacia el punto particular que está referido.

# CAPÍTULO IV

# ANÁLISIS DE LOS RESULTADOS

## 4.1. Presentación de resultados

Antes de presentar los resultados obtenidos en la presente investigación es preciso indicar que estos fueron trabajados según cada uno de los objetivos específicos propuestos. La información recabada del análisis de las carpetas fiscales fue organizada en fichas de análisis, las entrevistas del mismo modo. Se trabajó una interpretación de cada resultado, cuyo contenido desarrolla los resultados encontrados tras la aplicación de las fichas de análisis documentario aplicadas a la normatividad y la teoría analizada.

## GUÍA DE ANÁLISIS DE CARPETAS FISCALES

OBJETIVO: Analizar qué criterios justifican que los delitos informáticos tutelan un bien jurídico colectivo, propiamente informático.

| | |
|---|---|
| Número de carpeta: | 503-2020-727 |
| Materia: | Penal |
| Delito: | Fraude informático |
| Bien jurídico | Patrimonio |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente el bien jurídico patrimonial afectado mediante la modalidad de **Pharming, Cracker, Casher**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 504-2019-333 |
| Materia: | Penal |
| Delito: | Fraude informático |
| Bien jurídico | Patrimonio |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente el bien jurídico patrimonial afectado mediante la modalidad de **Pharming, Cracker, Casher**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 503-2020-1253 |
| Materia: | Penal |
| Delito: | Fraude informático |
| Bien jurídico | Patrimonio |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente el bien jurídico patrimonial afectado mediante la modalidad de **Pharming, Cracker, Casher**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 503-2020-3117 |
| Materia: | Penal |
| Delito: | Contra la fe pública-suplantación de identidad |
| Bien jurídico | Identidad de persona jurídica |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente le bien jurídico patrimonial afectado mediante la modalidad de **Pharming, Keylogig, Malware**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 503-2020-4925 |
| Materia: | Penal |
| Delito: | Fraude informático |
| Bien jurídico | Patrimonio |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente el bien jurídico patrimonial afectado mediante la modalidad de **Pharming, Cracker, Casher**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 503-2020-2746 |
| Materia: | Penal |
| Delito: | Fraude informático, suplantación de identidad |
| Bien jurídico | Patrimonio, fe pública |
| IV. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| V. Análisis | En la carpeta se referencia entonces solamente le bien jurídico patrimonial afectado mediante la modalidad de **Phishing**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| VI. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

| | |
|---|---|
| Número de carpeta: | 503-2019-11058 |
| Materia: | Penal |
| Delito: | Fraude informático |
| Bien jurídico | Patrimonio |
| I. Fundamentos | **Fundamentos del archivo de la carpeta:** Resalta en el análisis, que el principal argumento del archivo, en este caso es la falta de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br>**Adecuación típica:**<br>En este punto notamos que en la tipificación figura delito informático contra el patrimonio en la modalidad de fraude informático contra el patrimonio, conceptualizando el delito como un crimen patrimonial cometido mediante una computadora un sistema informático, es decir el instrumento es una computadora. |
| II. Análisis | En la carpeta se referencia entonces solamente le bien jurídico patrimonial afectado mediante la modalidad de **Phishing**, **Banking**. No referencia a un bien jurídico colectivo, o un bien jurídico propiamente informático que haya sido afectado, como la seguridad del sistema financiero |
| III. Conclusiones | 1.- La tipificación no incluye la afectación de un bien jurídico colectivo<br>2.- En la práctica, el delito es tratado como un delito contra el patrimonio común<br>3.- Se archiva por falta de individualización del presunto autor |

En la totalidad de carpetas fiscales analizadas, la válida y principal razón por la cual terminan concluyendo archivos de las investigaciones iniciadas respecto a delitos informáticos, es porque no se puede individualizar al presunto autor de los mencionados delitos, cabe resaltar que en estas disposiciones no se hace mención alguna a los bienes jurídicos o se justifican de alguna manera, lo que nos lleva a concluir que el no identificar correctamente un bien jurídico como "propiamente informático", hace que este no sea de interés colectivo, por lo tanto, sea considerado de carácter individual y debe ser sometido a una investigación en plazos ordinarios, no considerando la complejidad de estos delitos y limitando la correcta

investigación y contribución para la identificación del sujeto activo de estos delitos, por lo que concluimos lo siguiente:

| | |
|---|---|
| **1.- Del archivo.** | Al respecto debemos resaltar que en la totalidad de carpetas analizadas, se ordena el archivo por la imposibilidad de individualización del presunto autor del delito, que es un presupuesto de la formalización de la acción penal.<br><br>Nosotros consideramos que esto en la práctica constituye una suerte de camisa de fuerza para los fiscales. Es decir al conceptualizar los delitos informáticos en un sentido lato, es decir solo como un delito de modalidad que afecta bienes jurídicos individuales, no tienen más remedio que ordenar el archivo.<br><br>Recordemos que en el X Congreso de Naciones Unidas sobre Prevención del delito y Tratamiento del Delincuente, celebrado en Viena en abril del 2000 se realizó una importante distinción que contribuye a una mejor precisión del concepto delitos informáticos.<br><br>• La Ciberdelincuencia puede entenderse en sentido estricto, comprendiendo cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y datos que se procesan.<br>• La Ciberdelincuencia también puede entenderse en sentido amplio, comprendiendo cualquier ilícito cometido por medio de un sistema informático o una red de computadoras o relacionados con estos, incluyendo la posición o puesta a disposición de información mediante sistemas de información o redes de computadoras. |

| | |
|---|---|
| | • Al respecto consideramos que se debe tener en cuenta lo que plantea el profesor Miro, "Si utilizamos el término de forma amplia, podremos definir como cibercrimen o delito informático, cualquier comportamiento delictivo realizado en el ciberespacio, **entendiendo además por el mismo, el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio**, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet(...)(Miró, 2013, p.10). |
| **2.- Del Bien Jurídico.** | Al respecto primero tenemos que precisar que los bienes jurídicos pueden ser individuales o colectivos. Los bienes jurídicos individuales son de titularidad o sirven a una persona determinada o a un grupo de personas determinadas la vida o el patrimonio individual ( Kindhäuser .1989. p. 144.). En ese orden de ideas encontramos que la totalidad de las carpetas fiscales solo hacen referencia a bienes jurídicos individuales.<br>• Del análisis, encontramos que en las carpetas fiscales no hay ninguna conceptualización respecto a estos bienes, entendemos nosotros que la afectación de bienes jurídicos individuales incide directamente en el libre desarrollo de una persona determinada o de un grupo de personas determinadas, mientras que la afectación de bienes jurídicos colectivos incide indirectamente en el libre desarrollo de todas las personas. En ese sentido planteamos que existe una afectación a un bien jurídico informático, constituido |

| | |
|---|---|
| | por la integridad misma del sistema informático que los sujetos sociales utilizan cotidianamente.<br>• Además suscribimos lo planteado por Jorge Gonzales, entendiendo que cuando se comete por ejemplo un fraude informático, que supone manipular los datos del sitio web de un banco, para transferir fondos de la cuenta de alguno de sus clientes a un tercero, no solo se afectan los intereses patrimoniales del titular de esa cuenta, también se incide en la funcionalidad informática (González. J. 2014).<br>• Por estas razones nuestro análisis, sustenta la necesidad de conceptualizar los delitos informáticos incluyendo un bien jurídico colectivo de naturaleza informática en su tipificación. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°1)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Luis Alberto Del Carpio Iquira |
| **Cargo** | Fiscal adjunto provincial penal |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No existe un bien jurídico específico, ya que conforme a la Ley Nº 30096, se sancionan varias conductas que tienen bienes jurídicos distintos como la información, la indemnidad sexual, la intimidad, el patrimonio, etc.; e inclusive son pluriofensivas. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Considero que si son pluriofensivos, porque con una misma conducta se vulneran distintos bienes jurídicos; como, por ejemplo, en el delito de fraude informático del artículo 8 de la Ley Nº 30096, se protege -además del patrimonio- el sistema informático, la libertad e intimidad personal, etc. |

| | |
|---|---|
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Porque atentan principalmente contra la información, como principal bien jurídico protegido, el cual es de interés colectivo. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Considero que la ley de delitos informáticos Nº 30096 como marco legal, sí constituye una herramienta efectiva para sancionar los delitos informáticos, ya que tiene como referencia al primer tratado internacional de lucha contra la ciberdelincuencia, como es la Convención de Budapest; la misma que fue modificada por la Ley Nº 30171, a efecto de aclarar ambigüedades y conceptualizar el contenido de algunos tipos penales. De esta manera, nuestro marco normativo, respecto de los delitos informáticos, se encuentra conforme a las exigencias internacionales suscritas por nuestro país. Más aún, que en muchos casos estos delitos traspasan las fronteras, es necesario que los países involucrados tengan legislaciones similares para evitar la impunidad. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Considero que existe un criterio general que en estos delitos es muy difícil identificar a los autores; sin embargo, si desde que tomamos conocimiento de la comisión del delito, se hace una debida preservación de la evidencia, es mucho más probable que tengamos resultados positivos. Por otro lado, también es necesario familiarizarnos con los |

| | |
|---|---|
| | procedimientos de preservación de información de las principales plataformas de redes sociales e internet. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | Considero que no existe suficiente información sobre los delitos informáticos, pero no sobre conocimiento de la Ley, sino sobre conocimientos de nomenclatura informática, recolección de evidencia digital, tratamiento de la evidencia, interpretación de evidencia y presentación de la misma. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Considero que en los delitos informáticos se ha tratado de proteger los bienes jurídicos más relevantes o de mayor incidencia; sin embargo, en un mundo cada vez más globalizado e informatizado, es latente que surjan nuevas conductas delictivas a través de los medios informáticos. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | El error en el tratamiento de los delitos informáticos, es el desconocimiento de cómo funcionan los sistemas informáticos y la manera de recabar información para identificar a los autores de estos delitos, lo cual es uno de los principales problemas. Se desconocen herramientas, convenios y procedimientos para poder acceder a la |

| | |
|---|---|
| | información de las principales plataformas de internet. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | La ley de delitos informáticos está hecha en base a la Convención de Budapest; quizás, se pueda mejorar el uso de terminología para que sea más comprensible. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°2)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 28/11/2021 |
| **Entrevistado** | Antonio Chacon Rossello |
| **Cargo** | Fiscal provincial penal |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, porque los medios informáticos son un medio a través del cual se ejerce, evidencia o transmite otros bienes. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Me remito a la respuesta anterior. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Considero lo mismo que respondí en la primera pregunta. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Siendo un medio, está bien la descripción de tipicidad, pero la misma debe crear un contenido con el bien jurídico afectado. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | N.E. |

OBJETIVO 2: I Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | La informática es muy variable y actualizable, no se tiene la información suficiente. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | No, conforme con mi primera respuesta esos delitos son medios. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | N.E. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Primero, la permanente actualización; segundo, la capacitación permanente. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°3)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 29/11/2021 |
| **Entrevistado** | Eduardo Antonio Atencio Ramos |
| **Cargo** | Fiscal Provincial |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | Sí, es la afectación de los sistemas, datos informáticos y otros relacionados. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque a través de medios informáticos se pueden afectar diferentes bienes jurídicos, como patrimonio, intimidad, libertad. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Los bienes jurídicos son colectivos por su reconocimiento y ejercicio por cada persona. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Es un muy buen avance frente a la criminalidad que emplea medios informáticos para cometerlos. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | El marco normativo de la Ley 30096 desarrolla los tipos penales clasificados como delitos informáticos. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No hay demasiada literatura. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | No, solo establecen los medios empleados para cometer delitos ya conocidos. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Son medios especiales de comisión de delitos comunes, como los delitos patrimoniales. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Debería hacerse una adecuada redacción entre el artículo 5° de la Ley 30096 y el artículo 176-B segundo párrafo, para evitar concursos aparentes de normas. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°4)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 30/11/2021 |
| **Entrevistada** | Cristal Velásquez Fernández |
| **Cargo** | Fiscal Provincial |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, porque lo que se protege es la información, la cuál puede ser pública o privada, datos sensibles, patrimoniales; es decir, es indistinta. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque en la sociedad dónde se desenvuelven los datos están interrelacionados, un solo dato puede afectar distintos bienes. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Porque afectan los artículos 1 y 2 de la Constitución. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | No porque, a diferencia de otros delitos, estos presentan una sofisticación que excede a la norma penal; además, no interrelaciona con las demás ramas del derecho. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Se debe tener especialistas en la materia y peritos para poder tratar adecuadamente estos delitos; pues, son complejos. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No, se debe crear una especialidad. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Sí, totalmente. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Sí, pues son especiales. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Se debe considerar organismos especializados para que analicen estos delitos que coadyuven a la labor fiscal, emitiendo informes que podrían constituir prueba constituida. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°5)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 03/12/2021 |
| **Entrevistada** | Elva Teresa Bravo Palomino |
| **Cargo** | Fiscal adjunta |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, estos delitos tutelan distintos bienes jurídicos, tales como la intimidad, la libertad sexual, patrimonio, etc. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque la comisión del mismo puede vulnerar distintos bienes jurídicos. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Porque los bienes jurídicos vulnerados, afectan no sólo a una persona, sino también a la sociedad y pone en riesgo un bien jurídico colectivo. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Considero que es un primer paso, pero no es suficiente y tampoco se adecua a nuestra realidad. Por lo mencionado, no es una herramienta totalmente efectiva. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Los delitos informáticos deberían ser tratados como delitos complejos; por lo mismo, alterar su plazo de investigación |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | En realidad, la doctrina (jurisprudencia respecto a delitos informáticos) es insuficiente y escasa en nuestro ordenamiento jurídico, lo cual es una dificultad para la capacitación constante de algunos operadores de justicia. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Claro, considero que todavía se debe identificar claramente cuál es el verdadero bien jurídico a proteger en estos delitos, pues pienso que no son los sistemas y datos informáticos. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Sí, a veces se le trata a un delito informático como un delito común; o viceversa, por lo que crea confusión. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Podría especificarse mejor el delito jurídico protegido, y no sólo como los sistemas o datos informáticos, como actualmente se encuentra. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°6)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Alex Rogelio Zegarra Cossio |
| **Cargo** | Docente |
| **Institución** | UNSA |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, está bien tipificado |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque en su comisión concurren otros tipos penales |
| **3.¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | No, porque el sujeto pasivo es una persona particular o jurídica. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | En parte sí, porque dinamiza la pretensión punitiva como tal. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Deben tratarlos como una alta especialización donde el operador de justicia debe tener una especialidad en tecnología informática |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Si |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Si |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Es de urgencia. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°7)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Yanina Juárez del Carpio |
| **Cargo** | Docente |
| **Institución** | Universidad continental |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | Si, pues su perpetración vulneran la seguridad financiera, personal, y jurídica en general. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque dependiendo de la modalidad encontraremos diferentes bienes jurídicos protegidos. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Si, la seguridad en general porque esté bien engloba las diferentes ramas dónde puede ser protegido ( personal, financiera etc.) |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Considero que debe tener una mejor redacción en cuanto a los elementos descriptivos del tipo pena. |

| | |
|---|---|
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Con celeridad y dando la importancia que merecen, son nuevas modalidades de criminalidad |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Si |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Si |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | La precisión de sus elementos descriptivos. |

## GUÍA DE ENCUESTA

## (ENCUESTADO N°8)

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Juan Carlos Condori Quispe |
| **Cargo** | Fiscal |
| **Institución** | Ministerio Público. |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, es pluriofensivo |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Si |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | También en algunos casos. Porque afecta a varios agraviados con un sola conducta |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | No. Porque falta incorporar algunas recomendaciones del convenio de Budapest, así como aparecido nuevas conductas delictivas por el avance tecnológico |
| **5. ¿Cómo considera que los operadores de justicia deberían** | Primero debería haber una especialización de este delito informático. Trabajar en |

| | |
|---|---|
| **tipificar los delitos informáticos?** | forma conjunta la divindat, fiscalía, poder judicial entre otras entidades |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No. Falta capacitación y especialización en los jueces y fiscales. Si bien, este año ha empezado a funcionar la fiscalía especializada de ciberdelincuencia, no es suficiente, se tiene que ampliar esta fiscalía a los demás distrito fiscales del Perú, así también se debería crear un juzgado especializado en ciberdelincuencia. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Sí. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Sí. Por falta de conocimiento y especialización |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Si bien tenemos implementada la normativa referida a la ciberdelincuencia, Ley Nro. 30096 además de encontrarnos dentro del convenio de Budapest, tenemos un camino importante por recorrer para el mejoramiento de dicha normativa, tomando en consideración la incorporación de diferentes componentes vinculados al análisis de conductas |

| | |
|---|---|
| | enmarcadas en la delincuencia informática |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°9)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Luis Cesar Salas Bejarano |
| **Cargo** | Fiscal |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | Sí. Porque ha merecido protección autónoma los sistemas informáticos y en otros casos se vinculan con otros bienes jurídicos (que utilizan las TIC como medios comisivos). |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Si, debido a que además de los bienes jurídicos específicos, en los tipos penales se involucran a otros como el patrimonio, la libertad, intimidad, etc. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Sí, porque no es atribuible a una sola persona (natural o jurídica). Sino que es un valor colectivo |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Necesita ajustes legislativos mínimos y de interpretación, no son lo adecuadamente efectivas las regulaciones por ausencia de |

| | |
|---|---|
| | órganos especializados que persigan esos delitos. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Son complejos y de intervención inmediata debido a la volatilidad de la prueba digital. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No, estamos en un franco desarrollo debido a la creación de la Unidad Fiscal Especializada. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Si, tienen bienes jurídicos autónomos y merecedores de protección penal. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Si, ya que la dogmática y la persecución requiere destrezas y actitud diferentes. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Mayor precisión conceptual que permita su aplicación a pesar del continúo avance de las TIC y sistemas informáticos sofisticados. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°10)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Glenda Vanessa Chávez Zúñiga |
| **Cargo** | Asistente de Juez |
| **Institución** | CSJAR |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | Si, por que se trata de información de carácter personal |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Si, vulnera distintos bienes jurídicos |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | Si, se trata de información personal y de entidades |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | Sí, todo delito tiene que estar sancionado por nuestro ordenamiento jurídico |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Como un delito grave por la alta complejidad y uso de tecnología para perpetrar un delito |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Si |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Si |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Las penas a imponerse de acuerdo a la tipificación y complejidad del delito. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°11)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Nazareth Olave Ugarte |
| **Cargo** | Fiscal Adjunta al Provincia |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, por cuanto si bien se señala que es el patrimonio, también podría considerarse el derecho a la intimidad, cuando se habla de extracción de datos relativos a la vida privada de connotación sexual de cada individuo. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Si, por que no sólo se vulnera con el acceso a un sistema informático que es de propiedad privada, sino también el patrimonio, la intimidad, el honor de acuerdo a los datos extraídos o manipulados. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | No, porque va depender de la forma de acceso al sistema informático |

| | |
|---|---|
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | No, porque muchas veces el problema es la obtención de las pruebas de la comisión del delito. |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Verificar el bien jurídico que efectivamente se prendió vulnerar, patrimonio, intimidad, debería ser una agravante por el medio empleado. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | No, es sólo un medio. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Si |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | La redacción de la norma. |

**GUÍA DE ENCUESTA**

**(ENCUESTADO N°12)**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| | |
|---|---|
| **Fecha** | 26/11/2021 |
| **Entrevistado** | Ronal Enrique Cueva Huanca |
| **Cargo** | Fiscal Provincial |
| **Institución** | Ministerio Público |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | No, porque sería pluriofensivo. |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | Sí, porque serían varios bienes jurídicos vulnerados. |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | No, porque son bienes jurídicos individuales. |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | No, puesto que falta aún más herramientas para individualizar a los autores de estos ilícitos |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | Con la mayor rapidez y prontitud, para evitar mayores daños personales y materiales. |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | No. Falta más información. |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | Sí. |
| **8. ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes?** | Sí. |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | Las herramientas para individualizar a los autores. |

**Respecto al primer objetivo planteado que es:**

OBJETIVO 1: Identificar la necesidad de conceptualizar la afectación de bienes jurídicos colectivos en los delitos informáticos.

| Pregunta | Análisis |
|---|---|
| 1 | En la primera pregunta planteada, se les preguntó si consideraban que existe un bien jurídico específico en los delitos informáticos, siendo que los encuestados consideran que no existe un bien jurídico protegido específico porque indican que se afectan varios bienes jurídicos protegidos, como, por ejemplo, la intimidad, la libertad sexual y el patrimonio.<br>• La mayoría de los encuestados conceptualizan los delitos informáticos, como pluriofensivos, sin embargo no consideran que exista un bien jurídico propiamente informático. |

| | |
|---|---|
| | • Al respecto consideramos que además de los bienes jurídicos tradicionales existe un bien jurídico común, denominado **funcionalidad informática** esto es, aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo (Mayer, 2017).<br>• Es importante resaltar que los delitos informáticos pueden tener como objetivo a los mismos sistemas informáticos. |
| 2 | En cuanto a la segunda pregunta planteada, se les preguntó si consideraban que los bienes tutelados en los delitos informáticos son pluriofensivos, al respecto la mayoría de los encuestados indicaron que los delitos informáticos son pluriofensivos porque se vulneran distintos bienes jurídicos.<br>• Al respecto debemos señalar que en nuestra tesis planteamos que los delitos informáticos son delitos pluriofensivos, que la afectación de los bienes jurídicos tutelados incluye a la seguridad de los sistemas informáticos.<br>• Además entendemos que el bien jurídico tutelado en los delitos informáticos se concibe de manera conjunta y concatenada, el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera (…).<br>• En este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal. |

| | |
|---|---|
| 3 | En cuanto a la tercera pregunta planteada, se les preguntó si creían que los delitos informáticos tutelan un bien jurídico colectivo, al respecto solo algunos de los encuestados consideraron que los delitos informáticos sí tutelan un bien jurídico colectivo porque afectan no solo a una persona sino a la sociedad y porque afectan los artículos 1 y 2 de la Constitución.<br>• Al respecto nosotros planteamos que los delitos informáticos tutelan bienes centrados en la persona individualmente considerada, y bienes jurídicos en el colectivo social (economía, mercado, información, etc.) (SOTO, S. 2003). Los bienes colectivos, por tanto, buscarían proteger ya no relaciones sociales esenciales o básicas dentro del sistema, sino relaciones sociales referidas al propio funcionamiento del sistema social (SOTO, S. 2003). |
| 4 | Respecto a la cuarta pregunta: ¿Considera que la ley de delitos informáticos es una herramienta efectiva? ¿Por qué?, solo 2 de los encuestados consideran que es una herramienta efectiva, sin embargo, los otros demás consideran que no, puesto que no se adecua a nuestra realidad y por la sofisticación del delito que excede a la norma penal.<br>• Al respecto cabe resaltar que la mayoría de encuestados refieren la dificultad para individualizar a los autores del delito. |
| 5 | Respecto a la quinta pregunta: ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?, se obtuvieron respuestas distintas, puesto que los encuestados no muestran que existe un criterio general en estos delitos, al respecto advertimos que a pesar que la Ley 30096 desarrolla los delitos informáticos, la mayoría los entiende como delitos comunes con un criterio de modalidad, es decir solamente como delitos cometidos por medios informáticos que afectan bienes jurídicos ya tutelados. |

Objetivo 2. Identificar las deficiencias en la persecución de los delitos informáticos.

| Pregunta | Análisis |
|---|---|
| 6 | Respecto a la sexta pregunta: ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos |

| | |
|---|---|
| | informáticos? La totalidad de los Fiscales consideraron que no, ya que es insuficiente la información que existe, lo que dificulta para la capacitación de los operadores de justicia.<br>Este punto es crucial para nuestro planteamiento, ya que consideramos que se requiere de fiscalías y juzgados especializados en delitos informáticos. |
| 7 | Respecto a la séptima pregunta: ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos? Cuatro de los encuestados consideran que el bien jurídico a proteger por estos delitos, todavía debe ser claramente establecido, puesto que, hasta el momento se protege los bienes jurídicos de mayor incidencia y relevancia, pero no existe claridad sobre el bien jurídico protegido por parte de los delitos informáticos. |
| 8 | Respecto a la octava pregunta: ¿Considera Ud. que muchas veces se comete el error de tratar los delitos informáticos como delitos comunes? Se obtuvieron distintas respuestas, el primer encuestado señala que el error radica en el desconocimiento de cómo funcionan los sistemas, el segundo encuestado contesta N.E., el tercer encuestado, considera que solo establecen los medios empleados para cometer delitos ya conocidos, el cuarto entrevistado, considera que son delitos especiales, en el caso del quinto entrevistado, indica que a veces se le trata al delito informático como un delito común y viceversa.<br>• De nuevo advertimos que la mayoría de los encuestados tipifican los delitos informáticos como delitos de modalidad que afectan bienes jurídicos ya tutelados como el hurto o la estafa.<br>• Sin embargo nosotros planteamos que además se afecta un bien jurídico propiamente informático, una afectación a los sistemas mismos. |
| 9 | Respecto a la novena pregunta: ¿Qué podría mejorar en la ley de delitos informáticos? La mayoría de encuestados coincide en que la ley está hecha, y lo que se debe mejorar es la terminología, redacción y conceptualización, el cuarto encuestado agrega que se debe considerar organismos |

| | |
|---|---|
| | especializados para que analicen estos delitos que coadyuven a la labor Fiscal.<br>• Al respecto advertimos que la mayoría coincide en señalar que las herramientas y las políticas fiscales son insuficientes a la hora de individualizar a los autores de estos delitos.<br>• Advertimos también que aunque no está claro en sus respuestas, la mayoría prefigura la complejidad de las estructuras criminales que cometen estos delitos. |

**FICHAS BIBLIOGRÁFICA**

**01.**

| Delito informático | |
|---|---|
| Cita: | *"Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos"* (Gómez, 1992). |
| Fuente: | GÓMEZ, M. *"Los Delitos Informáticos en el Derecho Español"*, Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi. |

**02.**

| Delito informático | |
|---|---|
| Cita: | De acuerdo con Rodríguez (como se citó en Acurio, 2005), el delito informático es:<br><br>*"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".* |
| Fuente: | Acurio, S. (2016). Delitos informáticos: generalidades. |

**03.**

| Delito informático | |
|---|---|
| Cita: | Santacruz & Hermoza (2019) sostienen que en los delitos informáticos:<br><br>*"Resalta el hecho de que las personas que cometen este tipo de delitos poseen conocimientos especiales para el manejo de los sistemas informáticos que no tienen el común de los delincuentes. Es más, en algunos casos, su situación laboral les permite tener acceso a lugares donde se maneja información estratégica de carácter sensible y en otros el delito puede cometerse desde otros lugares del mundo".* |
| Fuente: | Santacruz, H. & Hermoza, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E20), 391-400. |

**04.**

| Delito informático | |
|---|---|
| Cita: | Guerrero (como se citó en la Policía Nacional del Ecuador, 2017):<br><br>*"Los delitos informáticos son actividades ilícitas, que se las comete a través de medios y dispositivos tecnológicos y de comunicación, cuyo objetivo es causar algún daño, provocar pérdidas o impedir el uso de sistemas informáticos. En los últimos tiempos, la pornografía infantil, fraudes informáticos e incluso actividades terroristas, han sido consideradas como nuevos delitos informáticos".* |
| Fuente: | Guerrero, E. (2018). *La pornografía infantil como delito informático o ciberdelito, según el artículo 103 del COIP*. |

05.

| Delito informático | |
|---|---|
| Cita: | Los delitos informáticos, según Castillo (2018) son:<br><br>*"Acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actué con o sin ánimo de lucro".* |
| Fuente: | Castillo, J. (2018). *El delito informático y su implicación en el patrimonio económico en Colombia*. |

06.

| Delito informático | |
|---|---|
| Cita: | De acuerdo con Gamba (como se citó en Téllez, 2004), los delitos informáticos son:<br><br>*"Actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico). Además, posee conductas delictivas de cuello blanco (White collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas".* |
| Fuente: | Gamba, J. (2019). El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos. |

07.

| Delito informático | |
|---|---|
| Cita: | Levet, Espinoza, Macgluf & Fragoso (como se citó en Navarro, 2005):<br><br>*"Toda conducta típica, antijurídica y dolosa que utilice como medio comisivo o como fin un sistema de procesamiento de información digital, o que involucre al mismo como instrumento de almacenamiento de pruebas".* |
| Fuente: | Levet Rivera, C. E., Espinoza Maza, J. de J., Macgluf Issasi, A., & Fragoso Teran, J. M. (2019). La inconclusa reforma al Código Penal Federal en materia de delitos informáticos. *Interconectando Saberes*, (7). https://doi.org/10.25009/is.v0i7.2628 |

08.

| Delito informático | |
|---|---|
| Cita: | Cabrera (2020), refiere que:<br><br>*"Sequeiros Calderón, Ivett en su tesis Vacíos Legales que Imposibilitan la Sanción de los Delitos Informáticos en el Nuevo Código Penal Peruano- 2015, teniendo entre otras como conclusión, que los delitos informáticos poseen una naturaleza virtual, y que el dominio en ellos se convierte en confusos por lo que complica su tipificación en la investigación de los mismos".* |
| Fuente: | Cabrera Quiroz, M. (2020). Fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el período 2010-2018. |

09.

| Delito informático | |
|---|---|
| Cita: | Morán y Morán (como se citó en Mayer, 2017).<br><br>*"Por una parte, está la tesis que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales. Consiguientemente, según este 5 planteamiento, la diferencia entre un delito informático y otros delitos sería de fondo y no meramente de forma. El corolario de esta teoría suele ser la propuesta de normas penales, incluso separadas de otras disposiciones, tendientes a la tutela autónoma de este específico interés, que vayan más allá de una mera reformulación de los tipos penales tradicionales".* |
| Fuente: | Morán, J. & Morán, R. (2020). *Delitos informáticos. reforma al artículo 190 del COIP en el contexto de la emergencia sanitaria Ecuador 2020.* |

10.

| Delito informático | |
|---|---|
| Cita: | Celli (como se citó en Sáez, 2001):<br><br>*"El delito informático: "abarca, por una parte, la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos obtenidos mediante computadoras y por otra, delitos patrimoniales por el abuso de datos procesados automáticamente".* |
| Fuente: | Celli, S. (2019). *Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388 modificación del Código Penal argentino.* |

11.

| Delito informático | |
|---|---|
| Cita: | De acuerdo con Mayer (2018):<br><br>*"Son múltiples las motivaciones que puede llegar a tener el autor de un delito informático, no obstante, en general coinciden con las motivaciones de los autores de otra clase de delitos. La doctrina destaca que la motivación de los primeros hackers fue simplemente descubrir las vulnerabilidades de un sistema informático".* |
| Fuente: | Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159-206. |

12.

| Delito informático | |
|---|---|
| Cita: | *Para González, Bermeo, Villacreses y*<br><br>*Guerrero (2018):*<br><br>*"Los delitos informáticos se han desarrollado al mismo tiempo que las tecnologías de la información, con el auge de las tecnologías, la sociedad se ha visto sumergida en un avance y desarrollo en cada una de sus áreas, donde la delincuencia también se ha visto beneficiada, ahora tienen la capacidad de cometer un acto ilegal desde cualquier lugar del mundo, con gran acceso informático, a más de la ventaja del anonimato".* |
| Fuente: | Gonzáles, J.; Bermeo, J., Villacreses, E., & Guerrero, J. (2018, July). Delitos informáticos: una revisión en Latinoamérica. In Conference Proceedings (Vol. 2, No. 2) |

13.

| Delito informático | |
|---|---|
| Cita: | De acuerdo con Acosta, Benavides y García (2020):<br><br>*"Cuando se habla de delito informático, Fuentes, Mazún y Cancino (2018) la definen como el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos. Es necesario aclarar, que este tipo de delitos suceden en el ciberespacio".* |
| Fuente: | Acosta, M.; Benavides, M. & García, Nelson Patricio (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89),351-368.[fecha de Consulta 3 de Diciembre de 2021]. ISSN: 1315-9984. |

14.

| Delito informático | |
|---|---|
| Cita: | Loreto (citado por Díaz, 2019):<br><br>*El Delito informático, es la acción dolosa que presenta un individuo, provocando un perjuicio a personas o entidades, que usan una plataforma virtual o tecnológica, que dicho acto no necesariamente conlleve a un beneficio directo o indirecto del autor del delito, y aun cuando no lleve a un perjuicio de forma grave o leve a la víctima, empleando en este 9 delito acciones habituales, que solo generan molestias de la misma, sin embargo, esta última siente que se ha vulnerado o dañado algunos de sus derechos.* |
| Fuente: | Díaz, C. (2019). La aplicación de la ley Nº. 30096-Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. |

15.

| Delito informático | |
|---|---|
| Cita: | Para Espinoza (2017):<br><br>*"Los efectos de la criminalización de los delitos informáticos pueden ser nocivos sin la contención del poder punitivo en la sociedad de control, y que las disciplinas dedicadas a la informática y una política criminal adecuada, ayudan a la prevención de los delitos informático".* |
| Fuente: | Espinoza, M. (2017). Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control. |

# CAPÍTULO V

## 5.1 CONCLUSIONES

**PRIMERA.-** Consideramos que los delitos informáticos, son delitos pluriofensivos, los bienes jurídicos tutelados en los delitos informáticos configuran una relación de afectación correlativa; en primer lugar se encuentra los sistemas de información, entendidas como bases de datos, sistemas de gestión de e-comerce, aplicativos, registros, etc. y en el segundo lugar, un conjunto bienes afectados como la indemnidad sexual, intimidad, identidad, etcétera.

Sin embargo esta relación no es una relación jerarquizada, ambos tipos de bienes jurídicos son igualmente protegidos y se sancionan las conductas tipificadas en estas modalidades delictivas, -Pharming, Cracker, Casher, etc.- Entendemos pues en ese orden de ideas que existe una afectación de un bien jurídico que podría caracterizarse como un bien colectivo de naturaleza puramente informática; que afecta no solo los sistemas informáticos, sino la percepción que tiene el colectivo social de los mismos, afecta también bienes jurídicos individuales como el patrimonio o la identidad. Finalmente concluimos que existe un legítimo interés, por parte de la sociedad, de esperar una tutela efectiva y una efectiva persecución de los delitos informáticos, más aun teniendo cuenta que el desarrollo de las actividades modernas esta signado por la virtualidad.

En nuestra investigación hemos identificado al menos dos criterios que justificarían la conceptualización de un bien jurídico colectivo propiamente informático: en primer lugar los delitos informáticos no son solamente delitos cometidos teniendo como instrumentos computadoras, sino que afectan los sistemas informáticos que contienen datos o información, esta información es constitutiva de los demás bienes jurídicos protegidos, patrimonio, identidad, etc. En segundo lugar consideramos que ayudaría a la actividad fiscal y a una mejor persecución del delito, conceptualizar los delitos informáticos como pluriofensivos, articulando así nuestra normativa con la normativa internacional y los esfuerzos supranacionales colaborativos en la persecución e identificación de los autores del delito.

**SEGUNDA.-** Consideramos que los operadores jurídicos podrían beneficiarse de una conceptualización de los delitos informáticos como delitos pluriofensivos, ya que entre los bienes jurídicos que tutelan, se encuentran bienes jurídicos colectivos, esta conceptualización, no solo los distinguiría de otros delitos que protegen bienes jurídicos similares, sino que podría

habilitar nuevas posibilidades de persecución a los sujetos y organizaciones implicadas en estos delitos. Como por ejemplo la creación de fiscalías especializadas.

**TERCERA.-** Finalmente encontramos en el desarrollo de nuestra investigación que en la mayoría de delitos informáticos, los operadores encuentran un obstáculo a la hora de formalizar las denuncias. Principalmente porque resulta muy difícil la identificación de los presuntos autores del crimen, lo que ha llevado a que los fiscales no tengan otro remedio que archivar las denuncias de este tipo.

## 5.2 RECOMENDACIONES

**PRIMERA**.- Creemos que es importante reforzar la capacitación para jueces y fiscales en temas informáticos, habilitar espacios de discusión y desarrollo de propuestas para mejorar las estrategias de persecución de los delitos informáticos.

**SEGUNDA**.- Al considerar a los delitos informáticos como delitos pluriofensivos, que tutelan un bien jurídico colectivo, se podría justificar la creación de fiscalías especializadas en persecución de estos delitos, en este orden de ideas se podría considerar algunos delitos informáticos como casos de alta complejidad, lo que permitiría ampliar los plazos de investigación.

**TERCERA**.- En el análisis de las carpetas fiscales encontramos que muchas veces se refiere la imputación de la víctima o competencia de la víctima, en relación a la diligencia mínima de protección o autocuidado. Al respecto sugerimos que debe entender la naturaleza de los delitos informáticos en todas sus dimensiones, ya que en algunos casos incluso consideran que las victimas omiten su deber de diligencia simplemente al realizar actos de comercio electrónico, o en la utilización de medios digitales como pay pal; estos medios son cada vez más cotidianos y su utilización no debería ser considerada una falta de diligencia de la víctima.

## BIBLIOGRAFÍA:


- ABANTO VASQUEZ, Manuel A. 2006 Acerca de la teoría de los bienes jurídicos. Revista Penal, N° 18, 2006. En: http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/283/2 73. recuperado el 25 de noviembre de 2021.
- ACURIO DEL PINO, S. (s.f.). oas.org/jurídico. Recuperado el 14 de setiembre de 2021, de oas.org/jurídico: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- BERAÚN SÁNCHEZ, David. 2000: "El bien jurídico en el Derecho penal", Re vista Peruana de Ciencias Penales, Nº 10, Lima.
- BRAMONT ARIAS TORRES, Luis Miguel. 2002: Manual de Derecho parte general, 2ª edic. ; Lima, EDDILI.
- BUSTOS RAMIREZ, Juan. 2004: "Bienes jurídicos colectivos", Obras completas, T. II –Control social y otros estudios; Lima, Ara Editores.
- CARO CORIA, Dino. 2002: "Sociedades de riesgo y bienes jurídicos colectivos ", Imputación objetiva, delitos sexuales y reforma penal, México, UNAM.
- CONVENIO DE CIBERDELINCUENCIA DE BUDAPEST. 2001. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- BUSTOS RAMIREZ, Juan. 1991 Manual de Derecho Penal. Parte Especial. Ariel: Barcelona. 2004 Los bienes jurídicos colectivos. En: Obras completas. Tomo II. Ara Editores: Lima. pp. 175-796.
- CANCIO MELIA, Manuel y otros. 1998 Un nuevo sistema del Derecho Penal. Grijley: Lima.
- DÍEZ RIPOLLÉS, José Luis. 1998. "La contextualización del bien jurídico prot egido en un derecho penal garantista", en AA.VV. Teorías actuales en el Derecho Pena; Buenos Aires, Ah-Hoc.
- HASSEMER, Wilfred. 1995: "Derecho Penal Simbólico y protección de Bienes Jurídicos"
- HERZOG, Félix. 1993: "Límites al control penal de los riesgos sociales". (Una perspectiva crítica ante el derecho penal en peligro), trad. de E. Larrauri, Anua io de Derecho Penal y Ciencias Penales, T. XLVI, fasc. I, Madrid, Ministerio de Justicia.

- DIMUCCIO, B. Glosario de Términos Informáticos. Aragua - Venezuela: Ministerio de Educación. Obtenido de https://es.slideshare.net/giovainina/glosario-informatico-pdf
- DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA. (s.f.). Recuperado el 28 de octubre de 2021, de http://190.117.81.252/files/criminalistica/delito.pdf
- GALVES VILLEGA, Tomas Aladino 2012 Derecho Penal. Parte Especial. Tomo II. Juristas editores: Lima.
- HERNÁNDEZ MENDOZA, F. 2003. Apuntes para la Asignatura Informática I. Ciudad de México: Fondo Editorial F.C.A.
- MAYO CALDERÓN, Belén. 2005 Derecho Penal y Tutela de bienes jurídicos colectivos. Revista Peruana de Ciencias Penales. N° 17.
- MAYO CALDERÓN, Belén. 2017 La tutela de un bien jurídico colectivo por el delito societario de administración fraudulenta. Estudio del artículo 295° del Código Penal español y propuesta de lege ferenda. Comares: Granada.
- MOISÉS BARRIOS, A. 2017. Ciberdelitos Amenazas Criminales del Ciberespacio. Madrid: REUS.
- OXMAN, N. 2013. Estafa Informática a través de Internet: Acerca de la imputación del "Phishing" y el "Pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 211-262.
- PEÑA CABRERA FREYRE, A. R. 2011. Derecho Penal - Parte Especial (3° ed., Vol. II). Lima: Idemsa.
- PEÑA-CABRERA FREYRE, A. R. 2011. Derecho Penal - Parte Especial. Lima: Idemsa.
- RESOLUCIÓN LEGISLATIVA N° 30913. (12 de Febrero de 2019). Resolución Legislativa que aprueba el Convenio sobre Ciberdelincuencia.
- SCHUNEMANN, Bernd. 2007 ¡El derecho Penal es la última ratio para la protección de bienes jurídicos! Bogotá. Universidad externado de Colombia.
- SOTO NAVARRO, Susana. 2003 La protección penal de los bienes colectivos en la sociedad moderna. Comares: Granada.
- VILLAVICENCIO TERREROS, F. 2014. Delitos Informáticos. IUS ET VERITAS.
- VILLAVICENCIO TERREROS, F. 2014. Delitos Informáticos. IUS ET VERITAS.

## ANEXOS

## GUÍA DE ANÁLISIS DE CARPETAS FISCALES

OBJETIVO: Analizar qué criterios justifican que los delitos informáticos tutelan un bien jurídico colectivo, propiamente informático.

| | |
|---|---|
| Número de carpeta: | |
| Materia: | |
| Delito: | |
| Bien jurídico | |
| I. Fundamentos | |
| II. Análisis | |
| III. Conclusiones | |

## GUÍA DE ENTREVISTA

OBJETIVO 1: De qué manera abordan la tutela de bienes jurídicos colectivos, en la tipificación de los delitos informáticos.

| | |
|---|---|
| **Fecha** | |
| **Entrevistado** | |
| **Cargo** | |
| **Institución** | |

Preguntas:

| | |
|---|---|
| **1. ¿Considera que existe un bien jurídico específico en los delitos informáticos?** | |
| **2. ¿Considera usted que los bienes tutelados en los delitos informáticos son pluriofensivos?** | |
| **3. ¿Por qué cree que los delitos informáticos tutelan un bien jurídico colectivo?** | |
| **4. ¿Considera que la ley de delitos informáticos es una herramienta efectiva?, ¿por qué?** | |
| **5. ¿Cómo considera que los operadores de justicia deberían tipificar los delitos informáticos?** | |

OBJETIVO 2: Identificar las deficiencias en la persecución de los delitos informáticos.

| | |
|---|---|
| **6. ¿Considera que en los delitos informáticos los jueces y fiscales realizan un adecuado tratamiento de los delitos informáticos?** | |
| **7. ¿Según su criterio, los delitos informáticos van más allá de la afectación de bienes jurídicos ya protegidos?** | |
| **8. ¿Considera Ud. que muchas veces se comente el error de** | |

| | |
|---|---|
| **tratar los delitos informáticos como delitos comunes?** | |
| **9. ¿Qué podría mejorar en la ley de delitos informáticos?** | |