



Universidad
Inca Garcilaso de la Vega

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

TESIS

Mecanismos jurídicos para implementar la Ley 30096 en los
Delitos Informáticos contra el patrimonio frente a las nuevas
Tecnologías Informáticas.

PARA OBTENER EL TÍTULO PROFESIONAL

DE

ABOGADO

AUTOR

Giacommo Darío Vitteri Melgar

ASESOR

Karina bardales Becerra

2022

DEDICATORIA

Dedico este trabajo con todo mi corazón a mi madre, dado que sin ella no lo hubiese logrado. Tu bendición a diario a lo largo de mi vida me protege y me lleva por el camino del bien. Por eso te doy mi trabajo en ofrenda por tu paciencia y amor madre te amo.

AGRADECIMIENTO

Al curso de taller de tesis de la Universidad Inca Garcilaso De la Vega por brindarme la oportunidad de realizar mis estudios de investigación, y a mis compañeros de estudios por estar en todo momento recibiendo los conocimientos, a mi asesora por darme los conocimientos para culminar con este trabajo, y a los jurados examinadores de la tesis.

LISTA DE TABLAS

pág.

Tabla 1

Cuadro N° 1: “avance tecnológico informático y las nuevas modalidades de comisión de delitos informáticos” 74

Tabla 2

Cuadro N° 2 “la Legislación sobre los Delitos informáticos es de efectiva para sancionar las nuevas modalidades delictivos con el uso de la nueva tecnología”... 74

Tabla 3

Cuadro N° 3: “las empresas privadas o públicas están expuestas a ser víctimas de fraude informático”... 75

Tabla 4

Cuadro N° 4: “regulación legislativa para prevenir los delitos informáticos contra el patrimonio”... 75

Tabla 5

Cuadro N° 5: “fiscalía especializada en delitos informáticos para todas las regiones de nuestro país para lograr una efectividad en la aplicación de los delitos informáticos- Ley N° 30096 Ley de delitos informáticos”... 75

Tabla 6

Cuadro N° 6: “identificar al autor de la comisión de un delito informático”... 76

Tabla 7

Cuadro N° 7 “Considera usted que es de suma importancia tocar este tema más si estamos pasando este momento en nuestra sociedad con la evolución de la tecnología” 76

LISTA DE FIGURA

	pág.
Figura No 1	
Características del delito	11
Figura No 2	
Elementos Importantes del Delito	12
Figura No 3	
La Antijuricidad.....	15
Figura No 4	
Denuncias recibidas en la DIVINDAT	23
Figura No 5	
Evolución de denuncias semestrales por delitos informáticos... ..	24

RESUMEN

La presente investigación tiene como finalidad determinar los mecanismos jurídicos para implementar en la Ley No 30096 de delitos informáticos contra el patrimonio frente a las nuevas modalidades que existen hoy en día. Como fuente principal la creación de una fiscalía especializada en este delito, así también, en las demás modalidades que existen en nuestro ordenamiento y las que van surgiendo día a día, toda vez que genera una inseguridad jurídica en nuestra justicia y de tal modo que es ineficaz para poder demostrar la autoría o participación en una etapa preliminar, por lo que no se logra una efectiva sanción en este tipo penal.

En esta investigación se logró efectuar y aplicar el método inductivo, porque propondremos nuevos instrumentos necesarios para combatir la ciberdelincuencia que ocurre en este momento con mayor frecuencia.

Así mismo esta investigación busca como objetivo general determinar los mecanismos jurídicos para implementar la Ley N° 30096 de Delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas.

Con esta investigación se propone la creación de una fiscalía especializada en delitos informáticos para combatir la ciberdelincuencia que viene evolucionando de una manera constante en nuestra sociedad y en el mundo.

Palabras claves: Delito informático, ordenamiento jurídico, nuevas tecnologías, etapa preliminar

ABSTRACT

The purpose of this research is to determine the legal mechanisms to be implemented in Law No. 30096 on computer crimes against patrimony in the face of the new modalities that exist today. As main source the creation of a specialized prosecutor's office in this crime, as well as in the other modalities that exist in our system and those that are emerging day by day, since it generates a legal insecurity in our justice and in such a way that it is ineffective to be able to demonstrate the authorship or participation in a preliminary stage, so an effective sanction in this criminal type is not achieved.

In this research it was possible to carry out and apply the inductive method, because we will propose new instruments necessary to combat cybercrime that occurs more frequently at this time.

Likewise, this research seeks as a general objective to determine the legal mechanisms to implement the law 30096 in computer crimes against patrimony in the face of new computer technologies.

This research proposes the creation of a specialized prosecutor's office in computer crimes to combat cybercrime that is constantly evolving in our society and in the world.

Key words: Computer crime, legal system, new technologies, preliminary stage.

INTRODUCCIÓN

El delito informático es un problema que viene sucediendo en distintos países del mundo, siendo esta acción atípica generada por una persona a través de las plataformas del internet, es decir un espacio digitalmente hablando, toda vez que este tipo penal se origina por avance tecnológico de nuestra época conforme viene evolucionando esta ventana virtual, es por eso que en la actualidad ha generado que los delincuentes amplíen su campo de acción amedrentando con la seguridad de las personas, bajo ese mismo concepto, se puede reflejar que en países como España donde se ha regulado este tipo de delito, y se puede advertir que no solo le basto la mera implementación de la norma, sino que también ellos se han visto necesarios implementar mecanismos o medidas, para la correcta aplicación de la misma norma generada, llegando así a controlar el avance de este delito conforme a su evolución en su sociedad, de tal manera que tiene mucha relación con la investigación que se ha desarrollado en esta ocasión.

En tal efecto hemos desarrollado 6 capítulos a saber:

Capítulo I: Fundamentos Teóricos de la Investigación: Desarrolla las principales teorías en las se soporta la presente tesis y adicionalmente las investigaciones a través de la que consignamos tesis previas que han tocado en alguna magnitud el tema de nuestra investigación dándole un efecto enriquecedor. De igual manera establecemos el Marco Conceptual en el que se describen los elementos principales para la presente tesis y finaliza con el Marco Histórico en donde de manera sucinta explica la evolución del problema;

Capítulo II: El Problema, Objetivos, Hipótesis y Variables: de manera precisa plantea el problema y la descripción de su realidad con antecedentes teóricos y la definición del mismo. Continúa con una clara descripción de la finalidad y los objetivos de la presente investigación, formulando el objetivo general y los objetivos específicos, a través de los cuales se sustentará las conclusiones. También establece los factores de la delimitación del estudio, las justificaciones teóricas, prácticas y sociales que

han llevado al desarrollo de la tesis. Los supuestos teóricos, hipótesis y especificaciones, identificando sus variables independiente y dependiente.

Capítulo III: Método, Técnica e Instrumentos: Hace una descripción de los métodos generales y los específicos aplicados en su desarrollo sumándole el enfoque y diseño dados. Técnica e instrumento de recolección de datos.

Capítulo IV: Presentación y Análisis de los Resultados: La investigación hace la presentación de resultados, con la contratación de la hipótesis y finaliza con la discusión de sus resultados; Capítulo V: Conclusión y Recomendaciones: Las conclusiones se llevan a cabo basadas en su hipótesis, objetivos de la investigación, en el análisis e interpretación de los puntos tratados en capítulos previos; Capítulo VI: Iniciativa Legislativa: La investigación culmina con el desarrollo del respectivo Proyecto Legislativo

ABREVIATURAS

CPP	:	CONSTITUCIÓN POLÍTICA DEL PERÚ
DL	:	DECRETO LEGISLATIVO
CP	:	CÓDIGO PENAL
PL	:	PROYECTO DE LEY
MP	:	MINISTERIO PÚBLICO
UFEC:		UNIDAD FISCAL ESPECIALIZADA CIBERDELINCUENCIA
PNP	:	POLICÍA NACIONAL DEL PERÚ

ÍNDICE GENERAL

AGRADECIMIENTO	2
LISTA DE TABLAS.....	3
LISTA DE FIGURA	4
RESUMEN	1
ABSTRACT	2
INTRODUCCIÓN	3
ABREVIATURAS.....	5
ÍNDICE GENERAL.....	6
1.1 Marco Teórico	10
1.1.1 Teoría del delito.....	10
1.1.2 Teoría de la tipicidad	13
1.1.3 Teoría de la Antijuricidad	14
1.1.4 Teoría de la información ante las nuevas tecnologías de la comunicación.....	15
1.2 Investigaciones	17
1.3 Marco conceptual.....	19
1.3.1 Mecanismos jurídicos.....	19
1.3.2 Implementar.....	19
1.3.3 Delitos informáticos	19
1.3.4 El patrimonio	20
1.3.5 Nuevas tecnologías informáticas	20
1.4 Marco histórico	21
1.4.1 La Ciberdelincuencia en el Mundo	21
1.4.2 La evolución de los delitos informáticos en el Perú	22
1.5 Marco Jurídico	24
1.5.1 Ley N° 30096 Ley de Delitos Informáticos artículo 8.....	24
1.5.2 Convenio de Budapest.....	25
1.5.3 Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público.....	26
1.5.4 Constitución política del Perú	26
1.6. Sentencia del Tribunal Constitucional, EXP. N.º 1189-2019-PHC/TC	27
CAPÍTULO II.....	30
2.1 Planteamiento del Problema.....	30

2.1.1	Descripción de la Realidad Problemática	30
2.1.2	Antecedentes teóricos	31
2.1.2	Formulación del problema	33
2.2	Finalidad y Objetivos de la investigación.....	33
2.2.1	Finalidad	34
2.2.2	Objetivo general y específico	34
2.2.3	Delimitación del estudio.....	34
2.2.4	Justificación e importancia del estudio	35
2.3	Hipótesis y variables.....	36
2.3.1	Hipótesis General	36
2.3.2	Variables e indicadores	36
CAPITULO III.....		37
3.1	Población y Muestra.....	37
3.1.1	Población	37
3.1.2	Muestra	37
3.2	Diseño a utilizar en el estudio	37
3.2.1	El tipo de investigación.....	37
3.2.2	Métodos aplicables a la presente investigación.....	37
3.2.2.1	Métodos generales	37
3.2.2.1.1	Método deductivo.....	37
3.2.2.1.2	Método inductivo	38
3.2.2.1.3	Método analítico.....	39
3.2.2.2	Métodos específicos.....	39
3.2.2.2.1	Método dogmático	39
3.2.2.2.2	Método hermenéutico	40
3.2.2.2.3	Método exegético.....	40
3.2.3	Enfoque de la investigación.....	41
3.2.4	Diseño.....	41
3.3	Las técnicas e instrumentos de recolección de datos	41
3.3.1	Técnicas	41
3.3.1.1	Observación documental	41
3.3.1.2	Entrevista	41

3.3.2	Instrumentos de recolección de datos	42
3.3.2.1	Ficha de observación documental	42
3.3.2.2	Guía de entrevista	42
3.4	Procesamiento de Datos	43
CAPITULO IV		44
4.1	Presentación de resultados	44
4.1.1	Las nuevas tecnologías informáticas frente a los delitos contra el patrimonio	44
4.1.2	La regulación de los Delitos informáticos en el derecho comparado.....	46
4.1.3	Causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos de los operadores de justicia peruano.....	53
4.1.4	El procedimiento fiscal y judicial que se adopta en los delitos informáticos contra el patrimonio.....	54
4.1.5	Posturas de los Fiscales y sus asistentes, abogados, secretarios del poder judicial y efectivos policiales respecto de que a los delitos informáticos con relación hacia el avance tecnológico	56
4.2	Contrastación de Hipótesis.....	62
4.3	Discusión de resultados.....	63
CAPÍTULO V		67
5.1	Conclusiones.....	67
5.2	Recomendaciones	68
5.2.1	Deberían especializar a los efectivos policiales con un centro donde constantemente los capaciten sobre las nuevas tecnologías.....	68
5.2.2	Crear un centro de orientación sobre el avance tecnológico y desarrollarlo en las escuelas, centro de trabajos públicos o privados.....	68
CAPÍTULO VI		69
6.1	Proyecto de Ley	69
BIBLIOGRAFÍA.....		72
ANEXOS		74
Anexo 1.....		74
Anexo 2.....		75
B) Anexo 3.....		78

CAPÍTULO I

FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN

1.1 Marco Teórico

En esta parte de la presente investigación se dará desarrollo a teorías, conceptos y aspectos teóricos relevantes respecto al tratamiento jurídico penal de los delitos informáticos, así como en forma especial, en lo relativo al fraude informático. De la invención de la computadora y su posteriormente la implementación de las redes informáticas, internet y otros sistemas informáticos, el derecho se vio en la obligatoriedad a regular aspectos vinculados a la informática aunque en forma retrasada; sin embargo, lo es también la necesidad de regular en el ámbito penal debido a que las conductas ahí desarrolladas se constituyen intolerables por la sociedad, es así como nace el derecho informático y específicamente el derecho penal informático, dada la necesidad de sancionar conductas que afectan bienes jurídicos penalmente relevantes.

1.1.1 Teoría del delito

La teoría del delito es una herramienta de trabajo que permite organizar y explicar la investigación, con el fin de identificar y asegurar los medios cognoscitivos necesarios para demostrar, más allá de duda razonable, la ocurrencia del delito y su autor o participe.

También debe entenderse como un instrumento para proyectar la actividad investigativa, utilizado por el equipo integrado por el fiscal y la policía. Se constituye en un instrumento de superior importancia para facilitar el trabajo de investigación, para organizar, proyectar, planear, controlar y verificar resultados, esto con el fin de optimizar la actividad de recolección de la evidencia y que de esta manera permita demostrar la existencia de la conducta constituida de delito y quienes fueron los autores.

(Muñoz, 2004) afirma que, “La teoría del delito se ocupa de las características comunes que debe tener cualquier hecho para ser

considerado delito, sea este en el caso concreto una estafa, un homicidio o una malversación de caudales públicos” (p.1). La tendencia que se acaba de señalar es una de carácter personal puesto que estudia lógicamente las conductas que se ha realizado por el autor del delito.

1.1.1.1 Características de la teoría del delito

En el siguiente diagrama podemos ubicar las siguientes características de la teoría del delito dentro del panorama de la ciencia penal:

Figura 1

Las características de la teoría del delito

CARACTERÍSTICAS DE LA TEORÍA DEL DELITO	
• Es un sistema	Representa un conjunto ordenado de conocimientos.
• Son hipótesis	Son enunciados que pueden probarse, atestiguar-se o confirmarse solo indirectamente, a través de sus consecuencias.
• Posee tendencia dogmática	Al ser parte de una ciencia social, no existe unidad respecto de la postura con que debe abordarse el fenómeno del delito, por lo que existe más de un sistema que trata de explicarlo.
• Consecuencia jurídico-penal	El objeto de estudio de la teoría del delito es todo aquello que da lugar a la aplicación de una pena o medida de seguridad.

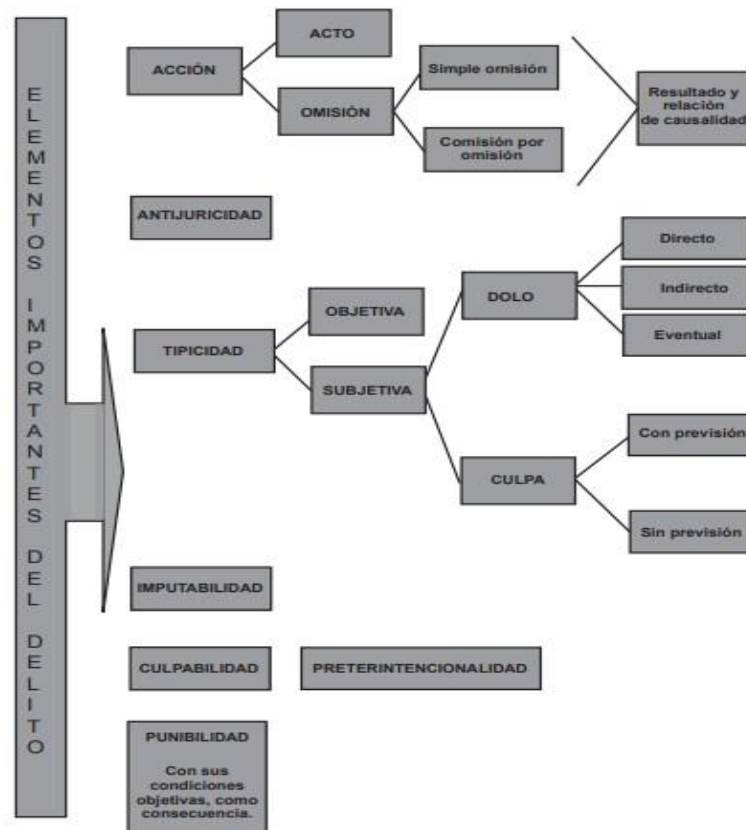
Nota: Extraído de (Almanza, Teoria del Delito, 2010, pág. 20)

1.1.1.2 Elementos importantes del delito

Los elementos del delito son de suma relevancia en el derecho de penal es así que (Almanza, 2010) señala que los elementos del delito son “La acción o conducta, tipicidad, antijurídica y culpabilidad (aunque también algunos autores agregan a lo anterior, la punibilidad). No obstante, aunque hay un cierto acuerdo respecto de tal definición, no todos le atribuyen el mismo contenido” (p.59). Comparto la opinión del autor ya que hay muchos conceptos básicos acerca de los elementos del delito, sin embargo, en la actualidad es el más usado por los juristas.

Figura 2

Elementos importantes del delito



Nota: (Almanza, Teoría del Delito, 2010, pág. 61)

1.1.2 Teoría de la tipicidad

La teoría de la tipicidad se podría definir como un comportamiento humano propiamente dicho cuya característica principal es que la conducta que se está realizando debe estar plasmada en un tipo penal, como por ejemplo el delito informático.

Señala (Ticona):

Es el resultado de la verificación de si la conducta y lo descrito en el tipo, coinciden. A este proceso de verificación se denomina juicio de tipicidad, que es un proceso de imputación donde el intérprete, tomando como base al bien jurídico protegido, va a establecer si un determinado hecho puede ser atribuido a lo contenido en el tipo penal (Ticona, 2012, pág. 1)

Así mismo el autor señala que la tipicidad cuenta con dos elementos objetivos y subjetivos para describir el delito.

En los elementos objetivos contamos con la descripción de la norma que es aquella que le va dar validez jurídica para describir las conductas que están prohibidas.

De tal forma se tiene los elementos subjetivos que se subdivide en el dolo y culpa. El dolo tiene por recabarse en el conocimiento y voluntad de la persona humana. Así mismo el individuo debe tener total conocimiento de que la conducta a realizar está prohibida. La voluntad de una persona tiene que estar acorde que la realización es, valga la redundancia, propiamente realizada sin ninguna exigencia de un tercero.

Si hablamos de dolo es factible mencionar al tesista Arellano que señala que el "dolo es la conciencia de querer y la conciencia de obrar, traducidas estas en una conducta externa, es decir, es la voluntad

consciente, encaminada u orientada a la perpetración de un acto que la ley prevé como delito” (Arellano, 2011, pág. 1). Como señala este último, el dolo es muy importante para que se configure la tipicidad al haber una realización de actos que estén en contra del derecho.

1.1.3 Teoría de la Antijuricidad

(Plascencia), quien menciona sobre la antijuricidad:

Se refiere a la contradicción del orden público a través de una acción, lo cual solo es admisible desde una perspectiva semántica o gramatical pues técnicamente la antijuridicidad contiene aspectos tanto formal, material como valorativos. Lo formal es la atención al ataque o contravención a lo dispuesto en la ley, en tanto lo material se enfoca a la lesión o puesta en peligro del bien jurídico protegido en la ley penal (Plascencia, 2004, pág. 132)

Lo que refiere el autor es que la antijuricidad es una acción en contra de lo dispuesto en una norma jurídica y que la acción es tiene por objetivo lesionar un bien jurídico, pero intencionalmente posible,

Por su parte, (Bacigapuldo) señala que:

El comportamiento de todo hombre puede producir efectos lesivos de bienes jurídicos lejanos que se sustraen a la dirección causal del agente, que no se pueden evitar ni con la mejor buena voluntad, ni poniendo extraordinario cuidado, la lesión del bien jurídico no puede ser todavía considerada como antijurídica, puesto que el juicio de antijuricidad expresa siempre la

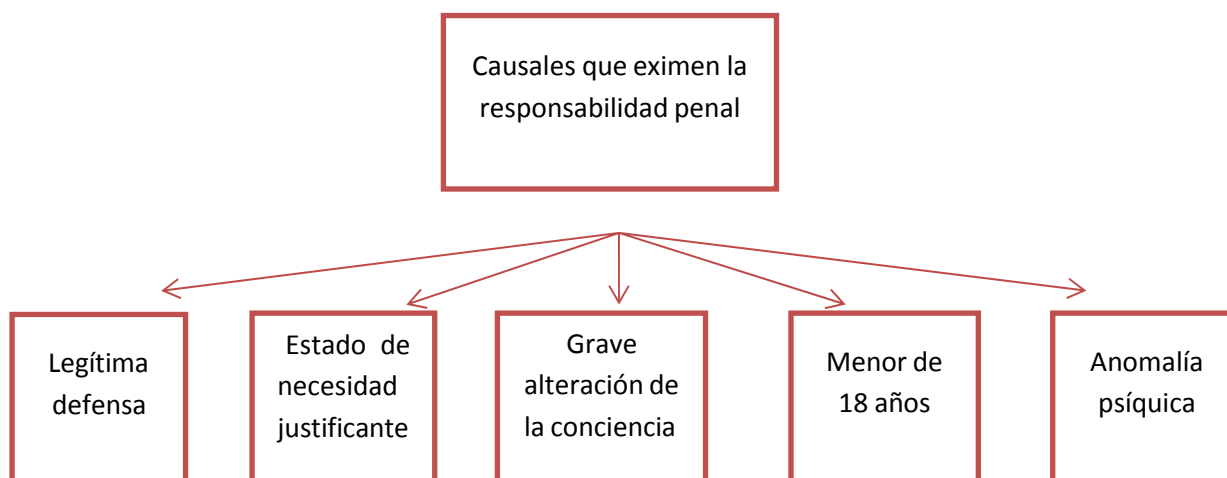
desaprobación de una acción en relación a la conducta jurídicamente mandada (Bacigapuldo, 1979, pág. 18)

El autor hace referencia que la conducta tiene que producir obligatoriamente una lesión al bien jurídico de una persona sin embargo debe existir una conectividad con la intención del autor de no reflejar daños.

De igual forma en el derecho penal peruano se mide a través de algunas causales que eximen la responsabilidad penal como, por ejemplo:

Figura 3

Causales que eximen la responsabilidad penal



Nota: Elaboración Propia

1.1.4 Teoría de la información ante las nuevas tecnologías de la comunicación

La Teoría de la Información es una disciplina que se basa en el análisis de la de las tecnologías y su relación con la informática se define “su objetivo fundamental es orientar y situar el conocimiento en torno a la comunicación, con una dirección concreta específica para investigar la información” (Aladro, 2011). Lo que tenemos aquí es una aclaración detallada de que esta herramienta busca investigar la información que se está recabando. No obstante, se tiene que orientar con ciertos fundamentos para que, de esta manera se pueda llegar a concretar su objetivo principal.

(Aladro) Afirma lo siguiente

Los expertos en Teoría Social de la información distinguen claramente el mundo social generado por las nuevas tecnologías digitales, de los mundos sociales no mediados por estas tecnologías. Así denominan “mundo para social” a esta esfera de relaciones autónomas respecto al contacto social primario o respecto a la comunicación masiva mediada, en las que nuevas formas, rituales, perspectivas de la comunicación, se están produciendo de modo vertiginoso (Aladro, 2011, pág. 91)

En el mismo sentido, sostiene que:

La recepción en la comunicación digital es una inmersión intensa en un mundo que en mucha medida es un espejo de la identidad intrapersonal y sus flujos de actividad, incorporando a la actividad de recepción comunicativa la entrada en las formas imaginarias más dúctiles y oníricas posibles (Ídem, 2011, pág.91)

Esta teoría puede ser vista desde dos formas, la primera, como aquella en que la información ha sido tomada como un medio negativo para canalizar una serie de comportamientos y/o conductas destinadas a lograr la obtención de determinados datos, y de otro lado aquel mecanismo para acceder a un conocimiento establecido, algo que se debe de tener en cuenta es que se debe diferenciar aquella información de carácter privado y privado como

criterio, para determinar si estamos ante un delito informático o no. Es por eso que con justa razón se indica que, “la teoría de la información busca absorber conocimientos del campo cognitivo y psicológico, y en otro, las metodologías de análisis del mensaje abrieron la disciplina al análisis cultural más amplio” (Valbuena, 1997, pág. 21). Esta determinada teoría extrae conocimientos de carácter psicológico para entender de qué manera se desarrolla en el campo tecnológico y sus efectos.

1.2 Investigaciones

Atendiendo a lo novedoso del tema, ha sido necesario recurrir a la búsqueda de aquellos trabajos de investigación que guardan relación con el tema, en ese sentido se ha realizado la búsqueda de tesis a nivel internacional, conforme se detallan a continuación:

Alejo Pardo Vargas, realizó la tesis titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima”, quien arriba a la siguiente conclusión:

1. El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de fraude es deficiente, puesto que dentro de esta modalidad directiva se ha comprendido todas las modalidades de delitos informáticos contra el patrimonio, y al ser este tipo penal muy abierto y ambiguo no permite la efectiva sanción de los delitos informáticos contra el patrimonio.
2. El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de sabotaje informático es deficiente, puesto que, pese a que en la vigente legislación se sanciona la destrucción de datos, no se regula en forma clara y expresa la afectación al patrimonio por medio sistemas informáticos, con o sin fines lucrativos, el cual genera impunidad de los actos de sabotaje informático contra las empresas o personas para reducir su competitividad.

3. El tratamiento jurídico penal de los delitos informáticos contra el patrimonio en su modalidad de estafa es deficiente, toda vez que la legislación peruana no regula expresamente este ilícito penal, por lo que, al no cumplirse con el principio de tipicidad, dificulta la investigación y sanción de los delitos informáticos contra el patrimonio en su modalidad de estafa. (Pardo Vargas, 2018, pág. 122)

Asimismo, se tiene la tesis presentada por el alumno Montoya Guillén, Franklin Abraham titulada “Regulación expresa del delito informático de clonación de tarjetas – Sede DIVINDAT, 2017”, dicho autor arriba a las siguientes conclusiones:

1. Se concluye que el delito de clonación de tarjetas no está claramente tipificado y definido en la actual Ley de Delitos Informáticos N° 30096, motivo por el cual la ley actual es insuficiente frente a las nuevas modalidades que se presentan, ya que si bien tenemos el Art. 8 sobre fraude informático no cumple con la protección adecuada. Asimismo, en nuestro país existe una confusión e incertidumbre jurídica, dado que al no tener una regulación expresa no es posible una correcta aplicación, motivo por el cual se requiere que la ley especial sea actualizada.
2. Se concluye que surge la necesidad de establecer un tipo penal propio para garantizar la protección legal respecto al delito de clonación de tarjetas, además de poder perseguir el delito de forma directa teniendo ejemplos la legislación comparada; los países que regulan de manera específica son México, España y Venezuela que contrastan con la regulación aplicada en el Perú. Asimismo, se puede mejorar añadiendo protección legal a todas las tarjetas que sirvan como medio de pagos.

3. Se concluye que los presupuestos regulados en la Ley N° 30096 se pueden aplicar, pero resultan insuficientes con relación al derecho comparado, debido a que se encuentra configurados específicamente con relación al delito de clonación de tarjetas, mientras que en el Perú solo tenemos la regulación en base al fraude informático evidenciando la necesidad de una regulación actualizada (Montoya, 2018, pág. 89)

1.3 Marco conceptual

1.3.1 Mecanismos jurídicos

Entendido como “el conjunto de acciones que facilitan la relación ciudadana y administración pública” (Helen, 2013, pág. 3). Se puede apreciar en este concepto que los mecanismos jurídicos pueden ser descritos como aquellas formas de relacionarse entre sí y también con la administración pública de la sociedad.

1.3.2 Implementar

El termino implementar puede describirse como "el cambio dirigido que sigue al mandato de una política, el proceso de reordenar patrones de conducta según el conjunto de prescripciones derivadas de una decisión” (Rivera, 1995, pág. 4). Es una modificación a través de un acuerdo o mandato recibido por una política dada en una organización.

1.3.3 Delitos informáticos

Señala (Acurio, 2007) sobre el delito informático.

Define al Delito informático como, 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. (pág. 10)

Para el autor Son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.

1.3.4 El patrimonio

Para el tesista, es entendido como el conjunto de bienes y obligaciones de una persona, considerado como una universalidad de derecho, es decir, como una masa móvil, cuyo activo y pasivo no pueden disociarse. Lo expuesto se respalda con define patrimonio como “el conjunto de bienes, créditos (activo) y obligaciones o deudas (pasivo) que tiene un sujeto. En términos más simples, el patrimonio es el conjunto de derechos patrimoniales y obligaciones atribuibles a un sujeto” (Torres, 2021, pág. 35), se entiende esta como atribuciones de ciertos valores específicos que tenemos todas las personas en nuestra propiedad intelectual y física.

1.3.5 Nuevas tecnologías informáticas

Se basa en el estudio, el desarrollo y la práctica de los sistemas informáticos, especialmente en lo que se refiere al uso del software y el hardware. Es por ello que se podría definir brevemente su actividad dentro del mundo de las computadoras.

Además, se podría decir también que la tecnología informática se ocupa de todos los procesos y los medios requeridos para tratar la información.

1.4 Marco histórico

1.4.1 La Ciberdelincuencia en el Mundo

Desde de la década de los 70 los países empezaron a sentir una propagación de ciertos crímenes que estaban al acecho de quienes usaban un sistema operativo. Tales como son aquellos que manipulaban las redes telefónicas, pero que, en ese tiempo se conocían como los “telégrafos”, los cuales eran tecnologías encargadas de transmitir datos, posteriormente fue cambiando hacia los teléfonos que trasmitían la comunicación de información a través de las voces. Así mismo los famosos delincuentes usaban manipuladores telefónicos para controlar el sistema y usar estos aparatos para hacer llamadas a larga distancia totalmente gratis.

En la época de los 80, aparecieron las computadoras personales (PC) que fue producto de la ciencia tecnológica, es aquí donde surge los famosos virus, que eran en términos sencillos, un programa que robaba toda la información almacenada en el equipo. Tras esto, se fue originando un problema complejo, ya que, los sistemas privados como por ejemplo los bancos eran el punto blanco para poder cometer estos ilícitos. Así mismo, simultáneamente se fueron dando los fraudes informáticos, en la que los usuarios, a través de los correos electrónicos se comunicaban con el estafador, existían diversos mecanismos empleados por estos malhechores, cuyo propósito era recibir un abono de sumas exorbitantes de parte de la persona estafada.

En la época de los 90 donde el avance tecnológico se fue desarrollando y cambiando ciertas tecnologías que no eran eficaces y remplazándose por otras, o quizás mejorándolas. Es aquí donde se desarrolla los servidores web, donde cualquier persona con una cuenta real o falsa, era libre de acceder. Este fue el punto clave, donde se volvió preocupante para la sociedad y para los estados, ya que gracias a esto se produjo de manera

constante la comisión de hechos delictivos e ilegales producto de las interacciones que se daba persona a persona por medio de estas redes sociales.

Algunos autores señalan que en el año 2000 fue donde se produjo el origen de los delitos cibernéticos al contener que las redes sociales cobraron vida con la serie en las que detallabas el perfil único de una persona y la información personal. También empezaron los hackeos de la información personal, a través de un virus que por casualidad uno había accedido por ingresar alguna página indebida o cliquear en algún sitio web poco fiable. A través de estos hackeos también podían vaciar cuentas bancarias a través de la clonación de tarjetas de crédito, robar información confidencial de los estados, etc.

En la actualidad podemos decir que aún siguen existiendo estos tipos de ciberdelitos, pero como se dijo anteriormente el mundo está en constante evolución y usuarios mayormente están dejando de lado las computadoras y cambiando por aplicativos que contienen los celulares.

1.4.2 La evolución de los delitos informáticos en el Perú

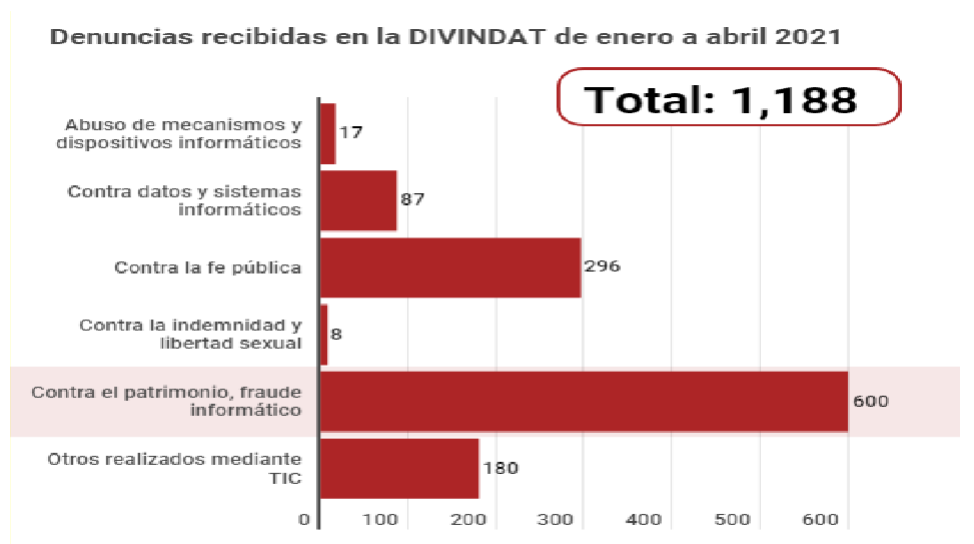
Según el diario (Peruano E.)Señala lo siguiente:

Entre enero y abril del 2021, se investigaron 1,188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía. Los casos más frecuentes están relacionados al fraude informático y a la suplantación de identidad. A través del phishing, los ciberdelincuentes engañan a los usuarios con páginas falsas que simulan ser los sitios web de los bancos o entidades financieras. Las víctimas registran sus datos personales y, con esa información, las organizaciones criminales realizan depósitos sin autorización. Además, los ciberdelincuentes ofrecen productos a muy bajos precios en Facebook y WhatsApp. Los usuarios son

engañados para realizar los pagos y luego los perfiles de los vendedores son desactivados. (Peruano", 2021, pág. 1)

Figura N°5

Denuncias recibidas en la DIVINDAT de enero a abril del 2021



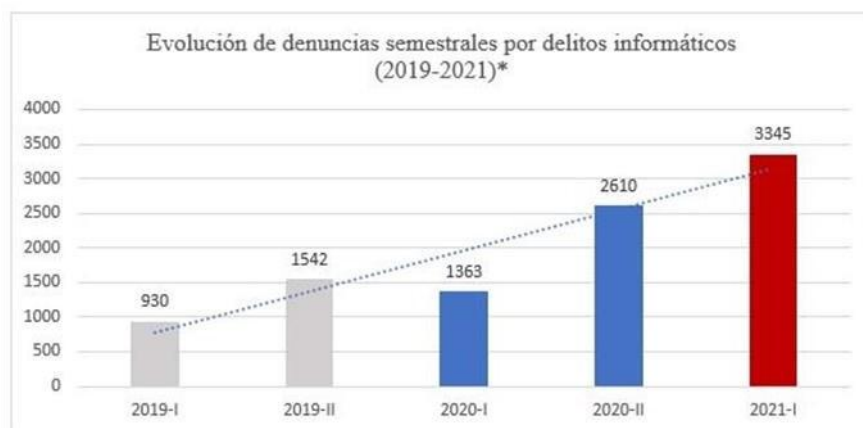
Nota: Extraído del Diario Oficial el peruano, junio, 2021

Como se puede apreciar en la imagen podemos notar la gran diferencia que existe hoy en día de que el delito que más se comete es contra el fraude informático que a la fecha aún sigue aumentando de forma muy numerativa.

Si hablamos desde que empezó la pandemia hasta el año pasado tenemos una imagen donde la policía nacional detalla como es el incremento de estas denuncias presentadas por las personas y como fue variando el numero con respecto a tiempos de covid-19, en el cual muchas de las personas acuden a estos sistemas informáticos como un sistema factible para el desarrollo de su vida y seguridad de su salud. Esto genera para muchos el menor contagio de la enfermedad que actualmente viene apareciendo en distintas partes del país. Pero que el mayor problema es el utilizar estos dispositivos como una herramienta ligeramente hablando que puedes registrar cualquier dato que pueda generar un objetivo para los delincuentes.

Figura N° 6

Evolución de denuncias semestrales por delitos informáticos (2019-2021)



Nota: extraído de la página web Institución de defensa legal, 21 de septiembre, del 2021, s/n, fuente PNP-DIRTIC-SECEJE-2021)

Hoy en día existen estas modalidades que todavía no tiene una solución posible y necesaria para las personas, dado es que en el Perú no existe un ente autónomo especializado que persiga estos delitos con mayor frecuencia, cautela y seguridad. Toda vez que se sigue propagando en todo el país y se vuelve incontrolable para la sociedad y el mundo.

1.5 Marco Jurídico

1.5.1 Ley N° 30096 Ley de Delitos Informáticos artículo 8.

El dispositivo legal denominado Ley de Delitos Informático, contiene en el artículo 8 la definición legal de que es el fraude informático que nos detalla (El peruano):

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. (El peruano, 2013, pág. 2)

1.5.2 Convenio de Budapest

El convenio de Budapest se creó en el 23 de noviembre del año 2001 y entro en vigor en el año 2004 el 1 de julio. Este convenio fue creado por el consejo de Europa, con la participación de los estados con el fin de luchar contra comisión de delitos informáticos que se estaban propagando en estos mismos.

El convenio (Budapest) señala lo siguiente:

Convencidos de que el presente convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas de redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detención, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable

Como ya lo señalamos anteriormente el estado peruano es uno de los integrantes de este convenio, pero que todavía en esta en tela de juicio su eficaz colaboración con nuestro estado, toda vez que en la sociedad se sigue practicando muchas de las modalidades

establecidas por la ley 30096 y también las que están incluidas en el convenio (Budapest, 2001, pág. 2)

1.5.3 Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público

La unidad fiscal del ministerio público especializada en delitos informáticos fue creada mediante resolución N° 1503-2020-MP-FN en el año 2020, donde se dispuso la creación de una red de fiscales especializados en ciberdelincuencia entre ellos 34 titulares y 30 alternos, así mismo esa red a la que integraron fue una adición a sus actuales funciones que venían desempeñando como fiscales.

La unidad fiscal tiene como objetivo principal efectuar una orientación técnica jurídica en las investigaciones referidas a los delitos informáticos como por ejemplo las estafas informáticas para robar información y acceder a las tarjetas de ahorro o créditos. Así mismo también tiene el poder de unificar criterios en procedimientos de investigación y métodos que tengan que criticar, de esta manera se tendrá que elaborar directivas, algunos lineamientos en el ámbito de su competencia para de esta manera orientar a los fiscales penales a la realización de sus investigaciones.

1.5.4 Constitución política del Perú

En el artículo N° 200 de la constitución política del estado peruano contiene una garantía constitucional llamada recurso de habeas data y que así mismo tenemos un autor que resalta para que nos sirva este recurso.

(Quiroz) Señala:

El recurso de agravio constitucional de Hábeas Data, es una garantía contenida en la Constitución Política del Perú de 1993, protege dos derechos fundamentales, el acceso a la información y la autodeterminación informativa o protección de

datos personales. Estos, son derechos humanos de tercera generación, cuyo principio es la solidaridad, en la que intervienen, las personas, el Estado y las empresas privadas. Esta garantía surge como respuesta al avance imparable de las nuevas tecnologías de la información y las comunicaciones, que, acopian, registran y procesan ingentes cantidades de datos personales, que, si no son protegidos de acuerdo a los tratados internacionales y a las normas internas de cada país, pueden constituir un grave riesgo a la privacidad de los individuos (Quiroz, 2016, pág. 2)

1.6. Sentencia del Tribunal Constitucional, EXP. N.º 1189-2019-PHC/TC.

Recurso de agravio constitucional interpuesto por don William Bernardino García Rosales, abogado de don Marcos Morales Vargas, contra la resolución de fojas 421, de fecha 5 de noviembre de 2018, expedida por la Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima, que declaró improcedente la demanda de habeas corpus de autos. Así mismo se solicitó que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017, que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y (ii) la Resolución de 26 de diciembre de 2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y, reformándola, le impuso ocho años de pena privativa de la libertad efectiva. Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal. Precisa que se condenó al beneficiario a través de una norma que no se encontraba vigente al momento que se cometieron los hechos delictuosos, pues tales hechos ocurrieron durante los meses de enero, febrero, marzo, julio, setiembre y octubre de 2013, pero fue condenado mediante la Ley 30096, que entró en vigencia el 23 de octubre de 2013, por lo que la norma aplicable era el artículo 185 del Código Penal, que en su forma agravada era el artículo 186, numeral 3 del referido código. El TC advierte que la sentencia de 16 de junio de 2017, el actor sustrajo en forma sistemática la suma de S/. 194,934.69 de la cuentas de los clientes de la empresa financiera Caja

Municipal de Ahorros y Crédito de Trujillo, en su condición de auxiliar de operaciones; asimismo, cuando trabajaba en la oficina ubicada en la agencia de Comas, Lima, logró manipular el sistema informático del pass word que se le entregó para el desarrollo de sus labores y la de otros trabajadores, con lo cual logró efectuar retiros de las cuentas de plazo fijo de los clientes de la financiera, para disminuir el saldo de capital de las mismas y apropiarse de dichos montos. Además, se le imputa haber falsificado la firma de algunos ahorristas a fin de simular su conformidad en los retiros. El 26 de marzo de 2014, la contralora de operaciones de dicha agencia advirtió su comportamiento, pues desde el mes de julio de 2013 utilizaba su clave de usuario y consultaba los saldos de las cuentas de los clientes que no efectuaban movimientos constantes para luego manipular el pass word de las cuentas de plazo fijo de la entidad financiera y apropiarse de dinero; es decir, que cometió diversas irregularidades, tales como la acontecida el 24 de marzo de 2014, en que había disminuido capital de la cuenta de plazo fijo, por la suma de S/. 12,000.00, sin contar con la presencia de la clienta, para lo cual falsificó su firma en el voucher respectivo; la del 13 de marzo de 2014, en que disminuyó el capital de la cuenta de plazo fijo, por el monto de S/. 5,000.00, sin contar con la autorización del titular de la misma, falsificando su firma en el voucher respectivo; y la disminución del capital de la cuenta de plazo fijo de otra clienta, por el monto de S/. 5,000.00, sin contar con su autorización, para lo cual falsificó su firma en el voucher de retiro. Esta conducta delictiva le permitió apropiarse de diversas sumas de dinero de otros clientes hasta por el monto de S/. 194,934.69. Asimismo considerando de la Resolución de 26 de diciembre de 2017, se aprecia que los hechos materia de instrucción datan de la conducta ilícita materializada en el año 2014, según consta de la denuncia fiscal, del auto de apertura del proceso y de los informes y documentos afines (en particular de los recibos falsificados que corren en autos), mientras que el delito informático en su modalidad de fraude informático agravado se encuentra previsto y penado por la Ley 30096 vigente desde el 23 de octubre del 2013, razón por la cual esta ley es aplicable al presente caso según lo previsto en el artículo 6 del Código Penal, descartándose así la aplicación retroactiva de dicha norma. (CONSTITUCIONAL, 2020, pág. 5)

Como se puede apreciar en el anterior párrafo se dio a conocer una grave situación que comprueba una vez más la gran problemática que existe en el Perú, toda vez que es un gran riesgo la manipulación de sistemas informáticos y más si no conocemos a las personas que realmente lo usan. Es así que se puede observar las grandes cifras de dinero que se apropió esta persona de los clientes de dicha caja municipal de ahorros.

Otra problemática que se puede observar es el tiempo en el que esta persona estuvo manipulando el sistema informático para ejecutar su conducta como el delito de fraude informático puesto que ello también se puede suponer que mucho antes ya había cometido este delito incluso antes de que esta promulgada dicha ley N° 30096.

El TC logro reafirmar declarando infundada la demanda del imputado puesto que se llegó a corroborar que se había cometido el delito de fraude informático dentro del plazo en que la ley estuvo completamente activa.

CAPÍTULO II

EL PROBLEMA, OBJETIVOS, HIPÓTESIS Y VARIABLES

2.1 Planteamiento del Problema

2.1.1 Descripción de la Realidad Problemática

En el Perú desde hace muchos años se viene globalizando la tecnología informática vista como una ayuda científica para las personas o empresas de nuestro país, que actualmente vienen accediendo a estas como un servicio de alta calidad para la vida cotidiana y para el desarrollo más fácil de los trabajos. Pero hay que resaltar que también a través de esta tecnología se ha revolucionado nuevas modalidades de crímenes, como es el fraude informático y otras modalidades que actualmente vienen afectando a los mismos usuarios o empresas que acuden a estas para su efectivo fin. Así mismo en esta época de pandemia como es el Covid-19, se ha ido incrementando fuertemente y no tiene un control necesario para resguardar la seguridad de la sociedad.

Las personas con el paso de los años usaban las computadoras, que eran sistemas informáticos de comunicación, registro de información y datos y que a través de esto existía los hackeos de información que se ejecutaba a través de un virus que pondría en riesgo la información personal del usuario. Después fue apareciendo con la ciencia el teléfono celular o también llamado ahora Smartphone que podría decir que es una computadora portátil porque se puede generar cualquier acción que se efectuaba con la computadora y que mediante el cual registran un número de acceso para que se puedan comunicar libremente o mandar mensajes de textos, también tenemos el Facebook que un página web o aplicación que te puedes comunicar con una persona a larga distancia, así mismo también existe el WhatsApp que es un medio comunicador en cual puedes hacer video llamadas a larga distancia o mandar mensajes. Es a través de

estos mensajes que los delincuentes envían cierta información con el famoso premio y que solamente puedan acceder a esto ingresando a un link web para que puedan ganárselo, pero es aquí que muchos por ingresar sin malicia alguna el delincuente roba la información necesaria ingresando un virus en el dispositivo de las personas sin que estas se den cuenta de lo sucedido. A ello también existen los aplicativos gratuitos que cualquier persona puede descargar en su teléfono celular tales son como juegos, aplicativos de los bancos para registrar nuestras cuentas bancarias, correos, etc. Tras esto los delincuentes cibernéticos pueden ingresar un pequeño virus y hackear la información personal de las personas hasta también vaciar cuentas bancarias. Ahora con la evolución de la tecnología cualquier aparato tecnológico necesita el internet, como por ejemplo las impresoras, cámaras de seguridad, lavadoras, Tablet etc. y es aquí donde estamos ante un peligro muy cercano y que cualquiera hacker puede acceder y esto preocupa a muchas de las personas que actualmente contamos con estos dispositivos.

2.1.2. Antecedentes teóricos

Las tecnologías de la información, son cada vez más avanzados en sistemas tecnológicos de información en sus diversas modalidades que en la mayoría de casos ha generado el cambio del estilo de vida, el derecho no es ajeno a esta situación, y más aún el derecho penal, es por ello que, la problemática que aquí se aborda sobre los delitos informáticos necesariamente ha encontrado respaldo en una serie de teorías jurídicas que permiten la demostración de nuestra hipótesis.

Tal es el caso de la teoría del delito que guarda relación con el presente tema a tratar ya que es una herramienta indispensable para elaboración de una investigación procesal que se hará para verificar ciertos parámetros que consta en la presente norma.

Seguidamente, se tiene la teoría de la tipicidad que es una teoría muy interesante, al resaltar que gracias a este se puede describir los

comportamientos humanos atípicos que están regulados en nuestro ordenamiento jurídico peruano, es un claro ejemplo el delito informático que está plasmado en la ley N° 30096 en donde consta con artículos interesantes sobre las diferentes modalidades de cibercrímenes.

El comportamiento humano siempre está en constante evolución es por ello que la teoría de la tipicidad analiza ciertas conductas para estudiarlas y verificarlas si cuentan con algún problema que altere a la sociedad y más ahora con el cambio y avance tecnológico.

Así mismo tenemos también la teoría de la información que es aquella herramienta necesaria para investigar la información si es sumamente confiable o no. La teoría de la información es muy compleja propiamente dicha, ya que cuenta ciertos cambios tecnológicos que se vienen desarrollando, es por ello que tiene que mutar en diversas categorías para no generar problemas informáticos que vienen apareciendo con el avance tecnológico.

Se ha encontrado tesis que desarrollan en cierta manera y grado el tema que aquí se plantea, como es la tesis presentada por Alejo Pardo Vargas, titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima”.

Las conclusiones que resalta el autor son muy importantes para este trabajo de investigación puesto que en todo momento se reconoce que la ley 30096 presenta deficiencia en la modalidad de fraude informático, tanto en que se concentran diversas modalidades de delitos informáticos y por ser un delito ambiguo, no se puede permite ejecutar con efectividad. Un cierto acercamiento a esa duda está en la modalidad de sabotaje informático no se regula en forma clara y expresa esto quiere decir que no se da una cierta de definición a que esta modalidad se convierte a través de una afectación, pero con fines lucrativos. En el caso de la modalidad de estafa informática esta no se regula expresamente en la ley 30096 y

ocasiona una gran incertidumbre en el ordenamiento jurídico al dejar un vacío legal y presentaría que la investigación y la sanción se dificulten

También tenemos la tesis presentada por el alumno Montoya Guillén, Franklin Abraham titulada “Regulación expresa del delito informático de clonación de tarjetas – Sede DIVINDAT, 2017”.

Montoya hace 3 conclusiones claves para el desarrollo de su obra, el autor de esta presenta tesis comparte la opinión, por sobre todo de que la ley 30096 presenta deficiencias, pero es claro desarrollar ciertos puntos de la redacción antes mostrada. Así es que en la primera conclusión encontramos que el Delito de Clonación de Tarjetas no está claramente tipificado y definido en la actual ley. Es por ello que revisando la presente ley y haciendo un estudio de esta misma, se da por concluido que en el delito de fraude informático comprende varias modalidades de ciberdelincuencia y eso genera mucha confusión al momento de aplicar un delito de esta índole puesto que en otros casos tampoco están previstos como es el delito de estafa informática. Franklin menciona que analizando las legislaciones comparadas existe una cierta similitud a lo que quiere llegar su obra, puesto que en otros países si regulan de manera específica las nuevas modalidades de delincuencia informática. También para concluir señala que el delito de clonación de tarjetas debería independizarse del delito de fraude informático constituido en la ley, y esta es una apreciación que se comparte positivamente al ser este tipo penal distinto a los demás en su definición y en el fin objetivo.

2.1.2 Formulación del problema

¿Cuáles son los Mecanismos Jurídicos para Implementar la Ley 30096 en los Delitos Informáticos contra el Patrimonio frente a las nuevas Tecnologías Informáticas?

2.2 Finalidad y Objetivos de la investigación

2.2.1 Finalidad

La finalidad de la presente investigación es que nuestra legislación peruana cree una estructura base para todas las ciudades nuestro país con una fiscalía especializada en delitos informáticos, en las que cualquier persona tenga acceso a fácilmente y se les llega a retribuir tales perdidas las que han sido arrebatadas mediante este avance tecnológico.

2.2.2 Objetivo general y específico

2.2.2.1 Objetivo General

Determinar los Mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas

2.2.2.2 Objetivos Específicos

- a) Analizar las nuevas tecnologías informáticas frente a los delitos contra el patrimonio
- b) Establecer la regulación de los informáticos en el derecho comparado
- c) Identificar las causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos peruanos.
- d) Establecer el procedimiento fiscal y judicial que se adopta en los delitos informáticos contra el patrimonio
- e) Proponer la creación de una fiscalía especializada en delitos informáticos para lograr una mayor efectividad frente a la comisión de delitos informáticos.

2.2.3 Delimitación del estudio

2.2.3.1 Delimitación Temporal

La presente investigación se circunscribe a los datos del periodo de 2021-2022, asimismo a la ley de delitos información

2.2.3.2 Delimitación Espacial

El presente trabajo de investigación será desarrollado en la provincia de chincha, distrito de chincha alta.

2.2.3.3 Delimitación Social

La presente investigación será dirigida a personas del distrito de chincha y en general.

2.2.4 Justificación e importancia del estudio

2.2.4.1 Importancia

Esta investigación es de suma importancia porque a la vista de muchas denuncias presentadas a nivel nacional el 90 % de ellas son delitos cometidos contra el patrimonio como es en la modalidad de fraude y muchas de estas denuncias quedan estado de archivo al no encontrar la persona culpable de dicha conducta.

Es por ello que esta investigación propondremos a nuestra legislación crear una Fiscalía Especializada en Delitos Informáticos en la provincia para de estar poder llegar a una mejor efectividad de búsqueda criminal.

2.2.4.2 Justificación Teórica

La presente investigación encuentra su justificación en su aspecto teórico, ya que, en un sistema democrático de derecho, la persona humana es el fin supremo tal como lo establece nuestra Carta magna por ello, es necesario el aseguramiento de sus derechos fundamentales como consta, así como aquellos relacionados a sistemas informáticos, bases de datos, las comunicaciones y la reserva de las mismas y otros bienes jurídicos que contengan relevancia e importancia penal – patrimonial.

2.2.4.3 Justificación social

La elaboración de una fiscalía especializada a favor de los juristas, jueces, fiscales, para elaborar instrumentos informáticos, que pueden servir para

situaciones que serán investigadas de manera más fácil y útil, una vez que sean demostrados su validez y confiabilidad podrán ser utilizados en diferentes modalidades que surjan con la evolución de las nuevas tecnologías.

2.2.4.4 Justificación práctica

Esta investigación será práctica, porque será de suma utilidad en cuanto a la comprobación respecto a la aplicación de los nuevos mecanismos informáticos y con ello se resguardará la seguridad jurídica y la vigencia del debido proceso.

2.3 Hipótesis y variables

2.3.1 Hipótesis General

Los Mecanismos jurídicos para implementar la Ley N°30096 de Delitos Informáticos contra el Patrimonio frente a las nuevas Tecnologías Informáticas son:

- a) Promover la especialización de fiscales penales
- b) Incluir la tipificación expresa en el código penal peruano

2.3.2 Variables e indicadores

2.3.3.1 Variable Independiente

Los Mecanismos jurídicos para implementar la ley 30096

2.3.3.2 Variable Dependiente

En los delitos informáticos contra el patrimonio

CAPITULO III

MÉTODO, TÉCNICA E INSTRUMENTOS

3.1 Población y Muestra

3.1.1 Población

La población motivo de esta investigación está conformada por un total 30 personas naturales, dentro de ello 10 fiscales 10 policías y 10 personas de la ciudad del distrito de chincha alta que se comprometieron en respaldar este estudio a través de su conocimiento acerca de la situación actual de la ciudad La presente muestra que utilizaremos será la no probabilística.

3.1.2 Muestra

La muestra utilizada de la fuerza social en la presente investigación, aplicando el muestreo no probabilístico por conveniencia, está conformada por un total del 50 % personas del distrito de chincha alta. Siendo dicha muestra el orden de personas 5 fiscales, 5 policías y 5 personas naturales habiéndose utilizado preferentemente a personas que tenían conocimiento de dicha problemática e interés de participar sobre la problemática del Avance tecnológico en el país y sobre las consecuencias que pueden traer.

3.2 Diseño a utilizar en el estudio

3.2.1 El tipo de investigación

La presente investigación es Aplicada o lege ferenda ya que se busca proponer la creación de una fiscalía provincial penal especializada en delitos informáticos

3.2.2 Métodos aplicables a la presente investigación

3.2.2.1 Métodos generales

3.2.2.1.1 Método deductivo

La presente investigación utiliza el método deductivo ya que nos encontramos en una situación muy complicada con el avance tecnológico que se ha desarrollado en la sociedad y el mundo.

(Decoo, 1996)) Afirma lo siguiente:

Un método deductivo es aquél en el que el proceso de aprendizaje se mueve de lo más general a lo más específico, de las reglas que articulan la lengua meta a la aplicación de tales reglas en el uso cotidiano de tal 24 lengua. Este es un proceso consciente para el alumno, pues es instruido para que estudie tales reglas de forma que sea capaz de ponerlas en práctica. Así pues, un desarrollo deductivo del aprendizaje de una lengua extranjera implicaría poner en práctica métodos gramaticales y cognitivos (p.96)

(Ruiz) Señala al autor:

Pheby asegura que el método deductivo pasa de lo general a lo particular, de forma que partiendo de unos enunciados de carácter universal y utilizando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo, cuando las premisas de partida están constituidas por axiomas, es decir, proposiciones no demostrables, o hipotéticos-deductivo, si las premisas de partida son hipótesis contrastables. Distinción entre método deductivo y deductivismo, inconsistencias del deductivismo para el quehacer filosófico-científico: Un análisis deductivo puede favorecer una mejor comprensión de los fenómenos, sin embargo, es necesario hacer una distinción entre el método deductivo y el deductivismo (Ruiz, 2017, pág. 17).

3.2.2.1.2 Método inductivo

Se utilizó el método inductivo porque propondremos nuevos instrumentos necesarios para combatir la ciberdelincuencia que ocurre en este momento con mayor frecuencia.

Según (Rodríguez A.) señala:

La inducción es una forma de razonamiento en la que se pasa del conocimiento de casos particulares a un conocimiento más general, que refleja lo que hay de común en los fenómenos individuales. Su

base es la repetición de hechos y fenómenos de la realidad, encontrando los rasgos comunes en un grupo definido, para llegar a conclusiones de los aspectos que lo caracterizan. Las generalizaciones a que se arriban tienen una base empírica (Rodriguez D. , 1990, pág. 10).

3.2.2.1.3 Método analítico

La presente investigación utiliza el método analítico, porque vamos analizar la ley 30096, su modificatoria y su actual situación en la sociedad.

El método analítico es un procedimiento cognitivo que ayuda a encontrar problemas, soluciones, etc. se afirma que “el análisis es un procedimiento lógico que posibilita descomponer mentalmente un todo en sus partes y cualidades, en sus múltiples relaciones, propiedades y componentes. Permite estudiar el comportamiento de cada parte” (Rodriguez A. , 2017, pág. 8). No puede existir otra definición más propia para describir este método al ser uno de los más competitivos para el desarrollo de una tesis o investigación.

3.2.2.2 Métodos específicos

3.2.2.2.1 Método dogmático

(Tantaleán) Señala:

Aquí se estudia a las estructuras del derecho objetivo o sea la norma jurídica y el ordenamiento normativo jurídico. Por lo que se basa esencialmente, en las fuentes formales del derecho objetivo. En los estudios de dogmática jurídica se investiga lo que los humanos dicen que hacen con el derecho y se los conoce como dogmáticos porque en nuestra disciplina la norma jurídica es considerada un dogma (Tantaleán, 2016, pág. 4)

La presente investigación utiliza el método dogmático porque se llega a proponer una regulación legislativa como es la introducción de nuevos instrumentos tales un software que sea capaz realizar la búsqueda de los ciberdelincuentes sin mayor

complicación, así mismo una estructura donde se lleve a cabo las investigaciones con la ayuda de la policía nacional y a esto me refiero a la creación de Fiscalía especializada en delitos informáticos, para favorecer al estado y a los ciudadanos conforme al avance tecnológico que se ha desarrollado en la sociedad con el paso de los años

3.2.2.2.2 Método hermenéutico

(Hermida) Afirma que:

La hermenéutica provee una alternativa propia para la interpretación de los textos. La hermenéutica es, en sentido general, el estudio de la comprensión y de la interpretación, y en sentido particular, la tarea de la interpretación de textos. la hermenéutica no se limita a un conjunto de instrumentos y técnicas para la explicación de textos, sino que intenta ver el problema dentro del horizonte general de la interpretación misma (Hermida, 2019, pág. 75).

En este método es importante recalcar que lo utilizaremos porque llegaremos a interpretar como la norma de los delitos informáticos contra el patrimonio y su aplicación en la sociedad.

3.2.2.2.3 Método exegético

(Machicado) Consigna lo siguiente:

El Método exegético es el estudio de las normas jurídicas civiles artículo por artículo, dentro de éstos, palabra por palabra buscando el origen etimológico de la norma, figura u objeto de estudio, desarrollarlo, describirlo y encontrar el significado que le dio el legislador (Machicado, 2011, pág. 2)

La presente tesis utilizara el método exegético porque analizaremos la ley de delitos informáticos contra el patrimonio establecido en el artículo 8 de la ley 30096 y su tipificación en el código penal peruano para de esta manera tener una apreciación de cómo se maneja la imputación hacia a las personas activas del delito.

3.2.3 Enfoque de la investigación

Esta investigación es de enfoque mixto, el cual consiste en la realización de prácticas interpretativas que conduce a describir, analizar y discutir el fenómeno objeto de estudio a través de entrevistas, conversaciones, recurriendo a fuentes documentales para dar sentido a la interpretación del problema en estudio y responder a los cuestionamientos o interrogantes fácticos jurídicos, sociales, dogmáticos y prácticos.

3.2.4 Diseño

El diseño de investigación es cuasiexperimental, el cual se refiere a datos recopilados de manera no total, por medio de un proceso de investigación como es la recolección de datos de denuncias, entrevistas a personas del derecho y público en general.

3.3 Las técnicas e instrumentos de recolección de datos

Las técnicas e instrumentos utilizados en el desarrollo de la presente investigación son las siguientes:

3.3.1 Técnicas

3.3.1.1 Observación documental

Para la presente investigación haremos uso de la observación documental, por cuanto se procede a realizar la revisión y lectura de libros, revistas, artículos de investigación, tesis, que sirven para el desarrollo del tema.

Para conocer un poco más sobre este punto consideramos que es “una técnica en la cual se recurre a información escrita, ya sea bajo la forma de datos que pueden haber sido producto de mediciones hechas por otros, o como textos que en sí mismos constituyen los eventos de estudio” (Fuenmayor, junio 2012, pág. 79). Es así que en esta investigación recolectamos datos para analizarlos con el objeto de estudio.

3.3.1.2 Entrevista

Tenemos a (Folgueiras) que nos explicara que se entiende por la entrevista:

La entrevista es una técnica de recogida de información que además de ser una de las estrategias utilizadas en procesos de investigación, tiene ya un valor en sí misma. Tanto si se elabora dentro de una investigación, como si se diseña al margen de un estudio sistematizado, tiene unas mismas características y sigue los pasos propios de esta estrategia de recogida de información. Por tanto, todo lo que a continuación se expone servirá tanto para desarrollar la técnica dentro de una investigación como para utilizarla de manera puntual y aislada (Folgueiras, 2016, pág. 2).

En este sentido, la entrevista, en el desarrollo de la presente investigación ha sido aplicada usando canales de comunicación, esto es, por medios electrónicos, donde a través de cual se ha remitido las preguntas de entrevista formuladas de acuerdo a los objetivos de la investigación, dándose la libertad al entrevistado responde las preguntas de acuerdo a su convicción.

3.3.2 Instrumentos de recolección de datos

Los instrumentos de recolección utilizados en el desarrollo de la presente investigación son las siguientes:

3.3.2.1 Ficha de observación documental

La ficha de observación lo usare para comenzar una descripción específica de la investigación de campo a tratar en esta tesis, y lo complementare con una entrevista en donde se detallará los datos e información importantes de las personas que harán llegar.

3.3.2.2 Guía de entrevista

(Fuenmayor):

La guía para la entrevista es una herramienta que permite realizar un trabajo reflexivo para la organización de los temas posibles que se abordaran en la entrevista. No constituye un protocolo estructurado de preguntas. Es una lista de

tópico y áreas generales, a partir de la cual se organizarán los temas sobre los que tratarán las preguntas (Fuenmayor, junio 2012, pág. 53).

Por medio de este instrumento de recolección de datos, el investigador formulará un listado de preguntas abiertas de acuerdo a los objetivos de la investigación, el cual estará en forma ordenada, con el título y objetivo que busca el instrumento, dirigida al entrevistado, para de este modo facilitar al entrevistador y lograr la información que realmente se quiere obtener.

3.4 Procesamiento de Datos

Para procesar este dato voy a recurrir a cuadros comparativos para realizar las preguntas las entrevistas.

CAPITULO IV

PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1 Presentación de resultados

4.1.1 Las nuevas tecnologías informáticas frente a los delitos contra el patrimonio

Para hablar de tecnología informática debemos hacer una pausa para conceptualizar estos términos. Para el presente investigador se puede decir que es aquella que se ocupa de todos los procesos para tratar la información en su actividad dentro del mundo de las computadoras y sistema de comunicación como son los teléfonos celulares.

Una computadora se puede distinguir como una maquina eléctrica, creada para almacenar información que actualmente todas las personas conocemos, pero el uso de estas máquinas informáticas tiene ventajas y desventajas que a continuación desarrollare:

Ventajas en el patrimonio

En el ámbito jurídico

1. La realización de videoconferencias que se viene desarrollando en las audiencias por parte los organismos de justicia como es el poder judicial en conjunto con el ministerio público y los abogados.
2. El depósito de las tasas judiciales se hace mucho más fácil.
3. La información de expedientes judiciales, como resoluciones, sentencias, escritos presentados por las partes están guardados en un almacenamiento informático como es el data center.
4. La información de los procesos judiciales esta de modo organizado mediante programas informáticos.

5. Se puede digitar los escritos presentados por las partes y por los entes judiciales.

Desventajas en el patrimonio:

En el ámbito jurídico

1. Sabotaje informático
2. Clonación de tarjetas de crédito
3. Fraude informático
4. Aumenta la modalidad de extorsión
5. Roban información de las personas

Las tecnologías informáticas actualmente se vienen desarrollando de manera muy rápida, que en las distintas partes de nuestro país vienen aumentando el porcentaje de denuncias que viene tomando el control actual de la sociedad con el pasar de los años.

Una de estas tecnologías informáticas son las redes 4G que no exige el menor uso de red y los costos de los datos pueden ser menores para todos. Sin embargo, eso es el detalle de esta nueva tecnología, que no te exige un costo excesivo por el uso del aparato tecnológico (celular).

Si bien es cierto, es una ventaja para nuestra sociedad, pero también genera inseguridad jurídica, ya que cualquier usuario desconocido puede acceder de forma más fácil a contactarse con cualquiera de nosotros.

Es así que la tecnología informática genera muchas relaciones con nuestro ordenamiento jurídico y uno de ellas es la resaltante en nuestro proyecto de investigación y hablamos del delito informático contra el patrimonio en su modalidad de fraude informático que se relaciona a través de esas acciones atípicas como son los llamados

sabotajes informáticos en el cual se desarrolla vulnerando un sistema informativo y destruyendo con el objetivo de obtener un fin ilícito.

También se conoce la modalidad de clonaciones de tarjetas de créditos, que nace a través de un aparato tecnológico que introducen en el cajero automático de cualquier banco con el fin copiar la información del agente y así sustraer un patrimonio económico de este. Por otro lado, pueden diseñar, introducir o alterar el sistema informático de alguna persona con el fin de obtener una información que le pueda servir al delincuente para cometer hechos delictivos, un claro ejemplo son las transferencias inseguras de mercados ilícitos el cual diseñan alguna oferta de algunos productos que le genere importancia a la víctima.

Lo revolucionario es que estas modalidades se están desarrollando más ahora con el uso del internet en los dispositivos de comunicación como son los famosos teléfonos celulares que ya son llamados como computadoras portátiles que pueden ser llevados a cualquier lugar con la sola cobertura de zona wifi.

Los delitos contra el patrimonio según el artículo 8 de la ley 30096 hace mención cada de una de estas modalidades, pero que no son descritas de forma transparente por el ordenamiento jurídico. De modo que esa la gran problemática que existe hoy en día.

4.1.2 La regulación de los Delitos informáticos en el derecho comparado

a) Legislación Colombiana

En Colombia el 5 de enero del año 2009 el congreso de la Republica Colombiana promulgo la Ley N°1273, que modificaba su código penal creando un nuevo bien jurídico titulado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones,

entre otras disposiciones"(Diario Oficial de la república colombiana (p.1). Conocido esto como los nuevos delitos tipificados en su código penal en contra ante de las nuevas modalidades de ciberdelincuencia en el país.

La Ley N° 1273 de la república de Colombia se creó con el fin de salvaguardar los intereses de las personas naturales, empresas y el mismo gobierno por el incremento de ataques cibernéticos que hubo años anteriores como por ejemplo las clonaciones de tarjetas bancarias, vulneración y alteración de los sistemas de cómputos, transferencias de fondos mediante manipulación de programas y afectaciones a los mismos cajeros automáticos entre otras conductas.

Así mismo esta ley está dividida en dos capítulos a saber a saber:

Primero. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

En este primer capítulo encontramos todos los delitos dirigidos aquellas personas que ilícitamente se intercepten en los datos personales de las personas y empresas públicas o privadas como por ejemplo el acceso a un sistema informático sin autorización de un usuario, el que obstaculice ilegítimamente el normal funcionamiento de un sistema informático o una red de telecomunicación, así mismo también el que intercepte o dañe datos informáticos, el que introduzca o extraiga un software malicioso , y también el que suplante sitios web para capturar datos personales.

Segundo. De los atentados informáticos y otras infracciones

En este último capítulo encontramos dos delitos con un interés de carácter patrimonial por así decirlo, como por el ejemplo el delito de hurto a través de medios informáticos como es la manipulación de un sistema, red o la suplantación de un usuario con el sistema de autenticación permitidos por el gobierno.

En conclusión, de esta normativa generada por el gobierno colombiano fue motivo por el cual se fue descontrolando esta delincuencia que fue generado por el avance tecnológico que sufren todos los países del mundo. Así mismo la ley 1273 fue un paso importante en la lucha de los delitos informáticos en la república colombiana.

Por otro lado, deberían actualizar una nueva regulación ante nuevas modalidades labores como es el trabajo a distancia que conllevan una importante supervisión al manejo de información, también ante los nuevos aplicativos de transferencia bancarias.

b) Legislación Chilena

En Chile el 7 de junio del año 1993 entro en vigencia la ley N°19.223 sobre delitos informáticos. Esta ley tiene como finalidad proteger a un nuevo bien jurídico como es “la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan” (Acurio 2016, p. 38). Lo que refiere es que la información debe estar contenida si o si en un sistema automatizado como son las computadoras o algo cercano a ellos como son los celulares y que la información sea pura y buena calidad.

Esta ley consta de 4 artículos como señala (chileno, 1993)

Artículo 1. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo (Ministerio de justicia chileno, 1993, p.1 s/n)

Artículo 2. El que, con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento

de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4. El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado (chileno, 1993, pág. 1)

En conclusión, en estos artículos se contemplan los delitos informáticos sobre una base de 4 artículos así mismo se puede describir que la ley nos habla sobre el famoso sistema de tratamiento que se puede describir como un sistema informático. Conociendo estos términos se puede decir que el artículo 1 de la presente Ley trata de referirse a los daños que se puedan cometer contra el hardware sea inutilizándolo o destruyéndolo. El hardware es importante ya que es la base para poder realizar cualquier tipo de trabajo.

En el artículo 2 de la presente hace referencia al espionaje informático con el fin conocer una información en la que no está autorizado.

El artículo 3 se tipifica el sabotaje informático, así mismo el sabotaje se puede describir cómo hacer daño o destruir los datos contenidos en un sistema informático o en el caso de Chile un sistema de tratamiento.

En el último artículo de la presente ley nos señala que está previsto como ilícito el difundir datos de un sistema de información. Este último se refiere a difundir datos que contengan información privada de manera estrictamente privada puede ser de personas naturales o de alguna persona jurídica.

c) Legislación Argentina

En el año 2008 el 24 de junio el senado y cámara de diputados de la nación de argentina promulgo la Ley N°26.388 Ley de Delitos informáticos. Esta ley detalla la regulación de estas nuevas modalidades de delincuencia, así como también la comisión de acciones que atentan en provocar una violación de secreto y de la privacidad.

La ley consta de 13 artículos en específico.

Del artículo 1 al 3 consta de aquellos delitos cometidos en contra de la integridad sexual, como por ejemplo en estos acápites de la norma argentina está prohibido el producir, comercializar, publicar ofrecer etc. Todos aquellos dedicados a la actividad sexual, pero en menores de edad.

Si bien es cierto la integridad sexual para el autor tiene un significado muy profundo y delicado toda vez que considera que es aquella sociedad sexual de una persona que se conecta con su paz interior en conexión con el sistema emocional y físico de una persona.

Así mismo del artículo 4 al artículo 6 de la presente ley detalla aquellos delitos en contra de la libertad de las personas, por ejemplo, el que acceda o publique una comunicación electrónica, sistema o dato informático de una persona natural o jurídica sea pública o privada será sancionada jurídicamente.

Para hablar de libertad tenemos que hacer un hincapié en este acápite porque estaríamos hablando de uno de los derechos fundamentales que actualmente todos los países del mundo protegen.

Para el autor la libertad viene hacer aquellos poderes de una persona que puede realizar sin vulnerar las normas previstas de una nación. La persona tiene el derecho de poder crear modificar o alterar cualquier parte de su vida cotidiana sin afectar a otros.

Así mismo si hablamos de delitos informáticos, cualquier persona tendría el derecho de poder tener una comunicación privada con otro mismo, también la libertad de no compartir datos informáticos que mantenga en un sistema operativo como son las computadoras.

El artículo 7 y 8 de la norma argentina nos hablan acerca de aquellos delitos cometidos que atentan contra acceso y revelación de información de datos de bancos de datos personales.

Para identificar que son bancos de datos personales en la nación argentino el autor hizo una serie de investigaciones para poder conceptualizar dichos términos que son distintos a la información que normalmente conoce. Así mismo el banco de datos personales es aquel conjunto de información, sea física, electrónica dentro de un sistema operativo.

En el artículo 9 y 10 de la presente ley argentina identifica aquellos delitos cometidos a través del fraude informático. El fraude informático se puede diferenciar como aquel delito cometido mediante una red del internet con el objetivo de tener un provecho ilícito a hacia un tercero. El fraude se puede cometer a través de alguna página web, un sistema de comunicación como es el Facebook, WhatsApp, etc. Se configura con la sola obtención de algún patrimonio.

Del artículo 11 al 13 tenemos aquellos delitos comprendidos como sabotaje o daño que se pueden cometer contra algún sistema informático de la alguna empresa o persona en particular.

Para concluir el autor está de acuerdo con la regulación de aquellos delitos que tipifica la norma argentina. Como bien respecta son diversos delitos que normalmente todos los países regulan, como por ejemplo la pornografía infantil, el fraude informático, el daño o sabotaje informático que atente contra la seguridad privada o pública de la sociedad.

d) Legislación Peruana

En el Perú a partir de los años 2000 se pudo ver de igual forma los cambios tecnológicos informáticos que constantemente ocurrían como en otros países. Tras este aumento de tecnología también se pudo apreciar a sí mismo la gran cantidad de denuncias que presentaban las personas ante las criminalizaciones que se iban ejecutando por parte de los delincuentes usando la tecnología. Es así que, empezaron a salir a luz las clonaciones de tarjetas, las transferencias bancarias, las estafas cibernéticas y el sabotaje. Conforme a lo que sucedía fue que el gobierno peruano el 21 de octubre del año 2013 promulgo la ley de delitos informáticos Ley N° 30096 que criminalizaba las conductas que normalmente estaban dañando los sistemas informáticos y así mismo las integridades de las personas. Con esto el gobierno peruano pudo combatir gran parte de las criminalidades informáticas que ocurrían en el país en donde más se usaba estos tipos de servicios electrónicos.

Así mismo el gobierno peruano en el año 2019 suscribió un convenio para combatir la ciberdelincuencia llamado el “Budapest”, que tiene por finalidad combatir la delincuencia informática y que en ellos distintitos países que conocemos la forman como, por ejemplo, Estados Unidos de América, Italia, España, Japón, Canadá, Israel, Argentina, Chile, Costa Rica, Paraguay, República Dominicana, Panamá, Colombia. De tal forma que todos los países que la conforman según el artículo 35 del convenio de “Budapest” tiene el derecho de “garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que configuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos: Asesoramiento técnico, conservación de datos, obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos” (Budapest, 2001, pág. 40). Este convenio fue de mucha importancia para el estado peruano, ya que se convirtió en una herramienta se podría usar en

casos de emergencia como es la búsqueda de un criminal sospechoso o también alguna asistencia técnica que se podía desconocer en sistema informático del país.

4.1.3 Causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos de los operadores de justicia peruano.

Las causas por las cuales estas nuevas modalidades de ciberdelincuencia no son detectadas por nuestro sistema jurídico son los siguientes:

- a) Cuando se lleva a cabo las investigaciones preliminares no contamos aplicativos especiales para detectar los usuarios que logran su cometido. Al momento de que se presenta la denuncia en alguna comisaria o como es el caso de la localidad donde estamos investigando preguntamos a un oficial que estaba de servicio, si cuentan con alguna aplicación o software los efectivos policiales para detectar alguna amenaza de sabotaje informático o alguna denuncia por fraude de este tipo. Con lo cual respondió que no cuentan con alguna ciencia para hacer este tipo de trabajo pero que tiene la ayuda de ingenieros de sistemas para lograr bloquear estas páginas que son inseguras mas no de poder localizar al autor del delito porque es muy difícil poder identificarlo porque a veces estos mismos suplantan identidades de algunas personas. Esto da como resultado que lo advertido antes es totalmente negativo para el desarrollo de una investigación de esta índole.
- b) La mayoría de efectivos policiales no están capacitados para actuar ante estos delitos por no conocen mucho del avance tecnológico.

Los efectivos policiales no cuentan con algún centro de capacitación de tecnología informática que sea propiamente para rastrear algún usuario

que este atentando contra la integridad de una persona o poder lograr constituir una denuncia que sea acorde a lo que se presume por delito informático.

Deberían crearse un centro de capacitación para los efectivos policiales para crear una organización especial no tanto para tener conocimientos de los tipos penales comunes sino también de conocimientos tecnológicos para que tengan conocimiento de que se enfrentan y como ubicarlos.

- c) No existe motivación por parte de los operadores de justicia para socorrer a tiempo estos tipos de delitos

La motivación de los operadores de justicia como son principalmente los fiscales y efectivos policiales que buscan el cuerpo del delito, mayormente por ser un tipo penal de informática no les dan la motivación al caso a menos de que ya esté ubicado el autor del crimen por ser propio del proceso.

La motivación se puede desarrollar de dos formas, la primera es la motivación de investigación que es nada menos que la intención de querer llegar a encontrar indicios del crimen y descubrir al autor o autores que estén involucrados. La otra forma de motivación es la de carácter profesional. Si bien es cierto esta motivación es de suma obligatoriedad para estos operadores de justicia por lo que se considera poco profesional el dejar que estos tipos de casos se archiven de manera ligera y más con los casos de fraude informático que son los delitos que mayormente se están cometiendo.

4.1.4 El procedimiento fiscal y judicial que se adopta en los delitos informáticos contra el patrimonio.

El procedimiento del fiscal y judicial en los procesos de los delitos informáticos es el proceso que normalmente se adopta en cualquier tipo penal que se presente comúnmente. Pero hay que aclarar que

la etapa donde mayormente existe la debilidad de operar justicia es en la etapa de investigación preparatoria.

Esta etapa de investigación preparatoria se divide en dos sub etapas la investigación preliminar y la investigación preparatoria propiamente dicha. En etapa preliminar el fiscal directamente o con intervención de la policial nacional realiza los actos de investigación de la denuncia presentada que conste de los tipos penales que rigen en la ley N° 30096. No obstante, estos operadores al momento de recibir la denuncia, en conjunto logran llevar a cabo las diligencias para recabar y asegurar los elementos materiales de la comisión de un delito, así como individualizar las personas involucradas y asegurarlas debidamente.

Los elementos materiales de la comisión de un hecho delictivo en el caso de los delitos informáticos contra el patrimonio no son más que aquellos documentos de transacciones económicas, páginas web inseguras en las cuales se relaciona la víctima, como por ejemplo el Marketplace de Facebook donde las personas hacen compras online y mediante esta red se presenta la inseguridad de ser estafadas. Es por ello que el fiscal aquí recaba toda la información necesaria para saber si ha cometido un delito o no. Después de ello se tiene por objetivo saber quién o quiénes son las personas involucradas en este delito cometido como es el delito informático contra el patrimonio. Mediante ello el fiscal en conjunto con la policial nacional piden apoyo para la investigación a la unidad de fiscales especializados en delitos informáticos, para este desarrollo el tiempo es necesario ya que para ser esta petición se da por entendido que se toma algunos días en comunicarse con esta unidad y tener respuesta alguna.

Por lo general y acorde con realidad nunca se llega a encontrar a las personas involucradas, tal es el grado de que el fiscal tiene que dar por archivado la presente investigación si no hay un indicio necesario para seguir ampliando la investigación.

Si se logra llegar a encontrar a la persona involucrada y recabar los elementos materiales de la comisión del delito, automáticamente a pedido del fiscal se da el requerimiento de la conclusión de la investigación preparatoria y por ende formular la acusación. Es aquí donde el juez de investigación preparatoria convoca a diligencias preliminares para debatir la procedencia y conforme se sigue las demás etapas del proceso penal.

4.1.5 Posturas de los Fiscales y sus asistentes, abogados, secretarios del poder judicial y efectivos policiales respecto de que a los delitos informáticos con relación hacia el avance tecnológico

A efectos de ahondar en el desarrollo de cada uno de los objetivos se ha realizado una entrevista a fiscales, secretarios del poder judicial, abogados y efectivos policiales, la misma que será procesada conforme a continuación se detalla mediante cuadros comparativos.

Tabla 1

Pregunta 1 ¿Qué opina usted respecto al avance tecnológico informático y las nuevas modalidades de comisión de delitos informáticos?

ENTREVISTADO	RESPUESTA
N° 1	Es muy preocupante porque con el avance tecnológico existen más modalidades de delitos
N° 2	El avance tecnológico es bueno, pero también tiene sus desventajas en la sociedad.
N° 3	Hay que saber controlar esta tecnología con mejores presupuestos penales.
N° 4	El avance tecnológico siempre es bueno en la vida cotidiana y para mejorar cosas en nuestro país, pero trae consigo nuevas formas de ejercer la delincuencia.
N° 5	Estoy de acuerdo con el avance, pero hay que saber controlarlo
N° 6	El avance tecnológico es algo que ya no se puede evitar hoy en día.
N° 7	El avance de hoy es mucho más rápido que el que existía antes, ahora las mejoras científicas se dan cada año y eso es un problema para los legisladores de nuestro país, porque van a tener un grado modificaciones para ir controlando estas nuevas modalidades de delitos.

Nota: Elaboración propia

Tabla 2

Pregunta 2

¿Considera usted que la Legislación sobre los Delitos informáticos es efectiva para sancionar las nuevas modalidades delictivas con el uso de la nueva tecnología?

ENTREVISTADO	RESPUESTA
N° 1	Si, pero estaría bien que mejoren la parte procesal para que exista una investigación más profunda.
N° 2	No estoy de acuerdo porque creo que deja algunos vacíos en la norma con el constante avance.
N° 3	No es efectiva y se nota con las constantes denuncias que existen.
N° 4	Para mí no es tan eficaz, algunos fiscales hasta llegan a confundirse con otra norma penal.
N° 5	No es efectiva, debería modificarse.
N° 6	Si es efectiva, pero debería existir más capacitación para los fiscales.
N° 7	No es efectiva.

Nota: Elaboración propia.

Tabla 3

Pregunta 3

¿Es factible que las personas como las empresas privadas o públicas están expuestas a ser víctimas de fraude informático?

ENTREVISTADO	RESPUESTA
N° 1	Las personas siempre están expuestas más que todo porque ya cualquiera usa un celular mediante el cual registran todo tipo de información privada
N° 2	Mientras usen un dispositivo de comunicación están expuestas a que haya un delincuente atrás para robar información
N° 3	Siempre estamos expuesto y más ahora con la nueva tecnología
N° 4	Las personas de hoy en día usan un dispositivo celular algunos no saben usarlo y eso también puede ser una ventaja para los delincuentes.
N° 5	Sí, siempre estamos expuestos, y más ahora con muchas mejoras que tienen los aparatos tecnológicos incentiva a las personas que se compren más.
N° 6	Ambos están en expuestos, ya que ambos usan la misma tecnología
N° 7	Los que están más expuestos son las personas que hoy en día compran equipos con sistema de información y no saben usarlo.

Nota: Elaboración Propia

Tabla 4

Pregunta 4

¿Considera usted necesario una reforma legislativa para prevenir los delitos informáticos contra el patrimonio?

ENTREVISTADO	RESPUESTA
N° 1	Si es necesario, nos convendría a todos en esta sociedad

N° 2	Si claro que si es necesario y también la creación de una fiscalía especializada en delitos informáticos como fue el caso del medio ambiente.
N° 3	No es necesario, sino más que se cree un centro donde especialicen constante a los operadores de justicia.
N° 4	Si es necesario para combatir más la ciberdelincuencia
N° 5	Se perdería tiempo, solo se necesita más capacitación
N° 6	Estoy de acuerdo con la reforma
N° 7	No estoy de acuerdo con una reforma.

Nota: Elaboración Propia

Tabla 5

Pregunta 5

¿Considera usted que debería crearse una fiscalía especializada en delitos informáticos para lograr una efectividad en la aplicación de los delitos informáticos- Ley N° 30096 Ley de delitos informáticos?

ENTREVISTADO	RESPUESTA
N° 1	Estoy de acuerdo que se cree una fiscalía especializada en delitos informáticos, estamos ante una eminente lucha combatiendo la ciberdelincuencia y una ayuda muy importante para la investigación de estos delitos es la creación de esta misma.
N° 2	Estoy totalmente de acuerdo con la creación de esta fiscalía.
N° 3	Sí, estoy de acuerdo que se cree una fiscalía especializada en estos tipos de delitos que son de suma importancia.
N° 4	Si creo que es necesario para el país, como anteriormente lo dije igual fue el caso de las empresas mineras y la contaminación ambiental que después de ello se creó una fiscalía especializada en delitos ambientales.
N° 5	Es muy importante la creación de esta fiscalía ayudaría a todos los peruanos y generaría un poco más de seguridad para ellos mismos
N° 6	Si, esta creación debió proponerse desde que empezamos a tener estos de tecnología
N° 7	Si para combatir más la ciberdelincuencia

Nota: Elaboración Propia

Tabla 6

Pregunta 6

¿Respecto a su profesión y su experiencia laboral se logra identificar al autor de la comisión de un delito informático?

ENTREVISTADO	RESPUESTA
N° 1	No siempre logra identificar en la etapa de investigación, muchos de estos casos se archivan por estas razones
N° 2	A veces no se logra mucho identificar quienes son los que cometen estos tipos de delitos por lo mismo que suplantan identidades
N° 3	De cada 10 casos que he tenido siempre he visto que llegan a equivocarse el ministerio público en la tipificación del tipo penal.
N° 4	A veces se logra, pero ahora con la tecnología cualquiera puede suplantar identidades.
N° 5	Según las investigaciones no se logra detectar al verdadero autor del delito
N° 6	Según mi experiencia, he visto muchas denuncias, pero casi siempre se archivan por falta de pruebas o no llegan a impulsar con la investigación
N° 7	A veces se llega a identificar, pero en el proceso no se demuestra con pruebas suficiente

Nota: Elaboración Propia

Tabla 7

Pregunta 7

¿Considera usted que es de suma importancia tocar este tema más si estamos pasando este momento en nuestra sociedad con la evolución de la tecnología?

ENTREVISTADO	RESPUESTA
--------------	-----------

N° 1	Si y más ahora con el avance que tenemos actualmente de las tecnologías es bueno informarnos más sobre este tema.
N° 2	Si y te agradezco por esta entrevista, ya que existen modalidades que aun los legisladores no conocen y que deberían poner un poco de conocimiento.
N° 3	Sí. Estaría bien que se haga un pequeño hincapié en este tipo de delitos.
N° 4	Los congresistas deberían tomar conocimiento de las altas denuncias que se vienen presentando por los mismos fraudes informáticos que existen.
N° 5	Si es muy importante para que la sociedad empiece a tomar conciencia también que usar los medios tecnológicos es una desventaja para ellos mismos.
N° 6	Si es de suma importancia para que todos sepan que no es juego manejar las tecnologías y tomar precauciones para uno mismo
N° 7	Es de suma importante la entrevista y los temas porque solo así podemos llegar a los oídos de los congresistas y pongan mano dura en este tema.

Nota: Elaboración Propia

4.2 Contrastación de Hipótesis

Luego de haber desarrollado los objetivos específicos en sus diversos variantes como son las nuevas tecnologías informáticas frente a los delitos contra el patrimonio, la regulación de los Delitos informáticos en el derecho comparado, las causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos peruanos y el procedimiento fiscal, judicial que se adopta en los delitos informáticos contra el patrimonio y una propuesta de La creación de una fiscalía especializada en delitos informáticos para lograr una mayor efectividad frente a la comisión de delitos informáticos. Demostraremos de esta manera acerca de nuestra hipótesis es meramente negativo o positivo.

Si bien es cierto encontramos deficiente

a) Promover la especialización de fiscales penales

El Ministerio público de nuestra nación no adopta un programa organizacional de especialización de fiscales a nivel nacional, para que estas estén en constante ejercicio innovativo de conocimiento de las nuevas modalidades de ciberdelincuencia que vienen apareciendo en la sociedad.

Llevar a cabo especializaciones para cada fiscal tenga un conocimiento técnico informático-tecnológico para que pueda proporcionar asistencia rápida con el tema de los software y hardware proporcionándolo a través de las investigaciones preliminares que es la base del proceso penal.

b) Incluir la tipificación expresa en el código penal peruano

La tipificación de la norma que nos detalla la ley 30096 no está contemplada en el código penal peruano. Si bien es cierto, esta norma es una de las premisas importantes para que el titular de acción penal pueda ejecutar los modelos de delitos que contiene.

Es de suma importancia que este también contemplada en el código penal peruano, porque ese será el eje para que la sociedad sepa que delitos informáticos no están permitidos y cuales si están permitidos.

La sociedad de hoy en día no está bien preparada para este tipo de situaciones. Peor aún si no está tipificado en el código penal peruano como corresponde en el título x - artículo 207 en el que constaba los delitos informáticos que es la herramienta que comúnmente venimos usando para saber qué acciones están bien y cuales están mal.

4.3 Discusión de resultados

En el resultado del primer objetivo específico realizado se puede entender que las nuevas tecnologías informáticas frente a los delitos contra el

patrimonio pueden tener ventajas como así mismo lo contrario, por ser una tecnología avanzada que trae consigo mismo una serie de factores que destruyen la barrera jurídica para regular los delitos informáticos contra el patrimonio en la sociedad actual.

En el segundo objetivo específico se desarrolla las legislaciones comparadas y se hace referencia de algunas similitudes de aquellas regulaciones sobre los delitos informáticos que en nuestro caso vamos un poco adelantados, así como también actualizar algunas nuevas modalidades de ciberdelincuencia.

En el tercer objetivo específico desarrollado tenemos las causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos de los operadores de justicia en la cual se ha hecho un pequeño estudio de los causales más previstas en nuestro ordenamiento que son muy deficientes y se logra encontrar ciertos parámetros que actualmente se nuestros representantes tienen que tomar conciencia.

En el cuarto objetivo específico tenemos que hacer un pequeño hincapié ya que esto forma una parte fundamental para determinar si se logra recabar los elementos de convicción e individualizar a los autores involucrados del delito informáticos contra el patrimonio y por lo cual se discute muchas perspectivas, una de ellas es la individualización del imputado, al ser un delito informático no se tiene la tecnología necesaria o el apoyo necesario para esclarecer este punto y determinar quiénes han sido. Es por ello que normalmente existe muchas denuncias y correspondiente a ellos archivos sobre este tipo penal.

Como es de colegir de las entrevistas realizadas (tablas del 1 al 3) se puede apreciar que los entrevistados presentan un conocimiento reflexivo y conocen el sistema que actualmente contiene el Perú para regular las nuevas formas de crímenes. Pero también aclaran que la Ley 30096 no es factible para poder criminalizar estas conductas que actualmente se

están desarrollando, así mismo también reconocen que no es suficiente la norma para la completa regulación.

El autor está de acuerdo que este pequeño alcance que resalten los entrevistados, toda vez que el avance tecnológico es muy importante en el mundo, pero, también existen una serie de problemas jurídicos que hoy en día es escaso para el controlar estos nuevos sistemas informáticos.

Por otro lado, tenemos las (tablas del 4 al 5) las preguntas son totalmente puntuales la misma que es si se podría llegar hacer una reforma legislativa sobre los delitos informáticos y crear una fiscalía especializada en estos delitos. De los 7 entrevistados 4 de ellos están de acuerdo con la reforma mientras que los otros 3 aclaran que no es necesario sino más bien que se cree centros de capacitaciones para los fiscales.

El autor respeta la opinión de los entrevistados, pero en esta ocasión está de acuerdo con la parte que aclaran que no deberían reformar los delitos informáticos, porque ya existe una base estructural de regulación en el Perú, y lo que necesita esta misma es una institución que al menos pueda capacitar bien a los operadores jurídicos de justicia constantemente.

Así mismo respecto a sí se debería crear una fiscalía especializada en delitos informáticos, todos los entrevistados contestaron que sí están de acuerdo con esta propuesta, dado que generaría una ayuda jurídica solidaria para todos los ciudadanos al ser beneficiados con esta.

El autor comparte la misma respuesta que todos los entrevistados porque al poder crearse una fiscalía especializada en delitos informáticos tendría un poco de autonomía esta situación que ya tiene globalización en todo el mundo y se está apoderando de la vida cotidiana de todas las personas. Esta parte es muy importante porque el mayor problema de hoy puede causar la destrucción de cualquier sociedad más adelante y más ahora que la ciencia va cambiando constantemente y aparecen nuevas problemáticas.

Por último, tenemos las preguntas de las tablas del 6 al 7 las preguntas son puntuales que así mismo detallan si en las experiencias de los entrevistados como profesionales se logra identificar siempre al autor de la comisión de los delitos informáticos y la importancia de tocar este tema más si estamos pasando este momento en nuestra sociedad con la evolución de la tecnología. Con respecto a la pregunta sobre si llega a conocer siempre al autor principal de los delitos informáticos, se puede precisar que los entrevistados aclaran que casi siempre nunca se llega a reconocer quien es el verdadero autor del delito, toda vez que nadie sabe quién está de atrás de una pantalla o bien siempre suplantan identidades de algunas personas y capturan al equivocado o algunas veces por ser esto tipo de delitos archivan los casos por no tener pruebas suficientes.

Para el autor y para los entrevistados es de suma importancia tocar este tema sobre los delitos informáticos porque al mayor alcance de todos nosotros tenemos un dispositivo de comunicación que genera si una ayuda importante para nuestra vida, pero también una serie de problemas para la sociedad y es bueno controlarlo de alguna manera posible y como no el de crear una fiscalía especializada en estos delitos que atormentan ahora a cualquier usuario.

CAPÍTULO V

5.1 Conclusiones

1. La manipulación de nuevas tecnologías informáticas conlleva un gran aumento de nuevas modalidades delictivas por parte de los usuarios. Fomenta la ciberdelincuencia con el fin de obtener un patrimonio de un tercero. Fomenta delitos contra el patrimonio tales como: hurto agravado, estafa y el sabotaje informático.
2. Países como Argentina y Colombia han implementado la regulación de los delitos informáticos en la ley N°26.388 y la ley N°1273, respectivamente, La regulación de los Delitos informáticos en los distintos países detalla la gran importancia de poder criminalizar estas conductas delictivas. Surge la importancia de poder estabilizarlo de alguna forma para que no genere más problemas tanto para las personas naturales y jurídicas, así mismo con la similitud Perú tiene las mismas regulaciones que estos países, pero con el deficiente que en el actual esta ley esta derogada en nuestro ordenamiento jurídico como es el código penal. Pero a eso se le suma que en la ley N° 30096 no se esclarece las modalidades de ciberdelincuencia descritos en el artículo 8 que corresponde a los delitos contra el patrimonio.
3. Las causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos peruanos y encontramos como una de ellas la falta de conocimiento por parte de los organismos de justicia, son cuando se lleva a cabo las investigaciones preliminares no contamos aplicativos especiales para detectar los usuarios que logran su cometido, la mayoría de efectivos policiales no están capacitados para actuar ante estos

delitos por no conocen mucho del avance tecnológico, No existe motivación por parte de los operadores de justicia para socorrer a tiempo estos tipos de delitos

4. El procedimiento en la investigación preliminar es deficiente / juicio no hay suficiencia probatoria/ se adopta en los delitos informáticos contra el patrimonio es el mismo procedimiento como son con todos los procesos judiciales de cualquier delito contemplado en el código penal.

5.2 Recomendaciones

Las recomendaciones del autor son las siguientes:

- 5.2.1 Deberían especializar a los efectivos policiales con un centro donde constantemente los capaciten sobre las nuevas tecnologías.
- 5.2.2 Crear un centro de orientación sobre el avance tecnológico y desarrollarlo en las escuelas, centro de trabajos públicos o privados.

CAPÍTULO VI

6.1 Proyecto de Ley

Proyecto de Ley N° _____

**Sumilla: LEY QUE PROPONE LA CREACION
DE LA FISCALIA ESPECIALIZADA PENAL EN
MATERIA INFORMATICA EN LA PROVINCA
DE CHINCHA**

El Congresista de la República firmante del presente proyecto de Ley que a iniciativa del Congresista _____, ejerciendo su derecho de iniciativa legislativa al amparo del artículo 107° de la Constitución Política del Perú y acorde con lo establecido en los artículos 75° y 76° del Reglamento del Congreso de la República, ponen a consideración el siguiente Proyecto de Ley:

FORMULA LEGAL

LEY QUE PROPONE LA CREACION DE LA FISCALIA ESPECIALIZADA PENAL EN MATERIA INFORMATICA EN LA PROVINCA DE CHINCHA

Artículo único. Creación de la Fiscalía Especializada en Materia informática en la provincia de Chincha, ubicada en el departamento de Ica.

1. EXPOSICIÓN DE MOTIVOS:

Esta investigación tiene como punto principal la creación de una fiscalía especializada en la región de Ica para de esta manera combatir a los famosos ciberdelincuentes que han ido aumento con el avance tecnológico, si bien es cierto estas personas que se aprovechan de las sistemas operativos como son las computadoras, celulares no son detectadas fácilmente o hasta a veces nunca llegan a ser detectadas es por eso que parto de esta premisa

para que nuestros legisladores representantes del pueblo pueda llegar a tomar conocimiento de esta situación que viene sucediendo en nuestro país. La creación de una fiscalía especializada en este delito en la región de Ica y en todas las regiones del Perú se podría combatir más estos tipos de cibercrímenes que cada vez más vienen aumentando. Habría un control más seguro para los operadores de justicia.

Esta fiscalía tendría que contener como mínimo fiscales con experiencia en informática avanzada y capacitarlos anualmente para que logren una constante efectividad al logro de los autores.

Dicha fiscalía también tendría que contener una estructura especial basada en que trabajara en conjunto con el servicio policial. Debe contener todas las máquinas de última generación para hacer el uso efectivo de que la información pueda descargarse completamente.

Así mismo, tendría que contener software de última generación para que los fiscales y los efectivos policiales puedan hacer uso fácilmente y poder controlar de inmediato el acto ilícito cometido.

INCIDENCIA DE LA NORMA SOBRE LA LEGISLACION NACIONAL

Los efectos de la iniciativa legislativa no contravienen norma alguna de nuestro Sistema Jurídico Nacional

LA PROPUESTA SE ENMARCA EN LAS POLÍTICAS DEL ACUERDO NACIONAL

La presente iniciativa legislativa se enmarca en las siguientes Políticas de Estado del Acuerdo Nacional:

Política de Estado N. °01: Fortalecimiento del Régimen Democrático y del Estado de Derecho.

Política de Estado N. ° 08: Descentralización política, económica, y administrativa para propiciar el desarrollo integral, armónico y sostenido del Perú.

Política de Estado N. ° 24: "Afirmación de un Estado eficiente y transparente".

BIBLIOGRAFÍA

- Acurio, S. (2007). *Delitos informaticos, generalidades*. Ecuador: UDGvirtual.
- Aladro, E. (2011). La teoria de la informacion ante las nuevas tecnologias de la comunicacion. *Cuadernos de informacion y comunicacion*, 1-11.
- Almanza, F. (2010). *Teoria del Delito*. Perú: Nomos & Thesis E.I.R.L.
- Arellano, p. (2011). Dolo, Culpa, preterintencionalidad. *Microsoft Word*, 1-23.
- Bacigapuldo, E. (1979). *Teoria del Tipo Penal*. Argentina: Depalma Buenos Aires.
- Budapest. (2001). *Convenio sobre la ciberdelincuencia*. Hungria: Council of Europe.
- chileno, M. d. (1993). Datos. *Ministerio de Justicia Chileno*, 10.
- Decoo, W. (1996). *The induction-deduction opposition: Ambiguities and complexities of the didactic reality*. Alemania: in-chief: Xuesong (Andy) Gao.
- El peruano, D. O. (2013). Ley de delitos Informaticos. *El peruano*, 1-5.
- Folgueiras, P. (2016). La entrevista. *Dipositorio, ub, edu*, 1-11.
- Fuenmayor, L. (junio 2012). *sistema de informacion bago ambiente web para la gestion electronica de documentos*. Venezuela: Universidad privada Rafael Belloso Chacin.
- Helen, A. (2013). Mecanismos jurídicos para el control social. *Slide Share*, 1-8.
- Hermida, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Universidad Nacional de Mar del Plata*, 1-10.
- Machicado, J. (2011). Metodos del Estudio del Derecho. *Apuntes Juridicos*, 1-4.
- Montoya Guillén, F. A. (2017). *Regulación expresa del delito informático de clonación de tarjetas - Sede DIVINDAT*. Lima: Universidad César Vallejo.
- Montoya, F. (2018). *REGULACIÓN EXPRESA DEL DELITO INFORMÁTICO DE CLONACIÓN DE TARJETAS*. Perú, Lima: Universidad Cesar Vallejo.
- Muñoz, F. (2004). *Teoría General del Delito*. Colombia: Temis S.A.

- Pardo Vargas, A. (2018). *Tratamiento jurídico penal de los delitos informático contra el patrimonio. Distrito Judicial de Lima*. Lima: Universidad César Vallejo.
- Peruano, D. E. (2021). Ciberdelitos en el Perú. *El Peruano*, 1.
- peruano, e. (2021). Denuncias sobre los delitos informaticos. *Diario oficial el peruano*, 1-3.
- Plascencia, R. (2004). *Teoria del Delito*. México : D.R.
- Quiroz, R. (2016). El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa. *Scielo*, 1-27.
- Rivera, J. (1995). LA IMPLEMENTACION: UN FENOMENO ORGANIZATIVO. *Departamento de Economia de la Empresa*, 1-24.
- Rodriguez, A. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Escuela de Administracion de Negocios*, 1-27.
- Rodriguez, D. (1990). Análisis de la Ley de Fraude Informatico. *Revista de Derecho de UNAM*, 192.
- Ruiz, D. (2017). *El método deductivo-inferencial y su eficacia en el aprendizaje de la matemática de los estudiantes del primer año de secundaria de la I.E. "José María Arguedas" San Roque – Surco – 2014*. Perú: Escuela de Posgrado de la universidad cesar vallejo.
- Ticona, E. (2012). Teoria de la Tipicidad. *Microsoft Power point*, 1-43.
- Torres, A. (2021). *Patrimonio*. Perú: Instituto Pacífico.
- Valbuena, F. (1997). Teoria de la Informacion. España: Noesis.

ANEXOS

Anexo 1

a) Ficha técnica del instrumento

FICHA TECNICA DEL INSTRUMENTO A UTILIZAR EN ENTREVISTAS A FISCALES Y SU ASISTENTES DEL MINISTERIO PÚBLICO, ABOGADOS, EFECTIVOS POLICIALES, SECRETARIOS JUDICIALES DEL PODER JUDICIAL.

- A) Tema del trabajo de Investigación:** Mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas
- B) Autor:** Giacomo Dario Vitteri Melgar
- C) Universidad:** Inca Garcilaso de la Vega
- D) Nivel Académico:** Pregrado
- E) Materia:** Derecho Penal
- F) Universo y población:** La población residente es de la provincia de chincha-distrito de chincha alta- región de Ica, población dirigida aquellos profesionales con conocimiento en derecho, entre ellos fiscales, asistentes del ministerio público, abogados, secretarios del poder judicial, efectivos policiales.
- G) Tamaño de la muestra:** La muestra diseñada consta de 10 entrevista y en lo que se pudo obtener en un margen se obtuvo 7 hasta la fecha
- H) Tipo de preguntas:** Cerradas y abiertas
- I) Numero de preguntas:** 7

Anexo 2
b) Guía de Entrevista



Universidad
Inca Garcilaso de la Vega

Mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas.

La presente investigación tiene como finalidad recabar su opinión para analizar e implementar los mecanismos jurídicos a la ley 30096 de los delitos informáticos contra el patrimonio

Entrevistado:

Cargo:

Institución:

Breve Resumen curricular:

1. ¿Qué opina usted respecto al avance tecnológico informático y las nuevas modalidades de comisión de delitos informáticos?

.....
.....
.....
.....

2. ¿Considera usted que la Legislación sobre los Delitos informáticos es efectiva para sancionar las nuevas modalidades delictivos con el uso de la nueva tecnología?

.....

.....

.....

.....

.....

3. ¿Es factible que las personas como las empresas privadas o públicas están expuestas a ser víctimas de fraude informáticos?

.....

.....

.....

.....

.....

.....

4. ¿Considera usted necesario una reforma legislativa para prevenir los delitos informáticos contra el patrimonio?

.....

.....

.....

.....

.....

.....

5. ¿Considera usted que debería crearse una fiscalía especializada en delitos informáticos para lograr una efectividad en la aplicación de los delitos informáticos- Ley N° 30096 Ley de delitos informáticos?

.....

.....

.....

.....

.....
.....

6. ¿Respecto a su profesión y su experiencia laboral se logra identificar al autor de la comisión de un delito informático?

.....
.....
.....
.....
.....
.....

7. ¿Considera usted que es de suma importancia tocar este tema más si estamos pasando este momento en nuestra sociedad con la evolución de la tecnología?

.....
.....
.....
.....
.....
.....

B) Anexo 3

c) Matriz de consistencia

<u>PROBLEMA</u>	<u>OBJETIVO</u>	<u>HIPOTESIS</u>	<u>VARIABLES</u>	<u>METODOLOGIA</u>
¿Cuáles son los mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas?	<p>GENERAL</p> <p>Determinar los Mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas</p>	Los Mecanismos jurídicos para implementar la ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas.	<p>Variable Independiente</p> <p>Los Mecanismos jurídicos para implementar la ley 30096</p> <p>Variable Dependiente</p> <p>En los delitos informáticos contra el patrimonio</p>	<p>Tipo de investigación</p> <p>La presente Investigación es Aplicada o lege ferenda ya que se busca proponer la creación de un ministerio publico especializada en delitos informáticos</p> <p>Enfoque</p> <p>Esta investigación es de enfoque mixto, el cual consiste en la realización de prácticas interpretativas que conduce a describir, analizar y discutir el fenómeno objeto de estudio a través de entrevistas, conversaciones, recurriendo a fuentes documentales</p> <p>Diseño de la Investigación</p> <p>Población</p> <p>La población motivo de esta investigación está conformada por un total de 30 personas entre ellos fiscales, abogados y efectivos policiales del distrito de chincha alta</p> <p>Muestra</p> <p>La muestra utilizada de la fuerza social en la presente investigación, aplicando el muestreo no probabilístico por conveniencia, está conformada por un total del 50 % personas del distrito de chincha alta</p> <p>Técnicas</p> <p>Entrevista</p> <p>Instrumentos</p> <p>Cuestionario de preguntas.</p>
	<p>OBEJTIVOS ESPECIFICOS</p> <p>✓ Analizar las nuevas tecnologías informáticas frente a los delitos contra el patrimonio</p> <p>✓ Establecer la regulación de los informáticos en el derecho comparado</p> <p>identificar las causas por las cuales las nuevas modalidades de ciberdelincuencia en los delitos contra el patrimonio no son detectadas por los sistemas informáticos peruanos.</p> <p>✓ Establecer el procedimiento fiscal y judicial que se adopta en los delitos informáticos contra el patrimonio</p> <p>✓ Proponer la creación de una fiscalía especializada en delitos informáticos para lograr una mayor efectividad frente a la comisión de delitos informáticos.</p>			