UNIVERSIDAD PRIVADA TELESUP

FACULTAD DE DERECHO Y CIENCIA SOCIALES

ESCUELA PROFESIONAL DE DERECHO CORPORATIVO

TESIS

"VACIOS LEGALES QUE IMPIDEN LA APLICACION DE SANCIONES POR DELITOS INFORMATICOS EN LA LEY N° 30096 Y MODIFICATORIA EN EL DISTRITO CERCADO LIMA 2017"

PARA OBTENER EL TITULO PROFESIONAL DE:

ABOGADO

AUTOR:

Bach. JOHNNY EFRAIN LEON CORDOVA

LIMA - PERU

2018

ASESOR DE TESIS

……

Dr. JUAN HUMBERTO QUIROZ ROSAS

JURADO EXAMINADOR

……

Dr. PERALES SANCHEZ ANAXIMANDRO ODILIO

Presidente

……..

Dr. FERNANDEZ MEDINA JUBENAL

Secretario

……

Dr. DIAZ VIVAR VICTOR RAUL

Vocal

DEDICATORIA

Este trabajo ha sido elaborado con la consigna de darles el mayor orgullo posible a mis padres que en todo momento han apostado por mí y me ha apoyado incondicionalmente. Y a Dios, por la fuerza y determinación que me regalado para concretar mis metas. A él amor y la gloria.

AGRADECIMIENTO

Los más sinceros agradecimientos a cada docente que me ha formado y guiado en el trasegar del derecho, a quienes, en todo momento, trato de inmolar y seguir paso a paso para ser el profesional que esperan. Asimismo, a mi casa universitaria, por la oportunidad de abrirme las puertas de sus claustro.

DECLARACIÓN DE AUTENTICIDAD

Yo, Johnny Efraín León Córdova, debidamente identificado con DNI N°07682478 con domicilio en Av. Aviación 3367 Dpto 105 San Borja **DECLARO BAJO JURAMENTO** que todos los datos e información presentados en este trabajo de tesis son auténticos y veraces, como también que los pensamiento e ideas de otros autores han sido citados y referenciados según corresponden.

En ese sentido, suscribo la presente en señal de conformidad con mi firma y huella digital.

Lima, 26 de Agosto de 2018.

Johnny Efraín León Córdova
D.N.I. N° 07682478

HUELLA

RESUMEN

Este trabajo de tesis nació de la necesidad de entender las consecuencias del paso de los años y del propio desarrollo de las tecnologías ya que esto ha servido de base para las nuevas formas criminales de ciber delitos. Es así que, pese a la creación de leyes especiales o modificatorias de las mismas, tales como la Ley N° 30096 “Ley de delitos informáticos” y la Ley N° 30171 “Ley que modifica la anterior”, se tiene claro que dichas inconductas repercuten en otros bienes jurídicos protegidos por las normas tales como el patrimonio, libertad sexual, intimidad, entre otros, y no sólo ello, sino que, tanto los operadores de justicia como los legisladores, deben luchar día a día con los avances y sus actualizaciones ya que, muchas veces, los sujetos que se encuentran detrás de la comisión de los ilícitos, se respaldan en que las leyes no los alcanzan por no haber estado tipificadas como ilegales las actividades que vienen realizando con la adquisición de nuevas tecnologías, quedando fuera del alcance de las sanciones previstas.

PALABRAS CLAVE: Delitos informáticos, Ley 30096, Ley 30171, vacíos legales, ciber delitos, tecnología.

ABSTRACT

This thesis work was born of the need to understand the consequences of the passage of time and the development of technologies, since this has served as the basis for the new criminal forms of cyber crimes. Thus, despite the creation of special laws or amendments to them, such as Law No. 30096 "Law on computer crimes" and Law No. 30171 "Law that modifies the previous", it is clear that such misconduct they affect other legal rights protected by the norms such as the patrimony, sexual freedom, privacy, among others, and not only that, but, both the justice operators and the legislators, must fight day by day with the advances and their updates since, often, the subjects that are behind the commission of the illicit ones, support themselves in that the laws do not reach them because they have not been classified as illegal the activities that they are carrying out with the acquisition of new technologies, being outside the scope of the sanctions provided.

KEYWORDS: Computer crimes, Law 30096, Law 30171, legal gaps, cyber crimes, technology.

INDICE DE CONTENIDOS

GENERALIDADES

Título: “Vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 y modificatoria en el distrito Cercado Lima 2017”

Autor: Johnny Efraín León Córdova

Asesor: Dr. Juan Humberto Quiroz Rosas

Tipo de investigación: Cualitativa, Básica, No experimental.

Línea de investigación: Derecho Penal, Derecho Informático

Localidad: El presente trabajo de investigación se ha realizado en Lima, específicamente en la Universidad Privada Telesup ubicada en La Avenida 28 De Julio Nº 1050 - 1052 - 1056 - 1062 - 1068 - Urb Santa Beatriz –Cercado de Lima. Así como también en el domicilio del investigador, sito en Av Aviacion 3367 dpto 105 San Borja
Lima-Perú.

Duración de la investigación: 6 - 9 meses

INTRODUCCIÓN

En estos tiempos, las personas se ven involucradas, de una u otra forma, en alguna actividad que se desarrolle mediante el uso de aparatos electrónicos y tecnológicos, ya sean en la vida diaria, en el trabajo, al concurrir a alguna institución pública, al momento de estudiar, etc., a fin de obtener beneficios de mejoras, rapidez y efectividad.

Lo lamentable de estos avances es el hecho de la existencia de aquellas personas que, de una forma despreciable, se apoyan en ellos para cometer delitos en contra de otras personas (naturales o jurídicas) o del estado, denominados ciber delitos, por lo que algunos países se encontraron obligados y necesitados de tipificar en códigos las conductas ilícitas y sancionarlas a través de sus legislaciones internas y decisiones políticas, pero que muchas veces quedan desfasados ya que los avances tecnológicos son constantes y no se detienen, lo que ocasiona que los delitos también avancen a la par.

En ese sentido, se creyó conveniente enfocar este trabajo desde diferente áreas o aristas tales como conceptualización de términos técnicos, aspectos legales, formas de combatir el cibre crimen, comentarios o apreciaciones de operadores de justicia, con la tendencia a encontrar aquellos vacíos legales en las normas especiales sobre Delitos Informáticos, que impiden sus respectivas sanciones y que generan la impunidad de los mismos, para ello se requiere analizar la tendencia de los mismos y una vez identificados, podremos realizar acciones para combatir estas conductas ilícitas en favor de la sociedad.

Finalmente, esta investigación presenta las conclusiones sobre el estudio realizado, comentarios, resultados y referencias bibliográficas tomadas en consulta.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Aproximación Temática

Es conocido que el hombre, al ser un ser social, necesita comunicarse constantemente con su entorno, razón por la cual, a través del tiempo, ha buscado la forma de realizar esta actividad de manera más dinámica, rápida y efectiva por lo que, en la lucha diaria de encontrar mecanismos que faciliten su labor, ha logrado desarrollar tecnologías que constantemente se vienen modificando y que permiten acceder a conocimientos con hacer un solo clic, por ejemplo.

A veces se olvida que las primeras herramientas rudimentarias elaboradas por nuestros antepasados ya eran tecnología porque forma parte de un conjunto de instrumentos destinados a la resolución de un problema concreto o específico presentado en la vivencia del hombre, sino que también sirven de medio para obtener información, de medio de comunicación, entre otros.

Tal es la trascendencia de la tecnología e informática que se podría hablar de un Poder Social nuevo por la capacidad de procesamiento y almacenamiento de información que viene desarrollando, por lo que dichas herramientas, en la actualidad, se han convertido en los medios o sistemas electrónicos, cibernéticos y/o mecánicos que conocemos y que, al estar en constante cambio o actualización, se escapan de las regulaciones jurídicas a nivel mundial, lo que ocasiona que muchas veces la forma de comisión de ilícitos penales se tecnifiquen y queden fuera del marco normativo porque simplemente la justicia o personal de investigación desconoce la forma de afrontarlos y conducirlos.

Al respecto, doctrinariamente también se ha tratado este tema, tal es así que Tiedemann considera que con la expresión “criminalidad mediante computadoras”, se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

Asimismo, Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.

Habiendo mencionado lo anterior, podemos apreciar que existen, determinados enfoques doctrinales sobre el delito informático, y que, a su vez, se convierte en un delito pluriofensivo, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general.

Dentro de nuestro territorio y realidad tenemos lo previsto en el literal a) del inc. 24 del art. 2° de la Constitución Política del Perú, el cual señala “Nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe”. Esto quiere decir que si al momento en que se ha realizado una actividad que tiene consecuencias delictivas, tales como los nuevos delitos informáticos, y no se encuentran tipificados en el código penal vigente al momento de su comisión, el sujeto activo no tiene ninguna limitación para no hacerlo, tal y como también señala nuestra Carta Magna en el literal d) del inc. 24 del art. 2°, el cual indica que “Nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté previamente calificado en la ley, de manera expresa e inequívoca, como infracción punible; ni sancionado con pena no prevista en la ley”.

Partiendo de lo anterior, es bueno tener presente que el código penal tiene como base fundamental el estricto cumplimiento del Principio de Tipicidad, el cual señala que, para que una persona pueda ser imputada por la comisión de dicho delito, debe estar expresamente contenido en la ley. Asimismo, dicho código sustantivo

data del año 1991 y a la fecha han transcurrido 27 años aproximadamente, lo que motivó que en el año 2013, a fin de contrarrestar los vacíos normativos respecto a delitos informáticos, el parlamento expidió la Ley N° 30096, la cual fue denominada "Ley de los Delitos Informáticos (2013)", pero nuevamente, tras los avances tecnológicos, los tipos penales cayeron en el círculo vicioso de los vacíos legales por lo que una vez se tuvo que emitir un cuerpo normativo capaz de protegernos de las contingencias que podrían ocasionarte, bajo ese orden estricto de ideas se promulgó la Ley Nº 30171, denominada "Ley Modificatoria de la Ley de Delitos Informáticos (2014)".

La ciberdelincuencia, lamentablemente, nos lleva unos pasos de ventaja, por lo que la dación de leyes no sólo debe ser el único mecanismo para poder resolver el inconveniente presentado por los vacíos legales porque, queramos o no, nuevamente retornamos al punto de inicio en el que precisamos que lo que no está prohibido se está permitido y no se puede procesar ni sancionar a nadie por un delito que, al momento del hecho ilícito, no se encontraba previsto en la legislación, lo cual también genera controversia y polémica porque hay quienes creen que al regular dichas conductas también se limitan derechos fundamentales como el acceso a la información, libertad de expresión, entre otros, por colisionar con la Constitución Política (norma de mayor rango) y es muy probable que esta realidad también sea enfrentada por otros países.

En el proceso penal no puede incoarse la acción penal con una finalidad genérica ni perseguir eternamente la posible criminalidad o los posibles comportamientos criminales en el seno de un grupo social lo que significa que, está prohibida la "inquisitogeneralis", o sea, la iniciación de una pesquisa o investigación general. Como quiera que el objeto del proceso penal está conformado por un hecho (acción u omisión), es pues, necesario e imprescindible que se afirme el hecho, debidamente definido, con indicación de sus circunstancias precedentes, concomitantes y posteriores, lo que a su vez, es una exigencia del derecho de defensa, de la cosa juzgada y, en general, del principio de seguridad jurídica.

La legislación sobre protección de los sistemas informáticos ha de procurar acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

Asimismo, podemos señalar algunos rasgos o características propias de los delitos informáticos, pues estos se desenvuelven en el sistema económico y en contextos sociales. Es muy probable que en los medios de comunicación hayamos escuchado escasamente, o en todo caso nunca, que las entidades financieras hayan denunciado ser víctimas de este tipo de delincuencia pues lo que buscan siempre es mantener la alta imagen y prestigio que los caracteriza para evitar generar un ámbito de desconfianza en sus usuarios, por ejemplo. En otros casos suelen tomarse denuncias anónimas o bajo circunstancias ajenas al hecho de querer denunciar.

Este tipo de ilícitos, hablando desde un punto económico, genera una gran rentabilidad pues se manejan cifras cuantiosas y más cuando estos a su vez generan efectos en terceras instituciones pese a que muchas ocasiones el modus operandi resulte ser por pequeños importes pero que en bloque suman una

cantidad considerable. He aquí los serios inconvenientes que se presentan para la administración de justicia respecto de cuál es la norma aplicable para el caso concreto, y cuál será su correcta interpretación judicial.

Entonces ¿qué contribuye a la comisión de este tipo de delitos? La respuesta resulta obvia pero mientras no se tomen cartas en el asunto seguiremos vulnerables a aquellos delincuentes que buscan tener ventaja sobre nosotros utilizando la misma tecnología que nos facilita la vida para encargarse de efectuar algún tipo de agravio en nosotros. Es necesario también contar con controles especializados que permitan perseguirlos, combatirlos y prevenirlos tal y como ha logrado Estados Unidos al crear a la Policía Informática que es el personal investigador por excelencia para poder reunir los medios de pruebas suficientes y pertinentes que la situación amerita.

Impacto*:* "En los años recientes, las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995. A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, la trata de niños con fines pornográficos. Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en «paraísos informáticos» - o sea, en países que carecen de leyes o experiencia para seguirles la pista -. Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números

de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU" (Herrera, 2010, p. 79)

En virtud a lo anterior y a modo de cierre, es necesario poder identificar cuáles son esos vacíos legales que sirven de argucias a los ciber delincuentes para que el derecho penal no los alcance, permitiendo acoplar y modificar a la actualidad dichos tipos penales y lograr una efectiva sanción por la criminalidad que atenta contra el desarrollo del país y la economía, desde un punto de vista macro, pero que a la vez suelen atentar contra bienes jurídicos propios de la persona humana.

1.1.1. Marco Teórico

1.1.1.1. Antecedentes de la Investigación

1.1.1.1.1. Antecedentes Nacionales

Es necesario precisar que este tema de investigación no es nuevo, es más, diversos profesionales del derecho, al momento de optar por el título de la carrera, decidieron abarcar esta materia con la sola consigna de disminuir el riesgo de implicarse las sanciones correspondientes. De otro lado, normalmente se tiene la disyuntiva de determinar si la comisión del delito informático ha sido parte de los actos preparatorios para la comisión de otros tipos penales o si este ha de subsumir las inconductas, ya que, de ser así, se tendría que ampliar la gama de delitos o modificar los ya vigentes a fin de contenerlos en ellos.

En investigaciones realizadas en el Perú se tiene la problemática que los delitos informáticos tienen su radio de acción principalmente en delitos tipificados en nuestro código penal vigente, tales como los atentados contra los derechos de

autor, violación de la intimidad personal, falsificación de documentos informáticos, entre otros, vulnerando considerablemente otros derechos fundamentales de la persona a través del mundo cibernético.

Podemos indicar, sin caer en el error, que a mayor diversificación de las formas de acceder a la tecnología e informática, más peligros corremos y estamos expuestos a las nuevas tendencias. Es una clase de razón de proporcionalidad que se maneja. Es así que Villavicencio (2014) indica que “el desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet” (p. 285).

Un tema latente con el que constantemente nos enfrentamos es el anonimato del ciber delincuente, ya que se escudriña detrás de un aparato electrónico y que muchas veces es manipulado para ocultar la ubicación, el IP o la propia identidad del sujeto activo, lo cual también dificulta el proceder de las autoridades. Esto también es de conocimiento de Ticona, quien indica que “aunque la mentira es una posibilidad inherente en la comunicación humana, internet ha favorecido que cualquiera pueda crear un contenido falso en la red. Por otra parte, internet ha propiciado nuevas formas de sociabilidad y de experimentación en los más jóvenes, entonces el trabajo respecto a este tema, puede que en la red social con mayor cantidad de suscritos, están creando identidades falsas para poder cometer delitos informáticos a través de las redes sociales” (Ticona, 2015, p. 7-14).

No obstante a ello, nuestros legisladores, en su afán de tratar de protegernos de la realidad en la que estamos, ha perseguido la mejor manera de regular y penar estos delitos pero, por la progresión de los mismos, se han vuelto un tanto deficiente las leyes dadas, por lo que han caído en vacíos legales que prácticamente permiten que los delincuentes queden libres de todo tipo de responsabilidad, lo cual debe ser subsanado lo más antes posible e impedir que la inseguridad ciudadana aumente considerablemente.

“Quizás somos el país con mayor cantidad de normativa que incide sobre temas de Sociedad de la Información, en especial ligada a Internet (…) por desarrollos normativos que han ido apareciendo, pero enfrentados a un problema de desorganización institucional (de entidades responsables) así como de alcances normativos (en las normas mismas) (…) viene la tendencia a que si es un espacio nuevo debería tener una legislación propia de manera completa, dado que la legislación fuera de la red no le alcanzaba. (…) mucha de la legislación vigente era aplicable a la red, pero que habían temas no regulados fuera de la red (Iriarte, 2012, 169). Entonces, Iriarte se estaba refiriendo a los vacíos que se encuentran en la legislación.

Para Sequeiros (2016) tiene como objetivo “determinar qué vacíos legales en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015” (p. 6). Concluyendo que “dada la naturaleza virtual de los delitos informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área” (p. 44).

Esto a su vez ha generado en otras ramas del derecho o actividades empresariales que los usuarios desconfíen de los mecanismos de seguridad que las empresas les brindan. Es así que Gil (2009), sostiene que “para hablar del Comercio Electrónico como eficiente es elemental abordar los temas de seguridad y privacidad. Mientras no existan garantías al respecto, tanto a nivel tecnológico como legislativo, seguirá existiendo aversión por parte de los consumidores de realizar operaciones por medios electrónicos” (p. 7).

En la actualidad vivimos en una inseguridad al estar expuestos expuestos por este tipo de crímenes. Una causa podría ser que “en la doctrina no hay uniformidad acerca de la clasificación, los criterios tomados para su agrupación son legalistas, técnicos o simplemente arbitrarios, lo que nos da entender que no hay seguridad

en los expertos en lo que se quiere estudiar y el cómo estudiarlo, esta ausencia denota la importancia de dotar de un estudio dogmático deslegitimador a los delitos informáticos" (Espinoza, 2017, p. 77).

1.1.1.1.2. Antecedentes Internacionales

Como ya hemos señalado en párrafos anteriores, este tema no es nuevo y no es ajeno fuera de las fronteras nacionales. Existen diversas investigaciones realizadas a nivel internacional sobre el tema en concreto o relacionados puesto a que los delincuentes están a la vanguardia de la tecnología día tras día, más aún que se están vulnerando otros bienes jurídicos que se encuentran fuera de las normas especiales pero que, por el solo uso de mecanismos tecnológicos e informáticos, se encuentran subsumidos en el tipo penal antes mencionado.

En Nicaragua, Rodríguez, Flores y Berríos (2014) sostienen que los efectos de "el desarrollo de la tecnología informática ha sido la aparición de una gama nueva de actos que por el dolo que los caracteriza y los perjuicios que causan, se han denominado Delitos Informáticos" (p. 121).

Unos investigadores Colombianos también han manifestado su pesar respecto a cómo se vienen desarrollando impunemente los delitos por intermedio de medios informáticos, tales como el hurto. Tal es así que "los delincuentes informáticos se han especializado principalmente en el hurto a través de medios informáticos, siendo este el delito informático de mayor ocurrencia en todo el territorio, y a lo cual no ha escapado la ciudad de Cúcuta, donde los ciudadanos también se han visto afectados por esta modalidad delictiva en los últimos años" (…)También señalan que "el bajo índice de capturas por este delito, responde a varios factores dentro de los cuales se destacan la falta de investigadores especializados en delitos informáticos por parte de la Fiscalía y la Policía que permitan hacer seguimientos en este campo a los delincuentes, a fin de lograr su captura, y posterior judicialización" (Granados y Parra, 2016, p.13 y 14).

Por ejemplo, en Bolivia tenemos a Terán (2015), quien señala que “la falta de tipificación de conductas delictivas en el área informática (…) imposibilita una calificación jurídico legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos” (p. 54).

Esta misma realidad encontramos en Costa Rica, Lemaitré (2014) refería que en su país “el sujeto activo contemplado en el tipo penal sólo vislumbra personas físicas, no contemplando personas jurídicas, lo cual en un contexto como el actual es un vacío grave”(p. 112), lo que conllevaba a la impunidad de los ciberdelitos, repitiéndose la misma historia que en otros países.

En Ecuador también existen investigadores al respecto, quienes han enfocado el tema desde la óptica del sujeto activo, ya que al emplearse tecnologías, la hipótesis radica en que tienen un acceso a educación y estatus económico mayor para poder implementar su red criminal.

Este es el caso de Herrera (2016) quien indica que “a estos sujetos no es fácil descubrirlos y sancionarlos, precisamente por el poder económico que ostentan, de ahí que las medidas represivas, en muchos casos no resultan efectivas y, por tanto, estos delitos pueden quedar en la impunidad" (p. 78). Además agrega que “la desconfianza que existe en las autoridades responsables de sancionar estos delitos, pues la ineficiente preparación para comprender, investigar y aplicar el tratamiento jurídico adecuado, hace que las víctimas, prefieran dejar el ilícito en la impunidad, antes de invertir tiempo, recursos y energías en una labor que bien saben, no tendrá éxito”(p. 84).

México no se queda atrás, Reyes y Fernández (2014) sostienen que “a medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho” (p. 22).

1.1.1.2. Bases Teóricas de las Categorías

1.1.1.2.1. Bases Legales

Partiendo de la pirámide de Kelsen, la Constitución Política del Perú (1993) nos da una gama de derechos fundamentales que se ven conculcados por los delitos informáticos de manera directa o indirecta, sin impedimento alguno más aún si contamos con el derecho a la información, a la libertad de creencia, de expresión, etc.

A nivel interno, hemos tenido regulación penal sobre el tema materia de investigación desde el año 1991 con la promulgación del Código Penal (vigente), pero enfocó la problemática de un punto más patrimonial, forzando muchas veces los tipos con la finalidad de hacerlos calzar en las conductas nuevas de ciber criminalidad, se creyó conveniente incluirlo dentro de las modalidades descritas por el artículo 186 del Código sustantivo, para ser preciso en el inciso 3 del segundo párrafo del mismo, el cual indicaba que el hurto también se configuraba “mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas”.

Posterior a ello, al ver que sólo se atacaba ciertas conducta y otras quedaban impunes, se incorporó el Capítulo X en el Código Penal, con los artículos 207°-A (interferencia, acceso o copia ilícita contenida en base de datos), 207°-B (alteración,

daño o destrucción de base de datos), 207°-C (circunstancias calificantes agravantes), 207°-D (tráfico ilegal de datos), y en las leyes penales especiales.

La ley N° 30096, Ley de Delitos Informáticos, publicada en el Diario Oficial El Peruano el 22/10/2013, en su artículo 1° indicaba que “La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciber delincuencia”.

Sin embargo, esto no fue suficiente por lo que, mediante la Ley N° 3017“Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos”, publicada en el Diario Oficial El Peruano el 10/03/2014 se persiguió el fin de adecuar nuestras normativa con lo establecido por el Convenio sobre la Ciber criminalidad (en adelante convenio de Budapest), al incorporar en la redacción los artículos 2, 3, 4, 7, 8 y 10.

Las modificaciones efectuadas a través de la Ley Nº 30171, son las siguientes:

- Art. 1°.- Modificación de los artículos 2°, 3°, 4°, 5°, 7°, 8° y 10° de la Ley N° 30096 Ley de Delitos Informáticos.

- Art. 2°.- Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley N° 30096 “Ley de Delitos Informáticos”.

- Art. 3°.- Incorporación del artículo 12° a la Ley N° 30096 “Ley de Delitos Informáticos”.

- Art. 4°.- Modificación de los artículos 158°, 162° y 323° del Código Penal.

- Art. 5°.- Incorporación de los artículos 154°-A y 183°-B del Código Penal. - Única Disposición Complementaria Derogatoria.- deroga el artículo 6° de la Ley N° 30096 “Ley de Delitos Informáticos”.

A nivel internacional podemos iniciar señalando a la Ley N° 1273, del 05 de enero de 2009, mediante la cual se modifica el Código Penal Colombiano, creando un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos”, teniendo como punto de partida el tipificar conductas que vayan en contra del adecuado manejo de datos personales y otras tantas que atenten contra el patrimonio de terceros, como en el caso de los clonadores de tarjetas de crédito o débito.

Según Informática Forense (2017) durante el año 2007 las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos en Colombia. Ante tal situación, es que los legisladores ven la necesidad de agregar a su Código Penal el Título VII BIS denominado "De la Protección de la información y de los datos" que trata este tema en 2 puntos: a) “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”; y, b) “De los atentados informáticos y otras infracciones”.

España no se quedó atrás y también a muy temprana edad, promulgó la Ley Orgánica 10/1195 de 23 de noviembre de 1995, se adelantó a los acontecimientos tecnológicos, sancionando cualquier actividad delictiva mediante el uso de la informática y tecnología. Asimismo, el Tribunal Supremo, al confirmar la prisión para una casa de *phishing,* señaló que “en una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación informática, no es preciso la concurrencia de engaño alguno por el estafador. Ello es así porque la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero” (Recurso N° 2249/2006; Resolución N° 533/2007, 2007).

México ha previsto sancionar a aquellos delitos en los que versen la revelación de secretos y acceso ilícito a sistemas y equipos de informática protegidos por mecanismos de seguridad, que estén considerados o pertenezcan al sistema financiero o al mismo Estado. Esto se encuentra en el Capítulo I y II del Título Noveno del Código Penal Federal.

Por ejemplo, el Artículo N° 167, Fracción I, del Código Penal Federal, sanciona con pena privativa de libertad y pena de multa al que, intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

Venezuela inició su batalla legal contra los ciber delincuentes tratando de erradicar los atentados contra los sistemas informáticos mediante la creación de la Ley Especial contra Delitos Informáticos del 30 de octubre de 2001, la cual tipifica 5 delitos de la materia, tales como: Los que van en Contra los sistemas que utilizan tecnologías de información; contra la propiedad; contra la privacidad de las personas y comunicaciones; contra los niños y adolescentes; y contra el orden económico.

Mediante Asamblea Legislativa, en El Salvador se promulgó el Decreto N° 260, denominado “Ley Especial contra Delitos Informáticos y Conexos” (Diario Oficial de la República de El Salvador en la América Central, tomo Nº 410, número 40 del viernes 26 de febrero de 2016), indicando en el Artículo 1° el objeto de la misma, la que a la letra dice: “La presente Ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley”.

Esto se debe a que, los delitos previstos en el Código Penal de la región, no alcanzaba a aquellos que se realizaban a través de medios informáticos y tecnológicos, razón por la cual era imposible su persecución y sanción.

1.1.1.2.2 Bases Teóricas

Delitos informáticos:

Al respecto, hemos indicado innumerable veces en este trabajo de investigación que, con el crecimiento vertiginoso de la tecnología, han ido modificándose y aumentando los ciber delitos, tanto así que muchas veces las leyes vigentes no pueden regular las inconductas y mucho menos aplicar sanciones por el perjuicio ocasionado en desmedro de los bienes jurídicos tutelados, muchas veces manipulando información, interceptando redes, rompiendo seguros de sistemas, clonando tarjetas de crédito o débito, entre otros.

Brizzio (2000), dice que “el crimen informático puede incluir delitos habituales como el fraude, el robo, chantaje, falsificación y el desfalco de patrimonios públicos en los que los ordenadores y redes han sido empleados como medios”. En cambio, Santivañez (2015) le da una connotación más fuerte al señalar que “el delito informático es un delito cuya arma letal es una computadora o elemento electrónico, o componentes-instrumentos que acompañen al elemento en sí, el mismo que permitirá al usuario perpetuar aquella conducta punible como si se tratase de un delincuente común” (p. 226).

Característica del ciber delito:

Este tipo de delito tiene características muy exactas y propias que permiten, en cierta forma, entender la forma de actuar y de pensar del ciber delincuente. Al respecto, Téllez (1996) indica que:

“Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

En su mayoría son imprudenciales y no necesariamente se cometen con intención.

Ofrecen facilidades para su comisión a los menores de edad.

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley".

Delitos tipificados en la Ley N° 30096 (Ley de Delitos Informáticos):

Delitos contra datos y sistemas informáticos (Capítulo II): Este capítulo está conformado por tres artículos, siendo los siguientes: Art. 2º (acceso *ilícito*), Art. 3º (*atentando a la integridad de datos informáticos*) y Art. 4º (*atentando a la integridad de sistemas informáticos*).

Art. 2º.- "*El que deliberada e ilegítimamente accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.*

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

Este tipo penal se consuma al momento de vulnerar las medidas de seguridad previstas para no permitir el acceso a la data o información, para lo cual debe ser vulnerado o quebrantado. Pero qué pasa si he ingresado ilegítimamente al sistema o base de dato como un correo electrónico porque simplemente conozco la contraseña y he decido ingresar para conocer la información confidencial que contiene. ¿Estaríamos cometiendo este delito?

Art. 3º.- "*El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa*".

Para entender esta figura penal debemos precisar en qué consiste cada verbo rector que lo comprende. Dañar (perjuicio, detrimento), introducir (ingresar algo en un lugar), borrar (quitar, desaparecer), deteriorar (menoscabar), alterar (modificar algo), suprimir (desaparecer parte o el total de algo) y hacer inaccesible los datos informáticos (esto a través de tecnologías de la información y comunicación). Si se realizan dichas acciones, se comete el delito.

Art. 4º.- *"El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su*

funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Este delito sanciona las conductas deliberadas e ilegítimas, consumándose el delito cuando se impide el acceso o el funcionamiento del sistema informático deja de funcionar porque se ve entorpecido.

Delitos informáticos contra la indemnidad y libertad sexuales (Capítulo III): Este capítulo está conformado sólo por el **Art. 5º** (*proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos*), que sanciona la propuesta sexual a niños, niñas y adolescentes utilizando los medios tecnológicos.

Art. 5º.-"*El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo36° del código Penal".*

Este delito se configura cuando aquel que contacta a un menor de edad con la sola consigna de obtener de él material pornográficos o para tener acceso carnal con él mismo o actos contra el pudor. Cabe señalar que el legislador ha hecho precisiones respecto a las edades de los sujetos pasivos (los menores), sin embargo, lo problemático de la redacción del tipo penal es que se rige al solo contacto con el menor sin importar si obtiene o no el material pornográfico o accede a tener actividad sexual, por lo que, si en caso una pareja de enamorados, uno mayor de

edad y otro menor, tuvieran conversaciones por redes sociales en que el primero le solicite fotos íntimas, se estaría configurando este tipo sin mayor miramiento.

Delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV): Este capítulo está conformado sólo por el **Art. 6º** (el cual fuera derogado De rogado por la ley 30171 Ley que Modifica la Ley 30096, Ley de Delitos Informáticos*)* y por el **Art. 7º** (interceptación de datos informáticos).

Art. 7º.-"El que deliberadamente e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.

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

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

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

El artículo menciona agravantes en su redacción que al ser estudiadas con detenimiento, podemos comprender lo que el legislador pretendió instaurar.

- El primer agravante, cuando la interceptación recaiga sobre información clasificada como secreta, reservada o confidencial, según lo dispuesto por la Ley 27806, Ley de Transparencia y Acceso a la información Pública.

- El segundo agravante, cuando la interceptación sea dirigida contra información que compromete a la defensa, seguridad o soberanía nacional.

- La tercera agravante, cuando el agente integra una organización criminal, comete el delito.

Entonces, se tiene que este tipo se configura con la sola interceptación de datos informáticos.

Delitos informáticos contra el patrimonio (Capítulo V): Este capítulo está conformado sólo por el **Art. 8º** (fraude informático).

Art. 8°.-"El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

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

Un requisito de configuración del delito es que no sólo se realicen las acciones señaladas sino que también se obtenga un provecho para uno mismo o un tercero.

Delitos informáticos contra la fe pública (capítulo VI): Este capítulo está conformado por el **Art. 9º** de la ley (suplantación de identidad).

Art. 9°.- "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

Nuevamente nos encontramos con un tipo penal que no sólo se basa para sancionar en el hecho de realizar las acciones descritas sino que se genere un perjuicio con esa conducta. Una interrogante sería si, el hecho de crear cuentas falsas en redes sociales con el nombre de un tercero, se configuraría este delito.

Disposiciones comunes (Capítulo VII): Este capítulo está conformado el **Art. 10º** (abuso de mecanismos y dispositivos informáticos) y el **Art. 11º** (agravantes).

Art. 10°.-"El que deliberadamente ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa".

Hasta cierto punto podemos decir que es un artículo numerus apertus porque lo que busca es trascender más allá de lo establecido en la ley. Lo interesante es que señala en el mismo texto que será sancionada toda actividad tendenciosa y previa para la comisión de cualquiera de los otros delitos antes mencionados, tratando de

salvar, de una forma, cualquier circunstancia que pudiera desencadenar en un futuro delito pero hasta dónde se podría llegar a reprimir dicha conducta.

Art. 11º.- “El juez aumenta la pena privativa de libertad hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley, cuando:

1. El agente activo integra una organización criminal.

2. El agente tiene posición especial de acceso a la data o información reservada.

3. El delito se comete para obtener un fin económico.

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

Según este artículo, se faculta al juez para que aumente la pena hasta en un tercio por encima del máximo legal fijado.

Art. 12º.-“Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito del levar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos”.

Este artículo fue incorporado por el Art. 3º de la Ley Nº30171 “Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos”, publicado el 10 de marzo del2014. Con el texto del artículo se exime de responsabilidad penal a toda persona que realiza alguna de las conductas reguladas en los artículos 2º, 3º, 4º y 10º de la Ley N° 30096.

Una vez estudiado los artículos precedentes de la ley, es momento de mencionar a las disposiciones complementarias finales en donde también se encuentran sanciones para personas jurídicas, tales como:

DÉCIMA.- "La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5del artículo 235° del Código Procesal Penal, aprobado por Decreto Legislativo 957.

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

La Superintendencia de Banca, Seguros y AFP determina la escala de multa de acuerdo a la característica, complejidad y circunstancias en las que las empresas, que se encuentran bajo su alcance, omitan una orden judicial respecto a la obligación de entregar la información correspondiente a la orden judicial de levantamiento del secreto bancario.

UNDÉCIMA.- "El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230° del Código Procesal Penal, aprobado por Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes

sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente."

El Organismo Supervisor de Inversión privada en telecomunicaciones también establece la escala de multas a las empresas bajo su supervisión que incumpla la obligación de posibilitar la diligencia judicial de intervención, grabación o registro de las comunicaciones y telecomunicaciones.

Convenio de Budapest (2001):

También conocido como "El Convenio de la Ciberdelincuencia".

Díaz (2010) señala que es "la mayor maximización de la cooperación en materia de delitos informáticos existente hoy en día en el plano internacional. En efecto, se trata del primer y único instrumento internacional existente hasta la fecha en esta materia, y su auténtica importancia se hará manifiesta a lo largo de este capítulo. Referente a los Estados que forman parte del mismo, a día de hoy tan sólo treinta Estados han ratificado el Tratado, de un total de cuarenta y seis firmas" (p. 195).

"El Convenio de Budapest, contiene disposiciones sobre material penal, procesal y de cooperativa internacional para sus actuales 54 países miembros. Una de las principales limitaciones que presentan estos acuerdos es la reducida cantidad de países miembros con los que cuenta, a abril de 2010 la Convención sobre el Delito Cibernético del Consejo de Europa tenía el más amplio alcance: ha sido firmada por 46 Estados y ratificada por 26, son los países desarrollados quienes cuentan con la experiencia y los recursos que demanda la implementación de este tipo de acuerdos. Un vacío legal en países sin las competencias necesarias para la persecución ofrece una oportunidad para los delincuentes quienes pueden causar estragos muchas veces con solo contar con un ordenador y una conexión a internet

sin importar mucho donde se encuentre al momento de realizar un ataque". (Loredo y Ramírez, 2013, p. 49).

De lo anterior se desprende que este convenio es el primer tratado a nivel internacional creado para combatir a los ciber delincuentes que día a día mejorar y actualizan su accionar delictivo, quedando, muchas veces, fuera del alcance de la ley. Persigue una política y persecución penal homogénea y común a través de cuerpos normativos que se adapten a la realidad y la cooperación entre los países miembros.

Es importante enfatizar que las disposiciones aprobadas en el Convenio no son de aplicación directa, ya que esta sirve como columna o guía que los Estados deben seguir al momento de legislar y crear sus normativas. Esto se puede apreciar en su propio contenido en cuando hace un llamado a los Estados adheridos al Convenio para que inicien sus reformas en la Comunidad Internacional, la misma que se fue dando a cabo paso a paso, por los que se ha ratificado y aplicado en ellos.

Es así que este Convenio posee un primer capítulo encargado de dar definiciones y/o conceptualizaciones como base para los Estados. En el segundo capítulo, establece las guías para la regulación que habrán de promulgar los Estados dentro de su cuerpo normativo. El tercer capítulo está dirigido a establecer los procedimientos de cooperación internacional en la materia. Además, su cuarto y último capítulo está dedicado exclusivamente a regular extremos tales como la aprobación, formas de adhesión y firma, denuncias, enmiendas, reservas etc.

Según nuestro Ministerio de Relaciones Exteriores (2017), el Perú se encuentra ad portas de ser parte de este Convenio, por lo que aún estamos a miras de concretarlo, no obstante a ello, se ha procurado adaptar las leyes vigentes a lo señalado en dicho tratado a fin de estar a la vanguardia de los países integrantes.

Vacío legal:

Basterra (2000) menciona que la “laguna normativa a aquella situación no contemplada en el ordenamiento normativo. Hay un "vacío" legal. El sistema jurídico no tiene una solución normativa para un caso concreto” (p. 285).

Esto tiene una explicación, según lo expresado por Goldschmidt. Puede ser que el creador de la ley omitió el contemplar una situación en concreto; o porque estamos ante un acontecimiento científico-técnico que el legislador no pudo haber previsto en el momento de la redacción.

Mecanismos de solución:

“La ciencia jurídica moderna ha llegado a la conclusión de que las leyes son siempre insuficientes para resolver los infinitos problemas que plantea la vida práctica del Derecho. Es decir, que pese a la aspiración del legislador de prever todas las hipótesis posibles, siempre quedan fuera de ellas casos no imaginados. Estos casos son las llamadas lagunas de la ley. La solución ante las lagunas jurídicas es la integración, y hay lugar a ella cuando el operador jurídico, ante la ausencia de un precepto que regule el caso, o este sea oscuro, tiene que hacer uso de una serie de elementos que se pueden encontrar dentro o fuera del cuerpo normativo relacionado para poder establecer una adecuada respuesta” (Galiano y Gonzáles, 2012, p. 436-437).

Ante cualquier vacío legal o laguna que exista en los cuerpos normativos, se deben integrar las fuentes del derecho para suplir aquellos “huecos” que impiden se puedan aplicar correctamente.

ATRIA y otros (2005) dicen que ante esta situación, “si a un juez se le solicita una resolución, no puede negarse y debe suplir la laguna jurídica a través de distintas herramientas” (p. 159 y ss).Asimismo, mencionan que las más habituales son:

Derecho Supletorio: El juez acude a la regulación de una rama del derecho supletoria.

Interpretación Extensiva: El juez hace una interpretación lo más extensiva posible de una norma cercana.

Analogía: El juez aplica normas que están dictadas para situaciones esencialmente parecidas.

Acudir a otras fuentes del derecho: Como la costumbre o los principios generales del Derecho.

Norma cruzada: Otra técnica significativa de solución de «lagunas jurídicas» es la de normas cruzadas con distintos rangos, unas principales y otras supletorias, de modo que se sabe cuál debe aplicarse con preeminencia y, al mismo tiempo, entre del derecho principal y el derecho supletorio, se minimiza al máximo la probabilidad de la existencia de lagunas del derecho.

De igual forma, nuestro sumo intérprete de la norma, el Tribunal Constitucional, en el Pleno Jurisdiccional (Exp. N° 047-2004-AI/TC), señaló en la sentencia que dentro de las **"Fuentes normativas con rango distinto a la ley encontramos:**

La jurisprudencia

La Costumbre

Los principios generales del derecho

El contrato (autonomía de la voluntad)

La doctrina".

Entonces, luego de haber indicado algunas cosas, podemos afirmar que el problema real no radica en saber que existen vacíos o lagunas que imposibilitan aplicar correctamente las sanciones por delitos informáticos, sino entender en qué momento y bajo qué circunstancias nos encontramos con una de estas imperfecciones legales. Estas fallas podemos ubicarlas cuando el juez tiene en la ley sólo una orientación general; cuando la misma ley no menciona nada en lo absoluto al no proveer el caso; o cuando ésta es incompleta al no contemplar alguna de sus posibilidades.

1.1.1.3 Definición Términos Básicas

Bases de datos : Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas a disposición de muchos usuarios.

Bien Jurídico : Dícese de aquellos bienes que son protegidos por el Derecho.

Ciber delincuente **:** Dícese de la persona que comete delitos informáticos o ciber delitos.

Cifrado **:** Codificación para transportar datos de manera segura en una red

Cookies **:** Almacenael nombre y contraseña para no volver a repetir en cada página del servidor propia de un usuario.

Cracker **:** Dícese del término empleado para quien utiliza sus conocimientos informáticos para extraer sin consentimiento información, distribuir virus, introducirse ilegalmente en redes, eliminar la protección anticopia del software comercial, burlar la seguridad de determinados sistemas informáticos, etc.

Cracker : Dícese del término empleado para quien utiliza sus conocimientos informáticos para extraer sin consentimiento información, distribuir virus, introducirse ilegalmente en redes, eliminar la protección anticopia del software comercial, burlar la seguridad de determinados sistemas informáticos, etc.

Cookies : Almacenael nombre y contraseña para no volver a repetir en cada página del servidor propia de un usuario.

Daño : Comportamiento consistente en dañar, destruir o inutilizar un bien, en este caso es el sistema informático.

Derecho : Conjunto de normas destinadas a regular la conducta humana.

Delito Informático : Conocido también como "Ciber delito". Dícese de las acciones típicas, antijurídicas y culpables realizadas mediante la aplicación de mecanismos informáticos con el objetivo destruir y dañar por medios electrónicos y redes de Internet.

Documento electrónico : Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles y tendientes a ser comprendidos.

Firewall : Parte de un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Fuentes del derecho : Se entiende como aquellos pilares que suplirán o cubrirán los vacíos que se encuentren en la legislación.

Gusano : Mecanismo que se infiltra en los programas ya sea para modificar o destruir los datos, los cuales no se regeneran.

Http y Https : Cuando una página se abre, ésta se encuentra identificada y con seguridad para prevenir la penetración de los Hackers.

Internet : Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP a nivel mundial.

IP : Número que identifica, de forma lógica y jerárquica, a una Interfaz en red de un dispositivo electrónico tal como computadora, tableta, portátil, Smartphone, u otros, que utilice el protocolo IP o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Modem : Equipo o aparato electrónico que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro.

Phishing : Fraudes realizados mediante el uso de internet, con la consigna de obtener datos confidenciales de usuarios como contraseñas o claves de acceso a cuentas bancarias. Un ejemplo del nuevo phishing es el SMiShing.

Red Inalámbrica : Conexión de ordenadores o computadoras a través de las ondasde un router sin la utilización de cables.

Router : Dispositivos que sirve para acceder a una red externa a través de cable o inalámbricamente (WIFI).

SMiShing : Es una variante del phishing, que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque. El resto del procedimiento es igual al del phishing: el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falseada, idéntica a la de la entidad en cuestión.

Tecnología : Conocimientos articulados entre sí bajo parámetros establecidos en procedimientos y métodos técnicos en favor de las personas para satisfacer sus necesidades.

Vacíos legales : Dícese de la situación en la que una norma o ley ha omitido en su texto alguna regulación en específico sobre un tema determinado por lo cual una conducta queda fuera de su alcance.

URL : Uniform Resource Locator, es decir Localizador Uniforme de Recurso, y se refiere a la dirección única que identifica a una página WEB en internet.

1.2 Formulación del Problema de Investigación

1.2.1 Problema General

¿Cuáles son los vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 y modificatoria en el distrito Cercado Lima 2017?

1.2.2 Problema Específico

¿Qué actividades ilícitas están tipificadas como delitos informáticos en el Cercado Lima vigentes al 2017?

¿Cuáles son los vacíos legales en la Leyes que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017?

¿Cómo, lo vacíos legales en la Leyes peruanas que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017, impiden la aplicación de sus sanciones?

1.3 Justificación

Recordemos, que en el año 2017 se realizó el Censo Nacional a cargo del Instituto Nacional de Estadística e Informática, el cual, pese a los temas logísticos e incidentes que mancharon su desarrollo, tomamos conocimiento que dicha entidad habría realizado convenios con otras instituciones públicas y privadas en el marco de lo dispuesto por el artículo 97° del Decreto Supremo N° 043-2001-PCM, mediante el cual se compromete a otorgar información estadística actualizada con los resultados del Censo, así como los perfiles de cada censado, tal como lo hizo con la Universidad César Vallejo y otras; y, a pesar que tiene carácter de confidencialidad, es de conocimiento público, ya sea por investigaciones periodísticas o porque uno mismo ha recibido la oferta, que hay personas que han obtenido nuestra data para comercializarla en puestos ilegales a la vista y paciencia de las autoridades como en el caso de los “jaladores” y abastecedores en la Av. Wilson en el distrito de Lima.

Esta información, está siendo empleada para poder cometer otros delitos y actualizar la modalidad de los delitos informáticos ya tipificados puesto que tienen “el nicho de mercado” ya establecido por índoles sociales, económicos, políticos, etc.

Entonces, podemos decir que los ciber delincuentes han creado formas mejoradas de realización de actividades ilícitas, por lo cual, constantemente nos vemos en el predicamento de encontrarnos vulnerables ante estas actividades que se alejan del ordenamiento jurídico, trasgrediendo los alcances de la ley penal y escabulléndose en sus vacíos legales, imposibilitando a los Magistrados el garantizar y velar por los derechos de tutela jurisdiccional y al debido proceso que todo agraviado posee y que la misma Constitución Política del Perú prescribe en su artículo 139°.

Es por ello que la inseguridad ciudadana se ha visto en crecimiento por las nuevas actividades delictivas y más aún cuando nuestra propia Carta Magna les da luz verde para su proceder al sostener que no se puede procesar ni sancionar por un acto u omisión que no haya estado previsto en la ley al momento de su comisión, otorgándoles nuevamente la oportunidad de afectar una y otra vez los bienes jurídicos.

Por lo antes expuesto, el presente trabajo de investigación se justifica desde una óptica legal, social y económica porque existe la necesidad de determinar cuáles son los vacíos legales que presenta la norma y sus modificatorias, y así poder proponer mejoras con la prontitud que se requiere, en beneficio de la colectividad y de quienes tengamos que aplicarlas.

1.4 Relevancia

Es importante realizar este estudio a fin de poder establecer lo que realmente limita el quehacer jurisdiccional al momento de emitir sentencia y sancionar a los que hayan cometido dichos ilícitos penales y así evitar que la ciberdelincuencia gane la batalla vulnerando o exponiendo más a la población con nuevas tendencias delictivas al encontrarse fuera del margen de la ley. No obstante, es también importante el poder establecer cuando nos encontramos frente a uno de estos vacíos y saber qué acciones tomar para combatirlos en pro de la comunidad.

1.5. Contribución

La precisión de los vacíos legales en las Leyes peruanas que regulan los delitos informáticos, tales como la Ley N° 30096 y su modificatoria por la Ley N° 30171, brindará una mayor protección a los bienes jurídicamente protegidos como el patrimonio, fe pública, libertad sexual, de la información, etcétera, que puedan ser afectados a través del empleo de Tecnologías de la información y comunicación,

permitiendo se pueda aplicar las sanciones vigentes en las leyes de la materia y no queden impunes.

De otro lado, quienes directamente podrán emplear este trabajo de investigación como punto de partida son los mismos administradores de justicia y quienes solemos ser los usuarios de los medios electrónicos o tecnológicos, quienes somos directamente presa y víctima de los inescrupulosos delincuentes que se esconden tras un ordenador y muchas veces son anónimas sus identidades, buscando disminuir la incidencia de la criminalidad cibernética.

1.6 Objetivos de la Investigación

1.6.1 Objetivo General

Determinar cuáles son los vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 y modificatoria en el distrito Cercado Lima 2017.

1.6.2 Objetivo Específicos

Determinar qué actividades ilícitas están tipificadas como delitos informáticos en el Cercado Lima vigentes al 2017.

Precisar cuáles son los vacíos legales en la Leyes que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017.

Establecer cómo, lo vacíos legales en la Leyes peruanas que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017, impiden la aplicación de sus sanciones.

CAPÍTULO II
MARCO METODOLÓGICO

2.1 Supuesto

2.1.1 Supuesto Principal

Existen vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 y modificatoria en el distrito Cercado Lima 2017.

Lo antes indicado, permitirá que no queden exentos de responsabilidad los ciber delincuentes que atentan contra bienes jurídicamente protegidos mediante la actualización o proyección de las normas manteniendo el espíritu de la norma y facilitando la participación de los operadores de justicia al momento de perseguir el delito y al finalizar el proceso con la sentencia condenatoria esperada.

2.1.2 Supuesto Secundario

Existen actividades en las que emplean tecnologías de la información y comunicación que atentan contra bienes jurídicamente protegidos que no están tipificadas como delitos informáticos en el Cercado Lima al 2017.

A mayor aumento de los avances de la tecnología, aumenta la tipificación de nuevos delitos informáticos.

Existen vacíos legales en la Ley N° 30096 que impiden se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima al 2017.

Existen vacíos legales en la Ley N° 30171, que modifica la Ley N° 30096, la cual impide se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima al 2017.

2.1 Categorías

2.1.1 Categoría principal

Vacíos legales

Delitos Informáticos

2.1.2 Categoría Secundaria

Alcances de las sanciones tipificadas por delitos informáticos en las Leyes N° 30096 y N° 30171.

Vacíos legales de la Ley N° 30096 que impiden la aplicación de sanciones de los delitos informáticos.

Vacíos legales de la Ley N° 30171 que impiden la aplicación de sanciones de los delitos informáticos.

Acciones típicas, antijurídicas y culpables realizadas mediante la aplicación de mecanismos informáticos y/o tecnológicos con el objetivo destruir y dañar por medios electrónicos y redes de Internet.

2.3 Tipos de Estudio.

Corresponde el tipo de estudio básico con enfoque cualitativo porque obtendremos información de los sujetos que forman parte de la presente investigación desde un plano subjetivo, basado más desde un plano de valor de calidad por ser un estudio jurídico, aplicando la lógica inductiva (de lo particular a lo general).

2.4. Diseño de Investigación

El diseño no experimental- descriptivo ya que procederemos a analizar nuestras variables del supuesto principal conforme está planteado, sin modificar contenido alguno, con el sustento y fundamento de los resultados desprendido de los antecedentes de la investigación y las bases teóricas que la integran.

Entonces, esta investigación es correlacional transeccional porque mediante este tipo de estudio se determinará el grado de relación existente entre las variables, conforme lo señala Moreno (2000).

2.5. Escenario de Estudio

Como escenario de estudio ha sido elegido el Cercado Lima ya que abarca la mayor parte del territorio de la capital, con un aproximado de 10’000,000.00 de habitantes, lo que conlleva que la actividad delictiva aumente y esto proporcione mayor carga laboral a nivel nacional.

2.6. Caracterización de los Sujetos

Para este trabajo de investigación se tomaron como sujetos a los fiscales provinciales del Cercado Lima en la sede de la Av. Abancay s/n cdra. 5-Cercado de Lima.

Cabe indicar que no se ha utilizado criterio alguno para elegirlos, por el contrario, se tomó el total de fiscalías penales que se encuentran en dicha sede.

2.7. Trayectoria Metodológica

Siendo este trabajo una investigación básica y método inductivo, ya que es la utilizada para trabajos de tesis de derecho al haberse recopilado información partiendo de la realidad, ya sea material bibliográfico, normativa nacional e internacional, encuestas u otros, se analizará mediante estadísticas que emanarán de las respuestas que darán nuestra población a quienes se les someterá a dicho instrumento. Asimismo, dichos datos obtenidos también serán interpretados y analizado sí o sí en función a nuestro marco teórico, el cual será el sustento de los análisis e interpretación que se efectuarán con los datos recolectados.

2.8. Población y Muestra

2.8.1 Población

Para tales fines, trabajaremos con fiscales provinciales penales del Cercado Lima que laboran en la sede de la Av. Abancay s/n cdra.5, distrito de Lima. Siendo un número de 57 fiscalías provinciales penales que se encuentran ahí.

2.8.2 Muestra

Por ende, la muestra corresponde a las fiscalías provinciales penales del Cercado Lima que laboran en la sede de la Av. Abancay s/n cdra.5, distrito de Lima. Para determinar el tamaño óptimo de la muestra, emplearemos la fórmula de muestreo aleatorio simple y así hacer una estimación real.

$$M = \frac{Z^2PQN}{E^2(N-1)+Z^2PQ}$$

Para un mejor entendimiento, procederemos a explicar el significado de cada componente de la fórmula.

Z = Valor de la abscisa de curva normal para una probabilidad del 95% de confianza.

P = Proporción de los fiscales que radican en el Cercado Lima que conocen sobre la deficiencia o vacíos legales en las leyes sobre delitos informáticos.(P=0.5).

Q = Proporción de los fiscales que radican en el Cercado Lima que no conocen sobre la deficiencia o vacíos legales en las leyes sobre delitos informáticos. (Q=0.5).

E = Error de muestra 0.05%.

N = Tamaño óptimo de la muestra.

Entonces el nivel de confianza del 95% y 5% como margen de error de muestra tenemos:

$$M = \frac{(1.95)^2(0.5)(0.5)(57)}{(0.05)^2(57-1)+ (1.95)^2(0.5)(0.5)}$$

$$M = \frac{54.185625}{1.090625}$$

$$M = 49.6802$$

$$M = 50$$

Finalmente, 50 serán los encuestados.

2.9. Técnicas e instrumentos de recolección de datos:

Técnicas:

Se procederá a recolectar los datos de manera anónima, mediante el contacto e interacción con la población a quien se le someterá al instrumento, que en este caso es la encuesta.

Encuesta:

Esta técnica se empleará para obtener los datos respecto a las opiniones de los fiscales a quienes se les someterá. Este instrumento posee preguntas escritas a fin que las respondan de la misma forma. Como se mencionó anteriormente, serán sin nombre ni identificación, ciñéndose especialmente al tema que nos atañe y precisando el objeto de estudio, además no implica demasiados costos.

Entrevista:

Para la recolección de datos se procederá a realizarse una entrevista con los sujetos de la muestra para encontrar convicción si mis supuestos están correctos de acuerdo a los objetivos. Esto se realizará de manera directa, mediante el diálogo sin influir en las respuestas, tendiendo a que los entrevistados focalicen su opinión.

Presentación de información:

Se procederá al vaciado de los datos adquiridos en tablas estadísticas no probabilísticas, trabajando con los porcentajes obtenidos. Se utilizará el programa Excel.

Interpretación:

Serán interpretados y analizados en función al marco teórico de la investigación, el cual servirá como sustento y fundamentación de los análisis e interpretación de los datos recolectados.

2.10. Rigor Científico

Al ser un trabajo de investigación con tipo de estudio cualitativo, el grado de certeza es más subjetivo. Se busca determinar que existen vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 y Modificatoria en el distrito fiscal de Lima en el 2018, por lo que la rigurosidad científica para la sustentación del problema y los supuestos en esta primera etapa es confirmada a través de la lectura analítica de la norma en cuestión.

Esta afirmación se verá confirmada o no por intermedio de la realización de las respectivas encuestas donde se podrán analizar las respuestas otorgadas. En relación a la metodología para la determinación de la población, muestra y diseño de las preguntas a realizar, estas se someterán previamente al escrutinio de nuestro asesor de tesis, por lo que considero que en este aspecto también cumplimos con la rigurosidad científica requerida.

2.11. Aspectos Éticos

Es necesario señalar que en este trabajo de tesis ha tomado como base a autores a quienes se han citado, los cuales han sido consultados y a quienes se les ha reconocido la autoría de las ideas y pensamientos referenciados conforme corresponde y se desprenden de las normas APA vigentes.

CAPÍTULO III

RESULTADOS

3.1 Análisis de Resultado

¿Usted cree que nuestro ordenamiento penal tiene alcances suficientes para combatir a los delitos informáticos?

Sí	15	30%
No	35	70%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 35 (70%) no cree que el Nuevo Código Procesal Penal tiene los alcances suficientes para combatir los delitos informáticos. Sin embargo, 15 (30%) tienen la creencia que sí los posee.

¿Usted cree que se están logrando aplicar sanciones por la comisión de delitos informáticos?

Sí	8	16%
No	42	84%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 42 (84%) no cree que se estén aplicando las sanciones por delitos informáticos. Sin embargo, 8 (16%) tienen la creencia que sí se aplican.

¿Usted cree que el legislador ha tipificado correctamente los delitos informáticos en la ley?

Sí	20	40%
No	30	60%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 30 (60%) no cree que estén correctamente tipificado los delitos informáticos. Sin embargo, 20 (40%) creen que sí.

En su labor como fiscal ¿podría hacer calzar en cualquiera de esos tipos penales alguna conducta delictiva nueva no prevista?

Sí	5	10%
No	45	90%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 45 (90%) dijeron que no. Sin embargo, 5 (10%) dijeron que sí.

En su labor como fiscal ¿ha tenido algún inconveniente para aplicar las sanciones previstas por delitos informáticos?

Sí	39	78%
No	11	22%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 11 (22%)dijeron que no. Sin embargo, 39(78%) dijeron que sí.

¿Usted cree que tendría algún inconveniente?

Sí	39	78%
No	11	22%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 11 (22%) dijeron que no. Sin embargo, 39 (78%) dijeron que sí.

¿Usted ha detectado, en la Ley N° 30096 (ley de Delitos informáticos) alguna falencia?

Sí	48	96%
No	2	4%

Interpretación:

Del total de encuestados, 2 (4%) dijeron que no han detectado falencias. Sin embargo, 48 (96%)dijeron que sí.

Ante un vacío legal detectado en la Ley N° 30096 ¿Archivaría el caso o se ciñe a una fuente del derecho para suplir la falta de regulación?

Archivo	6	88%
Fuentes	44	12%
TOTAL	50	100%

Interpretación:

Del total de encuestados, 6 (12%) dijeron que Archivarían el caso. Sin embargo, 44 (88%)dijeron que emplearían las fuentes del derecho.

CAPÍTULO IV

DISCUSIÓN

4.1 Análisis de discusión de resultados

Supuesto 1: Existen actividades en las que emplean tecnologías de la información y comunicación que atentan contra bienes jurídicamente protegidos que no están tipificadas como delitos informáticos en el Cercado Lima al 2017.

Los datos han arrojado que este tipo de delitos se realizan por intermedio de aquellas tecnologías de la información ya que genera mayor facilidad, factibilidad y libertad a los ciber delincuentes.

Pese a que el tiempo nos ha regalado estos adelantos científicos, nos encontramos ante la incertidumbre de no poder controlar del todo el mal empleo de los mismos, ya sea para cometer delitos contra el patrimonio, contra la libertad sexual, entre otros, en agravio tanto de la sociedad como del Estado, en algunas ocasiones.

Supuesto 2: A mayor aumento de los avances de la tecnología, aumenta la tipificación de nuevos delitos informáticos.

Al ser un tema de constante evolución por estar siempre en un proceso de cambio, es por ello que muchas de las actividades delictivas nuevas, en las que emplean la tecnología, pueden quedar fuera del alcance de la ley, lo mismo que arrojó nuestra encuesta ya que los sujetos sometidos a este instrumento indicaron que hay falencias en las mismas normas imposibilitando, muchas veces, su sanción.

Supuesto 3: Existen vacíos legales en la Ley N° 30096 que impiden se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima al 2017.

La gran mayoría de los fiscales encuestados coincidieron sobre la existencia de vacíos en este dispositivo legal tal como la manera de poder determinar agravantes, temas o conductas no previstas en la ley, su injerencia en otros delitos como interceptación telefónica, pornografía infantil, etc. Razón por la cual, no se cumplía el espíritu de la norma ni mucho menos poder sancionar.

Supuesto 4: Existen vacíos legales en la Ley N° 30171, que modifica la Ley N° 30096, la cual impide se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima al 2017.

Se tuvo la intención que al modificar ciertos aspectos de la Ley 30096, también esta posee vacíos, lo mismo que fue señalado por la mayoría de los encuestados, dado a los avances informáticos y tecnológicos.

Una vez realizada la contratación de resultados, se puede apreciar que existen vacíos legales en las Leyes N° 30096 y N° 30171, y que el esfuerzo en poder modificar algunas aristas a fin de que pueda cumplir su función, sólo quedó en eso, en esfuerzo de una manera apresurada y poco asertiva ya que, aparentemente, daría la impresión que sus promulgaciones solo fueron con la sola intención de estar a la vanguardia de otros países que ya habían adaptado su ordenamiento al Convenio de Budapest.

Hay artículos en la ley que podrían vulnerar la libertad de expresión y la libertad de prensa ya que se aumentaron las penas para la interceptación de información pública de carácter reservado, pero sin precisar nada sobre la difusión de la misma, lo cual puede prestarse a cualquier interpretación. De otro lado, los delitos

informáticos vinculados con la seguridad nacional suponen, con esta norma, penas elevadas, pero no hay una definición de lo que se puede considerar información secreta o de seguridad nacional, por lo que podría sancionarse arbitrariamente la difusión de una información secreta.

El conocimiento por parte de los fiscales de la Provincia Penal de Lima, nos da luces y preocupa la situación actual en la que nos encontramos porque podrían resultar vulnerados los derechos de los individuos que la ley pretende cuidar y proteger como cuando uno mismo desea revisar una cuenta o sistema informativo, realizar copias de bases de datos de data que la misma persona ha elaborado, etc., siendo muy ambiguo y oscura en muchas ocasiones, resultando compleja la adecuada aplicación de las leyes, del criterio y los fundamentos que se considera a la hora de dictaminar que pena corresponde o no para un delito informático, resultado confusa la tipificación de los delitos por parte de fiscales y jueces y más aún cuando las conductas no son típicas al momento de su realización, por lo que conlleva a que tengamos normas más dinámicas en función a la evolución tecnológica.

CAPÍTULO V

CONCLUSIÓN

Al inicio fue utilizada la informática desde una óptica de servicio de la comunidad pero a medida que pasó el tiempo y surgieron ciertas conductas o comportamientos delictivos vinculados a ella, pasando a ser medio para la concreción de delitos.

Los delitos informáticos no deben impedir que el usuario se prive de todo lo que proveen las tecnologías, al contrario, debería fortalecer el conocimiento y las políticas del estado a fin de robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

Al ser un medio virtual, se crea una atmósfera de anonimato que protege y promueve modalidades nuevas de atentados contra las personas e instituciones. Además, por la propia constitución de la red, las conductas delictivas adquieren una potencialidad lesiva que viene a multiplicar los posibles daños a terceros.

El avance de las tecnologías puede conllevar a la confusión al momento de la tipificación de los delitos y hasta resultar ciertas conductas delictivas en atípicas.

La ambigüedad u oscuridad en el tratamiento de los ciber delitos en las leyes, podrían vulnerar derechos de los individuos que deberían ser protegidos ya que, muchas veces, resultan muy abiertos los artículos que describen las inconductas.

Este tipo de delitos son considerados de índole transnacional, ya que se desenvuelve a niveles internacionales.

Los ciber negocios pueden entrañar diversas formas de delitos que escapan del alcance de las leyes como en las *“Dark web o Deep Web”*, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática.

La posible incompetencia de magistrados, la imposibilidad de extradición, la garantía del juez natural reconocida por los tratados internacionales de derechos humanos y otras anexas, como el debido proceso y el in dubio pro reo, limitan a la legislación más aún si no ha sido debidamente planificada para otorgar una protección efectiva a los agraviados.

El hecho que los infractores comprendan las imposibilidades de aplicación de las normas penales, genera indefensión ya que se les facilita poder evadirlas y resultar así en la directa inaplicabilidad del sistema.

Al momento de investigar estos delitos, se tiene la gran dificultad de obtener pruebas que identifiquen al autor, lo que deviene en la imposibilidad de penalizar al delincuente

Las entidades financieras poco o nada han hecho frente a la proliferación del fraude financiero electrónico, ante la falta de normativa específica, lo que ocasiona tengan grandes pérdidas económicas.

Se ha generado un grado de desconfianza respecto al sistema de justicia en el país por lo que estos delitos muchas veces no son denunciados a las autoridades pues no se cree que vayan a dar una solución.

Los operadores de justicia no cuentan con una adecuada preparación en estos temas, por lo que se ven desorientados al momento de tratar los delitos informático, dándoles la atención como si fueran delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas.

La necesidad del tránsito de datos conlleva también a la posibilidad creciente de estos delitos, lo que conlleva a considerar un gran reto para los legisladores, las autoridades policiales encargadas de las investigaciones y operadores de justicia.

A nuestro criterio, este tipo de inconductas, cuya realización afecta grandes intereses financieros, a su vez generan una significativa l inseguridad jurídica, tales como el fraude procesal y el fraude informático.

La figura penal de acceso ilícito, regulada en el artículo 2, se clasifica como un delito de mera actividad, porque en este ilícito el delito queda consumado en el mismo acto de vulnerar las medidas de seguridad de un sistema informático.

El tipo de atentado contra la integridad de datos informáticos, regulada en el artículo 3, es un ejemplo de delito de mera actividad, porque queda consumado con el solo acto de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos

El delito de tráfico ilegal de datos, señalada por el artículo 6, es derogado por la única disposición complementaria derogatoria de la Ley 30171. Siendo incorporado al Código Penal vigente (Artículo 154- A: tráfico ilegal de datos personales).

En cambio, respecto a la suplantación de identidad, regulada en el artículo 9, es un delito de resultado, porque no sólo basta con realizar la conducta sino que se debe generar un resultado posterior que sería el causar un perjuicio.

CAPÍTULO VI

RECOMENDACIONES

Es necesario que se deban crear nuevos métodos para protegerse con la misma tecnología para ello, puesto que con la modificación de la Ley N° 30096 se debió dar y quitar la incertidumbre que existe y evitar que ciertas conductas queden fuera de responsabilidad penal y estén exentas algunas otras en donde uno mismo desee traspasar la medida de seguridad que contengan los datos o sistemas informáticos sin incurrir en delito ni ser sancionado.

Es importante realizar observaciones a las leyes, tanto a nivel de casos, informes, jurisprudencias, encuestas y entrevistas a operadores de justicia por los problemas en que se han visto al momento de tratar de aplicar las sanciones.

Solo podrá combatirse la delincuencia informática si las leyes se siguen escribiendo tomando en cuenta la evolución tecnológica y el uso de fuentes del derecho para que las conductas no queden fuera de la ley.

Debería generarse el diálogo con los fiscales y jueces y el Poder Legislativo a fin de que se tomen acciones más dinámicas respecto a poder regular correctamente estas inconductas.

Se debe acceder a medios informáticos a través de una Red, tomando medidas de seguridad tales como: firmas electrónicas, certificados digitales, que estén emitidos por instituciones legalmente acreditadas.

Es necesario desarrollar programas de capacitación de magistrados y de los operadores de justicia sobre delitos informáticos.

Se debe fortalecer los laboratorios forenses destinados a realizar investigaciones sobre temas informáticos.

Es conveniente capacitar a la sociedad en valores y sobre los posibles casos de comisión de ciber delitos, a través de campañas, folletos, con el propósito de alejar a niños y jóvenes de las malas prácticas respecto al uso de la tecnología.

Se debe procurar considerar dentro de la problemática a la informática y todo tipo de tecnología en su conjunto, para evitar que la norma jurídica quede desfasada del contexto en el cual se debe aplicar las sanciones.

El problema más importante que enfrenta la propiedad intelectual, es la piratería y falsificación de las obras del intelecto humano, trayendo graves consecuencias económicas y sociales.

Se deben establecer mayor capacitación sobre Políticas Públicas y Legislación sobre el Convenio de Budapest Documento y así establecer más Lineamientos de Política para la ciber seguridad y ciber defensa. De igual forma, continúa capacitación respecto a la Legislación vigente y siempre mantener un registro documentado de los casos que no han podido ser condenados y así es qué parámetros o medidas tomar en las futuras modificatorias de la normatividad especial.

VII. REFERENCIAS BIBLIOGRÁFICAS

Cascante, L. G. M. (2013). Metodología de la investigación educativa: posibilidades de integración. Revista comunicación, 12(1), 182-194.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación. Sexta Edición. Editorial Mc Graw Hill. México. 2014. Hernández, R. Metodología de la Investigación. 6a Edición, Mc Graw Hill, México.

Lematire Picado, R. (2010) La impunidad de los delitos informáticos en la ciber-sociedad costarricense en el ámbito del derecho penal (tesis de pregrado). Universidad de Costa Rica, Rodrigo Facio, Costa Rica.

Herrera Calderón, E. A. (2016). “El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal” (tesis de pregrado). Universidad Central del Ecuador, Quito, Ecuador.

Morales Delgado, D. Y. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015 (tesis de pregrado). Universidad Señor de Sipán, Pimentel, Chiclayo.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho, 44(1), Págs. 261-285.

MAZUELOS COELLO, J. F. (2001). Los delitos informáticos: una aproximación a la regulación del Código penal peruano. Revista Peruana de Doctrina y Jurisprudencia Penales, N° 2.

Romero Echevarría, L. M. (2005). Marco conceptual de los Delitos Informáticos (tesis para optar el grado de magister). Universidad nacional Mayor de San Marcos, Lima, Perú.

Sequeiros Calderón, I. C. (2016). “Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano-2015” (tesis de pregrado) Universidad de Huánuco, Lima, Perú.

Gil Albarrán, G. E. (2009). Evaluación y diseño de un marco legal integral para mejorar el comercio electrónico en el Perú” (tesis para optar el grado de magíster), Trujillo, Perú. Villavicencio Terreros, F. (2014). Delitos Informáticos: Cybercrímenes. *Ius Et Veritas, N° 49*. Págs. 284-304.

Northcote Sandoval, C. (2013). Comentarios a la ley sobre delitos informáticos. *Actualidad Empresarial*, *Nº 289 - Segunda Quincena de Octubre 2013*. Págs. 1-4.

Reyes Sánchez, Y. y Fernández Aramburo, E. (2009). “Delitos Informáticos” (tesis de pregrado). Instituto Tecnológico de Durango, Durango, México.

Granados Ramírez, R. y Parra Rojas, A. C. (2016). “El delito de hurto por medios informáticos que tipifica el articulo 269i de la ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el período 2012 – 2014” (tesis de pregrado). Universidad Libre, San José de Cúcuta, Colombia.

Rodríguez Madrigal, B., Flores Vásquez, F. E. y Berríos Reyes, M. L. (2006). “Los delitos informáticos y la información como nuevo bien jurídico protegido” (tesis de pregrado). Universidad Nacional Autónoma de Nicaragua, León, Nicaragua.

Espinoza Coaila, M. (2017). “Derecho Penal Informático: Deslegitimación del poder punitivo en la sociedad de control” (tesis de pregrado). Universidad Nacional del Altiplano, Puno, Perú.

Iriarte, E. (2012). Marco Legal para el internet en el Perú. Exploración Inicial. *Derecho & Sociedad*, *Nº 39.* Págs. 169-170.

Ticona Yanqui, F. E. y Ramos Quispe, M. (2015). “Uso de las redes sociales en el Perú”. *Revista Científica “Investigación Andina”*, *VOLUMEN 15 – Nº 2 Julio–Diciembre 2015.* Págs. 7-14.

Guerra Valdivia, A. R. (2011). Delitos Informáticos-Casos de Estudio (tesis para optar el grado de magister). Instituto Politécnico Nacional, México Distrito Federal, México. Recuperado de http://www.repositoriodigital.ipn.mx/bitstream/123456789/12653/1/TESIS.%20DELITOS%20INFORM%C3%81TICOS-CASO%20DE%20ESTUDIO.pdf

Terán Rivero, R. A. (2015). “La necesidad de incorporar en el código penal el tipo penal de falsificación informática” (tesis de pregrado). Universidad Mayor de San Andrés, La Paz, Bolivia. Recuperado de http://repositorio.umsa.bo/bitstream/handle/123456789/13890/T4774.pdf?sequence=1&isAllowed=y

Santiváñez Antúnez, D. (2015). Ciberterrorismo: amenaza fulminante. Resumen de la tesis “El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley sobre Delitos Informáticos en el Perú”. Ius Et Praxis, (46), 225-240. Recuperado de http://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/673

Rodríguez Arbeláez, J. D. (2011). “Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación”. Recuperado de http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334

Tiedemann, Klaus (1985), Poder informático y delito, Barcelona, España.

VIII. ANEXOS

ANEXO 1: Matriz De Consistencia

"Los vacíos legales que impiden la aplicación de sanciones en los delitos informáticos en la Ley N° 30096 Cercado Lima 2017**"**

PROBBLEMAS	OBJETIVOS	SUPUESTOS	CATEGORÍAS	METODOLOGÍA
Problema General ¿Cuáles son los vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 Cercado Lima 2017? **Problemas Específicos** ¿Qué actividades ilícitas están tipificadas como delitos informáticos en el Cercado Lima vigentes al 2017? ¿Cuáles son los vacíos legales en la Leyes peruanas que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017? ¿Cómo lo vacíos legales en las Leyes que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017, impiden la aplicación de sus sanciones?	**Objetivo General** Determinar cuáles son los vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 Cercado Lima 2017. **Objetivos Específicos** Determinar qué actividades ilícitas están tipificadas como delitos informáticos en el Cercado Lima vigentes al 2017. Precisar cuáles son los vacíos legales en la Leyes peruanas que regulan los Delitos Informáticos en el Cercado Lima vigentes al 2017. Establecer cómo, lo vacíos legales en la Leyes que regulan los Delitos Informáticos en el Cercado Lima al 2017, impiden la aplicación de sus sanciones.	**Supuesto principal** Existen vacíos legales que impiden la aplicación de sanciones por delitos informáticos en la Ley N° 30096 Cercado Lima 2017. **Supuestos Secundarios** Existen actividades en las que emplean tecnologías de la información y comunicación que atentan contra bienes jurídicamente protegidos que no están tipificadas como delitos informáticos en el Cercado Lima 2017. A mayor aumento de los avances de la tecnología, aumenta la tipificación de nuevos delitos informáticos. Existen vacíos legales en la Ley N° 30096 que impiden se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima 2017. Existen vacíos legales en la Ley N° 30171, que modifica la Ley N° 30096, la cual impide se apliquen las sanciones prescritas por Delitos Informáticos en el Cercado Lima 2017	Vacíos legales Delitos Informáticos **Subcategorías** Alcances de las sanciones tipificadas por delitos informáticos en las Leyes N° 30096 y N° 30171. Vacíos legales de la Ley N° 30096 que impiden la aplicación de sanciones de los delitos informáticos. Vacíos legales de la Ley N° 30171 que impiden la aplicación de sanciones de los delitos informáticos. Acciones típicas, antijurídicas y culpables realizadas mediante la aplicación de mecanismos informáticos y/o tecnológicos con el objetivo destruir y dañar por medios electrónicos y redes de Internet.	**Tipo:** Básico **Nivel:** Descriptivo **Método:** Inductivo **Enfoque:** Cualitativo **Paradigma:** Interpretativo **Muestra:** **Técnica:** Entrevista y Encuesta. **Instrumento:** Guía de entrevista.

ANEXO 2: Validación de Entrevistas/ Encuestas Experto 1

CERTIFICADO DE VALIDEZ DEL CONTENIDO DE LOS INTRUMENTOS DE LA INVESTIGACIÓN

ITEM	CONTENIDO	PERTINENCIA			RELEVANCIA			CLARIDAD			SUFICIENCIA		
		Si	No	Corregir	Si	No	Corregir	Si	No	Corregir	Si	No	Corregir
	Preguntas de las entrevistas / encuestas a aplicarse												
1	¿Usted cree que nuestro ordenamiento penal tiene alcances suficientes para combatir a los delitos informáticos?												
2	¿Usted cree que se están logrando aplicar sanciones por la comisión de delitos informáticos?												
3	¿Usted cree que el legislador ha tipificado correctamente los delitos informáticos en la ley?												
4	En su labor como fiscal ¿podría hacer calzar en cualquiera de esos tipos penales alguna conducta delictiva nueva no prevista?												
5	En su labor como fiscal ¿ha tenido algún inconveniente para aplicar las sanciones previstas por delitos informáticos?												
6	¿Usted cree que tendría algún inconveniente?												

7	¿Usted ha detectado, en la Ley N° 30096 (ley de Delitos informáticos) alguna falencia?													
8	Ante un vacío legal detectado en la Ley N° 30096 ¿Archivaría el caso o se ciñe a una fuente del derecho para suplir la falta de regulación?													

Observaciones generales:			
Aplicable	Aplicable después de corregir	No Aplicable	
Opinión de aplicabilidad	X		

Apellidos y Nombres del Validador experto
Hijar Hernandez Victor Daniel
DNI
Especialidad Metodólogo
Firma UNIVERSIDAD PRIVADA PERUANA UNIÓN Mg. Daniel Hijar Hernández

Elementos considerativos para la evaluación
Pertinencia. El ítem corresponde al contexto de la investigación
Relevancia: El ítem es apropiado para representar el componente evaluado de la investigación
Claridad: El enunciado se comprende sin mayor dificultad, es conciso, exacto y directo
Suficiencia: El ítem evaluado tiene los elementos necesarios para cumplir su objetivo

ANEXO 3: Validación de Entrevistas/ Encuestas Experto 2

CERTIFICADO DE VALIDEZ DEL CONTENIDO DE LOS INTRUMENTOS DE LA INVESTIGACIÓN

ITEM	CONTENIDO	PERTINENCIA			RELEVANCIA			CLARIDAD			SUFICIENCIA		
		Si	No	Corregir	Si	No	Corregir	Si	No	Corregir	Si	No	Corregir
	Preguntas de las entrevistas / encuestas a aplicarse												
1	¿Usted cree que nuestro ordenamiento penal tiene alcances suficientes para combatir a los delitos informáticos?												
2	¿Usted cree que se están logrando aplicar sanciones por la comisión de delitos informáticos?												
3	¿Usted cree que el legislador ha tipificado correctamente los delitos informáticos en la ley?												
4	En su labor como fiscal ¿podría hacer calzar en cualquiera de esos tipos penales alguna conducta delictiva nueva no prevista?												
5	En su labor como fiscal ¿ha tenido algún inconveniente para aplicar las sanciones previstas por delitos informáticos?												
6	¿Usted cree que tendría algún inconveniente?												

7	¿Usted ha detectado, en la Ley N° 30096 (ley de Delitos informáticos) alguna falencia?													
8	Ante un vacío legal detectado en la Ley N° 30096 ¿Archivaría el caso o se ciñe a una fuente del derecho para suplir la falta de regulación?													

Observaciones generales:

	Aplicable	Aplicable después de corregir	No Aplicable
Opinión de aplicabilidad	X		

Apellidos y Nombres del Validador experto
Dra. Luisa Esther Delgado
DNI 10587264
Especialidad Derecho
Firma 

Elementos consideratívos para la evaluación
Pertinencia. El ítem corresponde al contexto de la investigación *
Relevancia: El ítem es apropiado para representar el componente evaluado de la investigación
Claridad: El enunciado se comprende sin mayor dificultad, es conciso, exacto y directo
Suficiencia: El ítem evaluado tiene los elementos necesarios para cumplir su objetivo