UNIVERSIDAD NACIONAL DE ANCASH

"SANTIAGO ANTUNEZ DE MAYOLO"

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO

Para optar el Título profesional de Abogado

PRESENTADO POR:

Bach. KARINA JOSELIN ZORRILLA TOCTO

ASESOR:

Mg. FANY SOLEDAD VERA GUTIERREZ

Huaraz – Ancash – Perú

2018

DEDICATORIA

A ti Papá Tocto que ya no estas más aquí conmigo y ahora gozas del descanso eterno.

A mis padres y hermanos, porque son mi principal motor para alcanzar mis objetivos. Todo esto es por y para ustedes.

A mi compañero de vida Alexander por su inmensa comprensión y apoyo incondicional.

AGRADECIMIENTO

A mi familia, amigas (os) y a todas las personas que contribuyeron ya sea facilitándome la información requerida o dándome sus puntos de vistas desde su experiencia profesional, a mi asesora por su guía constante, a todos ellos mi agradecimiento.

ÍNDICE

RESUMEN.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, «delitos informáticos».

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo. Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos. La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos.

***Palabras Claves**: Delitos Informáticos, tecnología, datos, acción, omisión, perjuicio. Manipulación.*

ABSTRACT.

Along with the advancement of computer technology and its influence in almost all areas of social life, a series of illicit behaviors called, generically, "computer crimes" have emerged.

Many students of Criminal Law have tried to formulate a notion of crime that would serve for all times and in all countries. This has not been possible given the intimate connection that exists between the social and legal life of each people and each century. The computer crime could be defined as any action (action or omission) made by a human being that causes harm to people without necessarily benefiting the author or that, on the contrary, produces an illicit benefit to its author although it does not directly or indirectly harms the victim, typified by the Law, which is carried out in the computer environment and is punishable by penalty.

In this sense, information technology can be the object of attack or the means to commit other crimes. Information technology has characteristics that make it an ideal means of committing very different types of crime, especially of a patrimonial nature (fraud, misappropriation, etc.). The suitability comes, basically, from the large amount of data that is accumulated, with the consequent ease of access to them and the relatively easy manipulation of that data. The recent importance of data systems, due to their great impact on the progress of companies, both public and private, has transformed them into an object whose attack causes enormous damage, which goes far beyond the material value of the objects destroyed.

***Keywords**: cybercrime, technology, data, action, omission, damage, handling*

INTRODUCCIÓN.

La presente investigación se titula “INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO”. Los delitos informáticos Ley N° 30096 y sus modificatorias son normativas que se acoplan a los nuevos cambios en el mundo, el avance tecnológico ha revolucionado las formas de celebrar contratos, transacciones, buscar información, difundir ideas, etc. todos estos cambian y a su vez posibilitan medios para delinquir, en ese sentido la Ley de delitos informáticos busca frenar esos medios o formas de delinquir, que si bien la presente ley no encuadra adecuadamente los tipos penales, pero es un intento de regularlos.

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

Capítulo I, se desarrollan los antecedentes del desarrollo normativos, histórico y sociales de los Delitos Informáticos de la Ley N 30096 y su modificatoria.

Capitulo II, se desarrolla el marco teórico, donde se desarrolla las variables independiente y dependiente, sus dimensiones respectivas y los indicadores de la investigación. El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho

Capitulo III, se presenta el resultado de la investigación y la validación de la hipótesis.

Capitulo IV, se presenta las discusiones, conclusiones y recomendaciones del trabajo de investigación, siendo algunas de las conclusiones: En el Perú no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa;, los desarrollos de las tecnologías de información y comunicación como las redes sociales generan infinidad de cambios y repercusiones en el comportamiento humano produciendo transformaciones de los ámbitos jurídicos y sociales de todo el mundo, etc.

Finalmente se presenta las referencias bibliográficas con las que se trabajó la presente investigación.

CAPITULO I

EL PROBLEMA Y LA METODOLOGÍA DE LA INVESTIGACIÓN

1.1. Descripción del problema.

En la presente investigación se precisara primero lo que la Ley Nº 30096[1] entiende por "el Sistema informático", así, en su Novena disposiciones complementarias y finales señala lo siguiente que el sistema informático es: *"todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, será el tratamiento automatizado de datos en ejecución de un programa"* ; Segundo la Ley 30096, señala lo que se entiende por "el Datos informáticos" como: *"toda representación de hechos, información o concepto expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función"*; tercero se definirá lo que es "la tecnologías de la información": La frase tecnología de la información es proveniente del inglés "Information technology", y se hace conocido a través del administrador de computadoras Jim Domsic en el año de 1985, con la finalidad de darle un término más actualizado al procesamiento de datos. La tecnología de la información es un término que comprende todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones. Los avances tecnológicos como el Internet, las

[1] Ley Nº 30096, Ley de delitos informáticos publicado el 22 de octubre de año 2013 en el diario oficial el peruano.

comunicaciones móviles, los satélites, etc. Han hecho significativos cambios en el sistema económico y social, influyendo en las relaciones sociales; por último se definirá "las tecnologías de la comunicación": la idea de tecnología se asocia a los conocimientos, las técnicas y los dispositivos que posibilitan la aplicación del saber científico. Comunicación, por su parte, se vincula a la transmisión de información entre un emisor y un receptor que comparten un mismo código. La tecnología de la comunicación, de este modo, está relacionada a las teorías y los artefactos que posibilitan el desarrollo de prácticas comunicativas. Por lo general la noción se emplea junto al concepto de tecnología de la información, que alude al uso de computadoras (ordenadores) y otros equipos para almacenar, procesar y transmitir datos. Por eso es habitual que se hable de tecnologías de la información y la comunicación, conocidas como TIC. De este modo es posible referirse al conjunto de los dispositivos y de los conocimientos que permiten el procesamiento, la transmisión y el almacenamiento de datos y que favorecen que las personas desarrollen comunicaciones. En la actualidad, desde todos los ámbitos de la sociedad en la que vivimos se apuesta por fomentar e impulsar las tecnologías de la comunicación y de la información. De ahí que se utilicen tanto a nivel personal como en el ámbito laboral e incluso en lo que son las aulas, en el campo de los negocios.

De acuerdo a la problemática actual en cuanto a la regulación de Delitos informáticos, se ha presentada inconsistencias y ambigüedades en la Ley Nº 30096, es así, como los expertos en la materia dieron a conocer las deficiencias y falta de precisiones en su regulación Normativa, posteriormente luego de aproximadamente seis meses de su entrada en vigencia fue modificada por la Ley

Nº 30171[2], si bien es cierto con esta modificatoria se preciso algunos articulos incongruentes de Ley anterior, esto Ley Nº 30096, sin embargo, se quiere resaltar la innecesaria regulacion de algunos articulos ya establecidos en nuestro codigo penal vigente por ejemplo la Ley Nº 30096 (2013) y su modificatoria la Ley Nº 30171 (2014) regula con el articulo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnologicos, Con respecto de este articulo 5 nuestro codigo penal[3] *ya* contiene figuras que protegen la libertad y la indemnidad sexual de las personas, independientemente del medio o herramienta que se haya utilizado para vulnerar dichos derechos. Así, tenemos los delitos de seducción (art. 175 cp.), actos contra el pudor (art. 176 cp.) y actos contra el pudor de menores (art. 176-A). por lo que habria superpocicion de tipos penales. Asi encontramos excesos o superposiciones de tipos penales entre los siguientes articulos: articulo 7 (Inteceptacion de Datos informaticos) de la Ley Nº 30096 (2013) y su modificatoria la Ley Nº 30171 (2014) y entre el articulo 162 del codigo penal que regula la interferencia telefonica por lo que habria un exceso de regulacion normativa y una superposicion de tipos penales. El articulo 8º (Fraude Informatico) de la Ley Nº 30096 (2013) y su modificatoria la Ley Nº 30171 (2014) se superpone con los artículos 196°, 196°-A y 197° del código penal. Así NORTHCOTE[4] dice: "No encontramos la justificación para esta diferencia en el tratamiento de las figuras cuando el perjuicio en el patrimonio puede ser tanto o más grave en las figuras de estafa previstas en el Código Penal que en la figura del fraude informático" . Asi encontramos tambien superposicion normativa entre

[2] Ley 30171, Ley que modifica la Ley 30096, Ley de delitos informáticos publicado en el diario Oficial el Peruano el 10 de marzo de 2014.
[3] Código penal peruano Decreto Legislativo Nº 635 publicado el 8 de abril de 1991.
[4] NORTHCOTE, C. (2013). Cometarios a la Ley de Delitos Informáticos. *Actualidad Empresarial*, 4(p. VIII-4).

el artículo 9 (suplantación de identidad) de la Ley Nº 30096 (2013) y el artículo 438 del código penal sobre falsedad genérica cuyo texto normativo dice lo siguiente: *-El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.* Como se puede apreciar de la regulación del código penal Vemos que este delito comprende al caso de usurpación de nombre, que no es otra cosa que la suplantación de una persona.

Las posibles causas del problema:

Como causas principales del problema se señala los siguientes; la innecesaria y superposición de tipos penales ya establecidos en nuestro código penal vigente. Así, la Ley Nº 30096 (2013) y su modificatoria la Ley Nº 30171 (2014) regula con el artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y señala: *El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1,2 y 4 del artículo 36 del código penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del código penal.* Con respecto de este artículo 5 nuestro código penal vigente *ya* contiene figuras que protegen la

libertad y la indemnidad sexual de las personas, independientemente del medio o herramienta que se haya utilizado para vulnerar dichos derechos. Así, tenemos los delitos de seducción (art. 175 cp.), actos contra el pudor (art. 176 cp.) y actos contra el pudor de menores (art. 176-A). Por lo que habría superposición de tipos penales.

Así mismo el artículo 7 de la Ley Nº 30096 (2013) su modificatoria la Ley Nº 30171 (2014) establece lo siguiente: *El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la ley 27806*[5]*. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organi1acion criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."* Esta figura ya viene siendo contenido en el artículo 162 del código penal que regula la interferencia telefónica y señala que: "El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años (…). Por lo que habría un exceso de regulación normativa y una superposición de tipos penales.

[5] Ley *27806, Ley de transparencia y acceso a la información pública.*

Por otro lado, el artículo 8 de la Ley Nº 30096 (2013) y su modificatoria la Ley Nº 30171 (2014) señala lo siguiente: *El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días de multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días de multa cuando se afecte el patrimonio del Estado destinado afines asistenciales o a programas de apoyo social*." con relación a este articulo 8, el código penal peruano ya contiene figuras que protegen el patrimonio vulnerado a través de actos de engaño y actos fraudulentos. Así, los artículos 196°, 196°-A y 197° del código penal regulan las formas de estafa de la siguiente manera: Artículo 196° Estafa.- *El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.* Artículo 196°-A.- Estafa agravada: *La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a doscientos días-multa, cuando la estafa: 1. Se cometa en agravio de menores de edad, personas con discapacidad, mujeres en estado de gravidez o adulto mayor. 2. Se realice con la participación de dos o más personas. 3. Se cometa en agravio de pluralidad de víctimas. 4. Se realice con ocasión de compra-venta de vehículos motorizados o bienes inmuebles. 5. Se realice para sustraer o acceder a los datos de tarjetas de ahorro o de crédito, emitidos por el sistema financiero o bancario.* Artículo 197° Casos de Defraudación.- *La defraudación será reprimida con pena*

privativa de libertad no menor de uno ni mayor de cuatro años y con sesenta a ciento veinte días-multa cuando: 1. Se realiza con simulación de juicio o empleo de otro fraude procesal. 2. Se abusa de firma en blanco, extendiendo algún documento en perjuicio del firmante o de tercero. 3. Si el comisionista o cualquier otro mandatario, altera en sus cuentas los precios o condiciones de los contratos, suponiendo gastos o exagerando los que hubiera hecho. 4. Se vende o grava, como bienes libres, los que son litigiosos o están embargados o gravados y cuando se vende, grava o arrienda como propios los bienes ajenos. Así NORTHCOTE[6] dice: "No encontramos la justificación para esta diferencia en el tratamiento de las figuras cuando el perjuicio en el patrimonio puede ser tanto o más grave en las figuras de estafa previstas en el Código Penal que en la figura del fraude informático".

Por último el artículo 9 de la Ley Nº 30096 (2013) Prescribe lo siguiente: *El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.* Sobre este punto el código penal ya contiene una figura en su artículo 438 sobre falsedad genérica, el texto normativo dice lo siguiente: *-El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.* Como se puede

[6] NORTHCOTE, C. (2013). Cometarios a la Ley de Delitos Informáticos. *Actualidad Empresarial*, 4(p. VIII-4).

apreciar de la regulación del código penal Vemos que este delito comprende al caso de usurpación de nombre, que no es otra cosa que la suplantación de una persona. Por ello nos preguntamos ¿si la suplantación sería más grave si se realiza con tecnologías de la información que mediante otras formas?, lo cual, nos parece, que no tiene un fundamento razonable, ya que el perjuicio para la persona es el mismo.

Cabe tener en cuenta que la Ley Nº 30096 publicado el 23 de octubre del año 2013 en el diario Oficial el Peruano se creo para llenar los vacios normativos; así, tenía por objeto prevenir y sancionar las conductas ilícitas mediante la utilización de tecnologías de la información o de la comunicación y de esta manera luchar contra la ciberdelincuencia , sin embargo, no estaria cumpliendo cabalmente con dicho objetivo, todo vez que se presentaron inconsistencias y ambiguedades luego de su inmedita publicacion, por lo que aproximandamente en un tiempo muy breve de aproximadamente de seis meses el 10 de Marzo de 2014 se publico una modificatoria la Ley Nº 30171.

Se observa que la regulacion apresurada, sin mayor analisis sobre los delitos informaticos en el futuro podria acarrear serias consecuencias, como cuando el agraviado no realiza la ponderacion de normas y ve entrampado si el ilicito o delito ocurrido esta dentro del codigo penal o de la Ley de delitos informaticos, esto debido a su superposicion normativa entre algunos articulos del codigo penal y la Ley de Delitos informaticos como ya se señalo lineas arriba.

Algunos expertos señala que la Ley de delitos informaticos pone en riesgo la libertad de expresion, afecta el acceso a la informacion por consiguiente debe ser derogado, modificado o incluso podria ser inconstitucional porque son ambiguas y afectan los derechos fundamentales de muchas personas.

1.2. Formulación del problema

1.2.1. Problema general.

¿De qué manera se muestran las inconsistencias y ambigüedades en la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento?

1.2.2. Problemas específicos.

a. ¿Existe superposición de tipos penales por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento?

b. ¿Existe exceso de regulación normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento?

1.3. Importancia del problema.

Desde que se inventó la computadora así como el sistema de comunicación masiva como el internet, las cifras de crecimiento de la criminalidad en materia de delitos informáticos ha sido problema de política criminal[7]. De allí, que existe la urgencia de establecer en el derecho penal ciertas conductas punitiva relacionadas con los avances tecnológicos de comunicación relacionados especialmente a la informática, y, en algunos casos verificar las innovaciones que pudieran darse en los tipos penales ya existentes.

Luis Bramont Arias, señala que la importancia del fenómeno informático es algo aceptado. El problema en cuanto a este fenómeno se traduce en buscar fórmulas efectivas de control, respecto a las cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social.

[7] Política criminal, es la reacción organizada de la sociedad, ante el desborde de conductas ilícitas que de alguna manera amenaza la paz social. Para ello recrea ciertos comportamientos punibles que los ciudadanos deben evitar cometerlos.

Nadie duda que el fenómeno informático produce en distintas ramas del ordenamiento jurídico, civil, procesal civil, mercantil, etc., un cierto trastorno a la hora de enfrentar tales hechos. Tal es la problemática generada por este fenómeno que ha motivado en la actualidad la necesidad de recurrir al derecho penal a fin de disuadir el uso abusivo al que lleva el empleo de computadoras, lo cual se ha plasmado ya en varias legislaciones extranjeras[8].

En el Perú, la codificación penal aún incipiente, no regula del todo los comportamientos delictivos derivados del uso de los llamados contactos virtuales (página web, internet, Facebook, etc.); sólo se consideran los delitos informáticos, en algunos casos como formas concursales mediales, siendo el delito fin uno de estafa u falsedad pública, etc. Es así, que el 22 de octubre de 2013 se publicó la Ley Nº 30096, Ley de delitos informáticos, esta Ley en vez de abordar y englobar temas no contenidas en el código penal vigente de 1991, presento muchas inconsistencias y ambigüedades en su regulación de delitos informáticos, hasta el extremo de regular lo ya estipulado en el código penal vigente de 1991 presentándose un exceso de regulación normativa. Por ello en tan solo 6 meses, el 10 de marzo de 2014 se publicó una nueva Ley 30171, Ley que modifica la Ley 30096, Ley de delitos informáticos, pese a esta reciente modificación y regulación normativa de los delitos informáticos aún existe inconsistencias y ambigüedades entre las Ley 30096 y su modificatoria la ley 30171 entre el código penal; por lo cual nos parece importante presentar un proyecto de Ley estableciendo rigurosamente las diferencias y precisiones entre los articulos superpuestos entre la Ley 30096 y su modificatotia la Ley 30171 entre el codigo penal peruano.

1.4. Justificación y viabilidad

1.4.1. Justificación teórica.

Esta investigación se circunscribe al tema de los Delitos informáticos Ley N° 30096 y sus modificatorias Ley N° 30171, la misma que tiene por objeto de evidenciar las inconsistencias y ambigüedades de la Ley, así como esclarecer la regulación normativa

[8] Ver en: http://www.teleley.com/5Bramont-51.pdf; extraído el 21-02-2017.

sobre los Delitos Informáticos y establecer precisiones ante las inconsistencias y ambigüedades entre la Ley de delitos informáticos Ley 30096 y su modificatoria Ley 30171 entre el código penal peruano y la realidad. Por lo que es muy importante evaluar cada artículo de la mencionada Ley.

1.4.2. Justificación práctica.

Se justifica por ser un problema latente en la sociedad actual donde los cambios sociales y tecnológicos hacen posibles los mundos virtuales, los mercados virtuales y las sociedades virtuales, que a su vez los medios y espacios para delinquir. Ese contexto la Ley de los Delitos Informáticos Ley N° 30096 y su modificatoria Ley N° 30171 busca regular estas nuevas formas de delinquir. En tal sentido el legislador ha incurrido en inconsistencias legales y ambigüedades, ya que algunos tipos penales ya son regulados por el Código Penal, superponiéndose los tipos penales.

1.4.3. Justificación Legal.

- ✓ La constitución Política del estado.
- ✓ El Código Penal.
- ✓ Ley Universitaria N° 30220.
- ✓ El Estatuto de la UNASAM.
- ✓ Reglamento General de Investigación de la UNASAM
- ✓ El Reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas de la UNASAM.
- ✓ Reglamento del Programa de Tesis guiada de la Facultad de Derecho y Ciencias Políticas de la UNASAM.

1.4.4. Justificación metodológica.

El paradigma metodológico que se empleará en la presente investigación será el enfoque cualitativo, es decir, se utilizará la recolección de datos sin medición numérica para describir o afinar preguntas de investigación en el proceso de interpretación de la Ley de Delitos Informáticos.

1.4.5. Justificación técnica.

Para la presente investigación se cuenta con el soporte técnico necesario, haciendo uso una computadora personal, impresora, escáner, y el Software respectivo Office 2015, haciendo uso de los programas del Word, Exel, los cuales fueron empleados en la etapa de planificación, ejecución y en la elaboración de la presente tesis.

1.4.6. Viabilidad.

El presente trabajo de investigación se centra en la ciudad de Barranca y responde como población de 30 entre profesionales de Derecho, Jueces y Fiscales. A quienes se le hará una encuesta para efectos de poder conocer sus pareceres sobre la inconsistencia y ambigüedad de la Ley de Delitos informáticos Ley N° 30096 y su modificatoria Ley N° 30171.

Respecto a la viabilidad de la presente investigación, podemos afirmar que cuenta con la viabilidad económica, bibliográfica, técnica y metodológica. Es decir, se cuenta con los recursos económicos para poder afrontar los gastos que ocasione el desarrollo de la presente investigación, los que serán cubiertos con recursos propios.

Así mismo la investigación es viable por se cuenta con los instrumentos necesarios para llevar a cabo la investigación, tales como: libros, laptop, papeles, impresora, etc. Se cuenta también con el capital humano necesario para realizar las encuestas, se cuenta

además con los profesionales del Derecho, docentes universitarios, jueces y fiscales a quienes poder aplicar la encuesta.

1.5. Formulación de objetivos.

1.5.1. Objetivo general.

Determinar de qué manera se muestran las inconsistencias y ambigüedades en la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, los cuales imposibilitan su eficaz cumplimiento.

1.5.2. Objetivos específicos.

a. Determinar de qué manera Existe una superposición de tipos penales por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento.
b. Determinar de qué forma Existe un exceso de regulación normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento.

1.6. Formulación de hipótesis.

1.6.1. Hipótesis General

a. La regulación y posterior sanción de los Delitos Informáticos en nuestro país son de suma importancia, pero debido a sus imprecisiones en su normatividad se está viendo ensombrecida, ello reflejado en las inconsistencias y ambigüedades encontradas en mencionados artículos de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, los cuales permiten el incremento de la Ciberdelincuencia o en su defecto que no se sancione a los responsables, imposibilitando su eficaz cumplimiento.

1.6.2. Hipótesis Específica

- Existe significativamente superposición de tipos penales por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley nº 30096 y su modificatoria Ley nº 30171.
- Existe significativamente exceso de regulación normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento.

1.7. Variables.

Las variables en la investigación, representan un concepto de vital importancia dentro de un trabajo de investigación. Las variables, son los conceptos que forman enunciados de un tipo particular denominado hipótesis. Así tenemos las siguientes variables:

Variable independiente:

Ley de Delitos Informáticos

Variable dependiente:

Inconsistencias y Ambigüedades

1.8. Metodología

1.8.1. Tipo y diseño de investigación.

1.8.1.1. Tipo

Corresponde a una Investigacion Jurídica, y de acuerdo al propósito de la Investigacion se permitio un nivel Dogmatico.

1.8.1.2. Diseño de investigación.

El diseño correspondió al denominado No Experimental[9], debido a que careció de manipulación intencional de la variable independiente, se observan los fenómenos en un ambiente natural y para después analizarlos[10].

Es una investigación de corte trasversal porque los datos se recolectaran en un único momento, su propósito es describir la variable y sus dimensiones de cada una de ellas y sus diferencia en un momento dado[11].

1.8.2. Plan de recolección de la información.

Para recoger la información necesaria y suficiente para alcanzar los objetivos de la investigación se empleó la Técnica Documental, cuyos instrumentos fueron las Fichas Textuales y de Resumen. Lo anterior permite realizar un plan de procesamiento y análisis de la información, basados en los objetivos. Para sistematizar la información en un todo coherente y lógico, es decir, ideando una estructura lógica, un modelo o una teoría que integre esa información se empleó el Método de Argumentación Jurídica.

1.8.3. Instrumentos de recolección de información.

El recojo de información del trabajo de campo se realizó a través de la Técnica Documental, empleándose como su instrumento las fichas, especialmente las Literales y de Resumen. También se utilizó la ficha de análisis de contenido para poder trabajar la doctrina respecto a nuestro problema de estudio.

Así como la realización de una Encuesta llevada a cabo en la ciudad de Barranca, durante el año 2018, en la cual participaron alrededor de 30 profesionales de Derecho, jueces y

[9] ROBLES TREJO, LUIS, Fundamentos de la Investigación Científica y Jurídica. Lima, Editorial Fecatt, 2012, p.34

[10] HERNÁNDEZ, FERNÁNDEZ, & BAPTISTA. *Metodología de Investigación.* México: Mc GRAUW-HILL Interamericana Editores S.A. de C.V. 2003, P. 58

[11] HERNÁNDEZ, FERNÁNDEZ, & BAPTISTA. *Metodología de Investigación.* México: Mc GRAUW-HILL Interamericana Editores S.A. de C.V. 2003, P. 270

Fiscales del Distrito Judicial/ Fiscal Huaura, respectivamente, con sede en la Provincia de Barranca.

Para el estudio de la normatividad se utilizó los métodos exegético y hermenéutico.

1.8.4. Plan de procesamiento y análisis de la información.

Los Datos que se obtuvieron con los instrumentos fueron evaluados en base a la teoría de la Argumentación Jurídica, toda vez que el Derecho puede concebirse como argumentación, la habilidad para presentar buenos argumentos a fin de justificar una postura.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes.

Se ha encontrado tesis y proyectos de investigación relacionadas con el presente trabajo.

- **A nivel internacional.**

SANCHEZ[12]. (2017). En su trabajo de investigación titulada *"*Análisis de la Ley 1273 De 2009 Y La Evolución De La Ley Con Relación a los delitos informáticos en Colombia Una aproximación al fenómeno de los jóvenes en el sicariato en la ciudad de Pereira*"* realizada en la Universidad Nacional Abierta y a Distancia -UNAD. Colombia. Para optar el Título de especialista en seguridad Informática, Llegó a las siguientes conclusiones sobre los delitos informáticos en Colombia señalando que:

- Dentro del desarrollo del presente proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia, teniendo en cuenta el origen y evolución de las nuevas tecnologías en el área dela informática y las telecomunicaciones.

  De esta forma, se observa la evolución en los métodos, técnicas o herramientas que pueden ser aplicaciones o dispositivos hardware que también se han desarrollado para facilitar la tarea de robo,

[12]SÁNCHEZ CASTILLO, ZULAY NAYIV (2017). *Análisis de la Ley 1273 de 2009 y la evolución de la Ley con relación a los delitos Informáticos en Colombia. Tesis.* Chichinquirà. Colombia.2017.

suplantación, estafa y demás delitos que puedan estar clasificados dentro de la lista creciente de las nuevas formas criminales de atentar contra la confidencialidad, integridad y disponibilidad de la información como activo primordial, así mismo que atentan contra los bienes de tipo mueble e intangibles con valor económico de las personas que son víctimas de los ataques o delitos informáticos. Por lo que con el presente proyecto se demuestra que aún falta normatividad en Colombia que logre abarcar todos los ámbitos de seguridad informática y que pueda sancionar correctamente este tipo de incidentes, que dejan daños en todos los entornos de desarrollo y crecimiento del país.

GONZÀLES (2013). En su trabajo de investigación titulada "Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta De reforma"[13], realizada en la Universidad Complutense de Madrid. Para optar el Título de doctor en Derecho, Arribo a las siguientes conclusiones en que trata la delincuencia informática en Madrid.

- La expansión exponencial de la ciberdelincuencia es innegable y así lo demuestra la dedicación que a estas nuevas prácticas delictivas han dado los diferentes Estados en sus normativas. Estamos ante un fenómeno relativamente novedoso, que además tiene una característica inherente al desarrollo tecnológico; la tecnología avanza a un ritmo vertiginoso, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho, esa misma

[13] GONZÁLES HURTADO, Jorge Alexandre. *DELITOS INFORMÁTICOS: Daños informáticos del artículo 264 del código penal y propuesta de reforma. Tesis.* Madrid.2013.

característica. Prueba de ello son los interesantes informes elaborados por el IC3 norteamericano donde se encuentran tablas cronológicas referidas al aumento de este tipo de delitos, e igualmente a las estadísticas que manejan las empresas privadas en cuyos múltiples informes también se recoge el indudable crecimiento exponencial de estas conductas prohibidas, o la recentísima puesta en funcionamiento del EC3 en la Unión Europea para coordinar la respuesta ante ciberataques en los Estados de la Unión.

GUERRA (2011) En su trabajo de investigación titulada "Delitos Informáticos-Caso De Estudio[14]" realizada en el instituto politécnico nacional de México. Para obtener el Grado de maestro en ingeniería en seguridad y tecnologías de la información, Llegó a las siguientes conclusiones con relación a los delitos informáticos en México:

- Los delitos informáticos en México, no son exclusivos de la competencia en materia penal, la diversidad de delitos variará con respecto a las ideas que tengan las personas que hagan uso de medios tecnológicos para delinquir. Los delitos informáticos no pueden ser una actividad que se someta al capricho temporal que vive día a día la sociedad y que está en constante crecimiento; por ende, se debe de aspirar a la creación de una ley más eficaz y amplia. México no puede permanecer en el caso de que se tengan que sufrir consecuencias para dar resultados, la jurisprudencia debe de ayudar a mejor legislación en cuanto a vacíos legales, sin embargo resulta complicado que haya

[14] GUERRA VALDIVIA, Alicia Rubí. *Delitos Informáticos-Caso de estudio. Tesis.* Mexico.2011.

resoluciones al respecto, sin antes existir una ley que los regule. No es posible seguirse apegando a figuras típicas que no resuelvan una problemática específica, pues desde su formación se puede apreciar si estas figuras cumplirán con el objeto primordial del derecho: lograr una correcta relación entre los miembros de la sociedad.

SANCHEZ & FERNANDEZ[15] (2009). En su trabajo de investigación titulada "proyecto de Investigación: delitos informáticos" realizada en el instituto tecnológico de Durango, Llegó a las siguientes conclusiones con respecto de los delitos informaticos:

- Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

  La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

[15] REYES SÁNCHEZ, Yuridia & FERNANDEZ ARAMBURO, Ever. *Proyecto de Investigación: Delitos Informáticos.* Durango.2009.

- **A nivel nacional.**

RUMICHE[16] (2015). En su trabajo de investigación titulada "Sombras de la normatividad que regula el incremento de la ciberdelincuencia" realizada en la Universidad Nacional José Faustino Sánchez Carrión de Huacho –Perú. Para obtener el Título de Abogado, Arribo a las siguientes conclusiones:

- Se logró determinar que el ejercicio de la actual normatividad que regula la ciberdelincuencia en lima 2015, contraviene en constates disyuntivas ya que es una carta abierta para su correcta aplicación y por lo tanto incide de manera significativa sobre todo en la manera de como se le brinda la adecuada protección al ciudadano, por ende su desfavorable aplicación puede llegar a causar un penoso impacto en nuestra sociedad. De la misma forma se puede establecer que si en la práctica se generaran tantos errores judiciales se devendría en ilegal, y por ende se generaría en inconstitucional. Todo ello generaría un gran impacto constitucional.

- Señalar que es evidente que la falta de cultura informática es un factor Crítico en el impacto de los delitos informáticos en la sociedad en general, los operadores de justicia cada vez deben tener mayores conocimientos en tecnología de la información.

- En nuestra actualidad es un poco riesgoso hacer negocios vía Web ya que los instrumentos legales no garantizan con un adecuado marco legal para su efectividad.

[16] RUMICHE PAZO, José Alfonso. *Sombras de la Normatividad que regula el incremento de la ciberdelincuencia en Lima 2015. Tesis.* Huacho- Peru. 2015.

HIDALGO[17] (2011).En su trabajo de investigación titulada "Delincuentes Modernos en la Ciudad de la Oroya: En Delitos Informáticos", realizada en la Universidad de Huánuco, Llegó a las siguientes conclusiones con relación a los delitos informáticos en la Oroya.

- Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

- La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

- Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el

[17] HIDALGO ÁVILA, Cesar Raúl. *Delincuentes Modernos en la Ciudad de la Oroya: En Delitos Informáticos. Tesis.* Oroya - Peru.2011.

único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

2.2. Bases teóricas.

2.2.1. Teoría jurídica.

El delito informático en un inicio se encontraba tipificado en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991. Esta regulación no era propia de un delito autónomo, sino como una agravante del delito de hurto[18]. Posteriormente, los delitos informáticos fueron incorporados por la Ley 27309[19] y estaban previstos en el Capítulo X del Código Penal: 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 cualificantes agravantes), 207-D (tráfico ilegal de datos), y en las leyes penales especiales.

Entre estas leyes penales especiales, se encuentra la Ley Nº 30096 [20]. Esta Ley de Delitos informáticos está conformada por siete capítulos que se estructuran de la siguiente manera: Finalidad y objeto de la Ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos Contra la fe pública (Capítulo VI) y las disposiciones comunes(Capítulo VII).

Posteriormente se promulgó la Ley Nº 30171[21], La finalidad de esta ley fue adecuar la Ley 30096 a los estándares legales del convenio sobre la *cibercriminalidad*

[18] BRAMONT - ARIAS, Luís. Delitos Informáticos. *Revista Peruana de Derecho de la Empresa, Derecho informático.2000.*

[19] Ley 27309. Ley que Incorpora los Delitos Informáticos al código penal. 17 de julio de 2000

[20] Ley Nº 30096, Ley de Delitos Informáticos. 22 de octubre de 2013.

[21] Ley Nº 30171, *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. 10 de marzo de 2014.

(en adelante Convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10 de la referida Ley la posibilidad de cometer el delito deliberada e ilegítimamente. Las modificaciones de la Ley Nº 30171 (2014), con respecto a los delitos informáticos, son las siguientes:

- Artículo 1; Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley Nº 30096 (2013) *Ley de Delitos Informáticos*.
- Artículo 2; Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096 *Ley de Delitos Informáticos*.
- Artículo 3; Incorporación del artículo 12 a la Ley 30096 *Ley de Delitos Informáticos*.
- Artículo 4; Modificación de los artículos 158, 162 y 323 del Código Penal.
- Artículo 5; Incorporación de los artículos 154-A y 183-B del Código Penal.
- Única Disposición Complementaria Derogatoria; Deroga el artículo 6 de la Ley 30096 *Ley de Delitos Informáticos*.

2.2.2. Variable dependiente.

Inconsistencia:

En derecho, la inconsistencia en las pruebas que se presentan puede ser un causal de culpabilidad en el caso que se intente con estas demostrar una inocencia. Es decir, si las pruebas no son lo suficientemente claras, no se sabe a ciencia cierta cuál es la procedencia de las mismas, no se tiene un claro panorama de la función de estas en torno a su veracidad.

Simplemente, la inconsistencia es la falta de solidez, en la mayoría de los casos, se necesita de la firmeza de algún material o instrumento para realizar una estructura con él, de lo contrario, dicha estructura también cederá debido a su inconsistencia. Es un

término relativo, como sustantivo, depende del entorno que lo rodea, las variables que lo afectan y los sentidos que se aplican para poder entender cómo funciona22.

Ambigüedad.

Concepto.

Ambigüedad es calidad de ambiguo. A su vez, los sinónimo de la palabra ambiguo son: confuso, oscuro, indeterminado, impreciso, etcétera. Por lo tanto, ambiguo es un adjetivo que hace referencia a todo aquello que puede entenderse de varias maneras23.

El término ambiguo hace alusión a todo aquello que puede tener más de un sentido o significado. Algunos ejemplos de palabras ambiguas son: apuntar (escribir o indicar algo), banco (mueble para sentarse, banco de peces, institución bancaria), carta (correspondencia, naipe de baraja y menú de los restaurantes), entre otras.

Definición:

La ambigüedad lingüística se da cuando una palabra, un sintagma, o una oración, es susceptible de dos o más significados o interpretaciones. La ambigüedad puede ser sintáctica (o estructural), semántica, o pragmática.

La palabra, sintagma u oración se puede entender de más de una manera; en tal sentido la ambigüedad tiene mucho que ver con la figura retórica o tropo llamado anfibología[24] y, por otra parte, con el doble sentido[25].

[22] Consultado en: http://conceptodefinicion.de/inconsistencia/

[23] Consultado en: https://www.significados.com/ambiguedad/

[24] La anfibología es el empleo de frases o palabras con más de una interpretación. También se la llama disemia (dos significados) o polisemia (varios significados) aunque, estrictamente hablando, una polisemia no es siempre una anfibología.

[25] Consultado en: https://es.wikipedia.org/wiki/Anfibolog%C3%ADa

En sentido genérico, la ambigüedad es el atributo de cualquier concepto, idea, declaración, presentación, o reclamación, cuyo sentido, intención, o interpretación, definitivamente no pueden ser resueltos según una regla o un proceso resoluble en un número finito de pasos.

2.2.3. Variable independiente.

2.2.3.1. Ley de delitos informáticos.

2.2.3.1.1. Concepto de delito informático.

ESTRADA[26] señala que El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión 'delitos informáticos' esté consignada en

[26] ESTRADA GARAVILLA Miguel. Delitos informáticos. S/f.

los códigos penales, lo cual en México, al igual que en otros muchos países, no ha sido objeto de tipificación aún".

Para Carlos Sarzana, en su obra Criminalita e Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española".

María de la Luz Lima dice que el delito electrónico "en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

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". Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

i. 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.

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

iii. 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.

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

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

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

vii. Son muy sofisticados y relativamente frecuentes en el ámbito militar.

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

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

x. Ofrecen facilidades para su comisión a los menores de edad.

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

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

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático. Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en Perú debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

2.2.3.1.2. Finalidad y objeto de la Ley de delitos informáticos.

El artículo 1º[27] de la *Ley de delitos informáticos* establece que el objeto de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas

[27] El artículo 1 de la *Ley 30096, Ley de delitos informáticos*

informáticos, y otros bienes jurídicos de relevancia penal (como el patrimonio, la fe pública, la libertad sexual, etcétera) que puedan ser afectados mediante la utilización de las TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y al desarrollo. Con esta Ley se intenta garantizar la lucha eficaz contra la ciberdelincuencia.

VILLAVICENCIO[28] señala que: Esta Ley no responde solo a la necesidad de ejercer la función punitiva del estado enfocado en la protección de la información; sino que tiene como principal objetivo la estandarización de la Ley Penal peruana con el ordenamiento penal internacional, principalmente por el Convenio contra la *cibercriminalidad* del Consejo europeo (CETS 185), denominado Convenio de Budapest.

2.2.3.1.3. Bien jurídico tutelado

VILLAVICENCIO[29] Refiere que: El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la *información* de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera. Respecto de la información deber ser entendido como el contenido de las bases y/o banco de datos o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico. Y es la importancia del *valor económico* de la información lo que ha hecho que se incorpore como bien jurídico tutelado. sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco

[28] VILLAVICENCIO Terreros, Felipe. *Revista IUS ET VERITAS, N° 49, Diciembre.*, P.288. 2014.

[29] VILLAVICENCIO Terreros, Felipe. *Revista IUS ET VERITAS, N° 49, Diciembre.*, P.288. 2014.

de la persona por la fluidez y el trafico jurídico, y por los sistemas que lo procesan o automatizan, los mismos que se equiparan a los bienes protegidos tradicionalmente, tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), la seguridad o fiabilidad del trafico jurídico probatorio (falsificación de datos o documentos probatorios), etcétera.

Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado[30], por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. En es ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal[31].

2.2.3.1.4. Perfil del ciberdelincuente.

El perfil del ciberdelincuente -*sujeto activo*- en esta modalidad delictual requiere ciertas habilidades y conocimientos en el manejo del sistema informático[32], por ello también se les ha calificado como delincuentes de "*cuello blanco*"[33], que tienen como características:

- Poseer importantes conocimientos informáticos.

[30] GONZALES DE CHAVES CALAMITA, María E. El Llamado: Delitos informáticos. *Anales de la Facultad de Derecho de la Universidad de la Laguna, Nº 21. España*, PP.44-45.2004.

[31] VILLAVICENCIO Terreros, Felipe. *Revista IUS ET VERITAS, N° 49, Diciembre.*, P.289. 2014.

[32] AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág.27.

[33] Se le denomina así a la delincuencia informática debido a los estudios sobre criminalidad informática orientados en las manifestaciones en el ámbito económico patrimonial, donde la doctrina determino que el sujeto activo del delito informático poseída un alto nivel socioeconómico", en AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", óp., cit., pág. 27- 28.

- Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (*se denomina delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema*).

Para Marcelo Manson, los infractores de la Ley penal en materia de Delitos Informáticos no son delincuentes comunes y corrientes sino que por el contrario, son personas especializadas en la materia informática[34].Agrega que "*las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es habilidades para el manejo de los sistemas informáticos y que por su situación laboran en puestos estratégicos donde se manejan información sensible."* Por su parte, Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas[35]. Tambien, Vives Antón y Gonzales Cussac afirman que "sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (operadores, programadores u otros), como terceros no autorizados que acceden a las terminales públicas o privadas"[36]

Gutiérrez Francés y Ruiz Vadillo difieren de estos puntos de vista y sostienen que "el autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados"[37].

Por nuestra parte, si bien consideramos que el sujeto activo puede ser cualquier persona (con conocimientos y habilidades en informática) y compartimos parcialmente la postura que el sujeto activo debe ocupar un puesto laboral que le permita acceder a

[34] MANSON, Marcelo; "Legislación sobre delitos informáticos", **en** https://dl.dropbox.com/u//dl. legislacioncomparada.pdf. [visto el 27 de diciembre 2013].
[35] CAMACHO LOSA, L; "El delito informático" GRAFICAS CONDOR, Madrid 1987, pág. 83- 84.
[36] VIVES ANTÓN y GONZÁLES CUSSAC, "Comentarios al código Penal 1995", Ed. TIRONT BLANCH, Valencia 1996, pág. 1238.
[37] GUTIERRES FRANCES, M; "Fraude informático y estafa"/ RUIZ VADILLO, E; "tratamiento a la delincuencia informática", en AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", óp., cit., pág. 29.

información sensible, sin embargo, no están excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática. Por ende, se trata de delitos de dominio.

Se pueden identificar diferentes sujetos activos que se les denomina de diferente manera dependiendo del modo como actúan y que conductas son las que realizan:

i. HACKERS.- Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, conocido como "delincuente silencioso o tecnológico". Les gusta indagar por todas partes, conocer el funcionamiento de los sistemas informáticos; son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. Para Sieber los hacker son "personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado"[38]. Morón Lerma define a los hacker como "personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado"[39]

ii. CRACKERS. Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como "piratas electrónicos." La característica que

[38] SIEBER, Ulrich: "Criminalidad informática: peligro y prevención", pág. 77, MIR PUIG, S; "Delincuencia informática".
[39] MORON LERMA, ESTHER; "Internet y Derecho Penal: hacking y otras conductas ilícitas en la red", ED. ARANZADI, Navarra, 2002, 2° ed., pág. 51.

los diferencia de los hacker es que los crackers usan programas ya creados que pueden adquirir, normalmente vía internet; mientras que los hackers crean sus propios programas, tiene mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos[40]29 .Por otra parte, Morant Vidal define a estos sujetos como "personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas"[41]30. También, Alfonso Laso sostiene que el cracker "es la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etc."[42].

2.2.3.1.5. Características del sujeto activo

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin

[40] AZAOLA CALDERON, Luis; óp., cit., pág. 32.
[41] MORANT VIDAL, J; "protección penal de la intimidad frente a las nuevas tecnologías", Ed. PRACTICA DE DERECHO, Valencia, 2002, pág. 44.
[42] DE ALFONSO LASO, D; "El hackerin blanco. Una conducta ¿punible o impune?", en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial, Madrid, 2001, pág.110- 111.

intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de habilidades no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de cuello blanco, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como delitos de cuello blanco, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

Asimismo, este criminólogo estadounidense dice que tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no son de acuerdo al interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil

descubrirlo y sancionarlo en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

2.2.3.1.6. Características del sujeto pasivo.

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad

de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

2.2.3.1.7. Clasificación de los delitos informáticos.

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

- **Como instrumento o medio:** en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:
    a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
    b. Variación de los activos y pasivos en la situación contable de las empresas.
    c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).
    d. Lectura, sustracción o copiado de información confidencial.
    e. Modificación de datos tanto en la entrada como en la salida.
    f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
    g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
    h. Uso no autorizado de programas de cómputo.
    i. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
    j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l. Acceso a áreas informatizadas en forma no autorizada.

m. Intervención en las líneas de comunicación de datos o teleproceso.

- **Como fin u objetivo:** en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

    a. Programación de instrucciones que producen un bloqueo total al sistema.

    b. Destrucción de programas por cualquier método.

    c. Daño a los dispositivos de almacenamiento.

    d. Atentado físico contra la máquina o sus accesorios.

    e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

    f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

a. ***Los que utilizan la tecnología electrónica como método***: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b. ***Los que utilizan la tecnología electrónica como medio:*** conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

c. ***Los que utilizan la tecnología electrónica como fin:*** conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

En lo que se refiere a delitos informáticos, Olivier Hance en su libro Leyes y Negocios en Internet, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a. ***Acceso no autorizado:*** es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.
b. ***Actos dañinos o circulación de material dañino:*** una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).
c. ***Interceptación no autorizada:*** en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.
d. ***Las leyes estadounidense y canadiense***, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y

penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

2.2.3.1.8. Tipos de delitos informáticos reconocidos por la organización de las naciones unidas (ONU)

A. Fraudes cometidos mediante manipulación de computadoras.

a. ***Manipulación de los datos de entrada:*** este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b. ***La manipulación de programas:*** es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c. ***Manipulación de los datos de salida:*** se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin

embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d. ***Fraude efectuado por manipulación informática:*** aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

B. **Falsificaciones informáticas.**

a. Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

b. Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

C. Daños o modificaciones de programas o datos computarizados.

a. ***Sabotaje informático:*** es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el

funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

i. **Virus**: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

ii. **Gusanos:** se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

iii. **Bomba lógica o cronológica:** exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su "detonación" puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento

de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

b. **Acceso no autorizado a servicios y sistemas informáticos:** se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

   i. **Piratas informáticos o hackers**: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c. **Reproducción no autorizada de programas informáticos de protección legal:** ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- ***Acceso no autorizado***: uso ilegitimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.
- ***Destrucción de datos:*** los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- ***Infracción al copyright de bases de datos:*** uso no autorizado de información almacenada en una base de datos.
- ***Interceptación de correo electrónico:*** lectura de un mensaje electrónico ajeno.
- ***Estafas electrónicas:*** a través de compras realizadas haciendo uso de la red.
- ***Transferencias de fondos:*** engaños en la realización de actividades bancarias electrónicas. Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:
    a. Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
    b. Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
    c. Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

d. Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

2.2.3.1.9. De los delitos informáticos en la Ley N° 30096 y su modificatoria Ley N° 30171

1. Delitos contra datos y sistemas informáticos (CAP. II)

Este capítulo está conformado por las siguientes figuras penales: **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".

Esta figura penal de *Acceso ilícito* sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático; el verbo rector "***acceder***[43]**"** se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema, y el término

[43] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=acceder [visto el 8 de enero 2018].

"vulnerar[44]" se entiende como *"transgredir, quebrantar, violar una ley o precepto"* que se entiende al hecho de trasgredir las barreras de protección diseñados por el sistema.

Por la característica que presenta este tipo penal -*acceso ilícito*- se le puede calificar como un *delito de mera actividad*, porque esta figura exige el acto de acceder *(entrar en un lugar o pasar a él)* sin autorización a un sistema informático, vulnerar *(transgredir, quebrantar, violar una ley o precepto)* las medidas de seguridad, de esta manera se configura el ilícito; por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo. *Vgr. el acceso a la cuenta de correo electrónico ajeno protegido mediante una contraseña de seguridad, el acceso no autorizado al sistema informático de una entidad aprovechando las debilidades inadvertidas por la programación*.

La fuente legal de este artículo es el Convenio de Budapest, porque cumple con describir la acción delictiva en los mismos términos estandarizados de la norma internacional: por mencionar los términos "*deliberación*", "*falta de legitimación*"[45] de la acción contenida en el texto del Convenio de Budapest guarda cierta identidad con el dolo (conocimiento y voluntad)[46].

> **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".**

[44] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=vulnerar [visto el 09 de Enero 2018]
[45] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 2º.- Acceso ilícito.
[46] VILLAVICENCIO TERREROS, Felipe, "Derecho Penal- Parte general", Ed. Grijley, Lima, 2013, pág. 354

Esta figura penal sanciona la conducta de dañar (causar detrimento, perjuicio, menoscabo), introducir (entrar en un lugar), borrar (desvanecer, quitar, hacer que desaparezca algo) deteriorar (empeorar, degenerar), alterar (estropear, dañar, descomponer), suprimir[47] (hacer cesar, hacer desaparecer) y hacer inaccesible los datos

Informáticos a través de la utilización de las TIC; por la característica que presenta este tipo penal –atentado a la integridad de los datos informático- es clasificado como un delito de mera actividad, porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior, por tanto el delito queda consumado al realizarse cualquiera de estos Actos.

Este artículo es compatible parcialmente con el Art. 4º del Convenio de Budapest[48] que sanciona el atentado contra la integridad y la disponibilidad del dato informático.

> **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".**

Está figura penal sanciona las conductas que están dirigidas a inutilizar[49] (hacer inútil, vano o nulo algo) total o parcialmente un sistema informático, entorpecer[50]

[47] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=suprimir [visto el 09 de Enero 2018].
[48] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 4º.Ataques a la integridad de los datos.
[49] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=inutilizar [visto el 9 de enero marzo 2018].
[50] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 9 de Enero de 2018].

(retardar, dificultar). E imposibilitar[51] *(quitar la posibilidad de ejecutar o conseguir algo)* su funcionamiento o la prestación de sus servicios utilizando las TIC; por la característica que presenta este tipo penal –*atentado contra la integridad de sistemas informáticos*- se clasifica como un *delito de resultado,* porque para la configuración de este injusto penal no basta con cumplir el tipo que es *(inutilizar o perturbar)*, sino además es necesario que la acción vaya seguida de un resultado *(impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios),* por tanto el delito se consuma cuando se impide el *acceso, imposibilita su funcionamiento, etc.*, del sistema informático, caso contrario el hecho solo dará lugar a la *tentativa.*

Este artículo guarda cierta relación de compatibilidad con el Art. 5º del Convenio de Budapest[52] en tanto se puede entender la "obstaculización grave" de un sistema informático con el de la "inutilización total o parcial" del sistema.

Son ejemplos de esta figura penal los siguientes delitos:

- *Delito de daño*.- comportamiento consistente en dañar, destruir o inutilizar un bien, en este caso es el sistema informático, expresa Bramont- Arias que el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito; la destrucción total de programas y de datos ponen en peligro la estabilidad económica de una empresa[53].El *modus operandi* se viene perfeccionando con el tiempo: *virus, cáncer rotudtine*. Estos actos deben causar un perjuicio patrimonial.

[51] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=imposibilitar [visto el 9 de enero 2018].
[52] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 5º.- Ataques a la integridad del sistema.
[53] BRAMONT- ARIAS, Luis A.; "Delitos informáticos", en Revista Peruana de Derecho de la Empresa, DERECHO INFORMATICO Y TELEINFORMATICA JURIDICA, Nº 51, ASESORANDINA. Lima.2000.

- *El sabotaje informático*.- consiste, básicamente, en *borrar, suprimir o modificar (alterar)* sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como "virus informático"[54] Marchena Gómez señala que el "*sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños*"[55] 51. Morant Vidal señala que "*el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas*" [56]

Las técnicas que permiten cometer sabotaje informático son las siguientes[57]:

- **Bomba lógica.-** introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.
- **Rutinas cáncer**.- Son distorsiones al funcionamiento del programa, la característica es la auto reproducción.
- **Gusano**s.- Se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse.
- **Virus informático y malware**.- Elementos informáticos que destruyen el uso de ciertos antivirus[58] . Vgr. borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente; cambiar la clave secreta o eliminar

[54] AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 69
[55] MARCHENA GOMEZ, M; "El sabotaje informático: entre los delitos de daños y desordenes públicos", en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid 2001, pág. 356.
[56] MORANT VIDAL, J; "Protección penal de la intimidad frente a las nuevas tecnologías", Ed. RACTICA DE DERECHO, Valencia 2003, pág. 46- 47.
[57] AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 70.
[58] MATA BARRANCO, Norberto J/ HERNÁNDEZ DÍAZ, Leyre; "El delito de daños informativos: una tipificación defectuosa"; **en**, Revista de Estudios Penales y Criminológicos, Vol. XXIX, España, 2009, pág. 311- 362.

la cuenta electrónica (correo, twitter, Facebook) para impedir al titular el acceso a su cuenta.

2. Delitos informáticos contra la indemnidad y libertad sexuales (CAP. III)

Este capítulo está conformado por el tipo penal del Art. 5º (proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos), que sanciona la propuesta sexual (solicitar u obtener material pornográfico, llevar a cabo actividades sexuales) 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 artículo 36° del código Penal".

Se sanciona el *contacto (establecer contacto o comunicación con alguien) realizado* con un menor de edad con fines a obtener material pornográficos o con el propósito de llevar a cabo actividades sexuales que involucren el quebrantamiento de la indemnidad o libertad sexual del menor (*violación sexual o actos contra el pudor*); en este artículo hay dos supuestos:

1. El primer supuesto es el **contacto** con un *menor de catorce* años para solicitar, obtener material pornográfico o para realizar actos sexuales, cuya pena es de 4 a 8 años de pena privativa de libertad e inhabilitación.

2. El segundo supuesto es el **contacto** con un *menor que tiene entre catorce y dieciocho* años para solicitar, obtener material pornográfico o para realizar actos sexuales, cuya pena es de 3 a 6 años de pena privativa de libertad e inhabilitación

Este tipo sanciona el acto de *contactar* que significa *"establecer contacto o comunicación con alguien"*, y el término "*para*" es un elemento subjetivo que determina la intención del sujeto activo y es este elemento que convierte a la figura penal en un *tipo de tendencia interna trascendente (delitos de intención)*[59] , porque este ilícito "parte interna" requiere de una intención especial, que no corresponde a la parte externa objetiva que en este caso es obtener material pornográfico y/o tener actividades sexuales con el menor; por consiguiente, el tipo legal queda consumado cuando se produce el resultado típico, no siendo necesario que el agente consiga realizar su especifica tendencia trascendente, por estas características se clasifica a esta figura como un *delito de resultado cortado,* porque en este ilícito el agente persigue un resultado que está más allá del tipo y que ha de producirse por sí solo, sin su intervención y con posterioridad[60].

En esta figura penal el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de contactar con el menor de edad, sin importar si logra su objetivo el cual es obtener material pornográfico o llegar a tener actividad sexual, sin embargo este articulo tiene muchas falencias que podría violar el principio de legalidad, al no tener una redacción clara, y a consecuencia de este error se podría sancionar a personas que solo contactan con un menor de edad sin tener la finalidad de obtener material pornográfico y otro similar porque el término *contactar* no está delimitado, por

[59] VILLAVICENCIO TERREROS, Felipe; "Derecho Penal- Parte General", 3° reimpresión de la 1° ed., GRIJLEY, Lima 2010 pág. 375, Define a los tipos de tendencia interna trascendente como aquellos delitos "cuya parte interna requiere de una intención especial que consiste en la búsqueda de un resultado diferente al exigido típicamente y que, por ende, no es exigente para la consumación del delito, debiendo entenderse solo para efectos de llenar el tipo".
[60] VILLAVICENCIO TERREROS, Felipe, op. cit. Pág. 375.

consiguiente se estaría sancionando el solo hecho de establecer un "contacto" o comunicación con un menor de edad.

- **Delitos contra la libertad sexual**.- son acciones destinado a vulnerar tanto la indemnidad sexual como la libertad sexual del menor. Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder a la actividad sexual, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática.
- **Pornografía infantil**.- en esta conducta tipificada se denota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos y otros y, su intimidad[61].
- Lo que se busca sancionar con esta tipo penal es el acto de ofrecer, vender, distribuir, exhibir material pornográfico de menores de edad. Esta conducta está referida a un sujeto activo indiferenciado (delito de dominio), es de mencionar que esta modalidad es dolosa: el sujeto ha de conocer la naturaleza del material y ha de querer realizarlo, difundir o poseer con dichos fines siendo indiferente que lo haga con ánimo lubrico o de lucro.

3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones (CAP. IV)

[61] ORTS BERENGUER, Enrique/ ROIG TORRES, Margarita; "Delitos informáticos y delitos comunes cometidos a través de la informática", TIRANT LO BLANCH, Valencia 2001, pág. 129.

Este capítulo está conformado por las siguientes figuras penales: **Art. 6º** (Derogado por la ley 30171 Ley que Modifica la Ley 30096, Ley de Delitos Informáticos[62]), **Art. 7º** (interceptación de datos informáticos).

Art. 6°.- (derogado por la Única Disposición Derogatoria de la Ley 30171 "Ley que modifica la Ley 30096")

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."

[62] El artículo 6º de la Ley Nº 30096, Ley de Delitos Informáticos; fue derogado por la UNICA DISPOSICION COMPLEMENTARIA DEROGATORIA de la Ley Nº 30171 "Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos"

La figura penal sanciona la conducta que deliberada e ilegítimamente intercepta[63] *(Interrumpe, obstruye una vía de comunicación)* datos informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas. Este artículo contiene tres agravantes:

- ✓ El primer agravante se aplica cuando la interceptación recaiga sobre *información clasificada como secreta, reservada o confidencial,* de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública. cuya penalidad oscila entre cinco a ocho años.
- ✓ El segundo agravante se aplica cuando la interceptación recaiga sobre *información que compromete a la defensa, seguridad o soberanía nacional*, cuya penalidad oscila entre ocho a diez años.
- ✓ La tercera agravante consiste en la calidad del agente –*integrante de una organización criminal*- comete el delitos como cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Este injusto penal -*interceptar datos informáticos*- es un delito de *peligro abstracto* y por ende, solo basta con demostrar la interceptación de datos informáticos para que el delito quede consumado. Por ende, se clasifica como un *delito de mera actividad* porque basta con el sólo hecho de interceptar datos informáticos para que se consuma el delito. *Vgr. interceptación de archivos que contengan información relacionado con una investigación reservada por ley, interceptación de comunicaciones que contenga información sensible que puede ser utilizado por algún país en un contexto bélico.*

[63] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=interceptar (visto el 10 de ENERO 2018).

4. Delitos informáticos contra el patrimonio (CAP. V)

Este capítulo está integrado por el **Art. 8** (*fraude informático*), que sanciona la acción de *diseñar, introducir, alterar, borrar, suprimir y clonar datos informáticos* en perjuicio de tercero.

> *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*".

Este injusto penal –*fraude informático*- sanciona diversas conductas, entre ellos: diseñar *(proyecto o plan)*, introducir *(entrar en un lugar)*, alterar *(estropear, dañar, descomponer)*, borrar *(desvanecer, quitar, hacer que desaparezca algo)*, suprimir *(hacer cesar, hacer desaparecer)66*, clonar *(producir clones)* datos informáticos o cualquier interferencia, o manipular *(operar con las manos o con cualquier instrumento)* el funcionamiento de un sistema informático procurando *(conseguir o adquirir algo)*[64] un beneficio para sí o para otro en perjuicio de tercero; y por la forma como está estructurado–*a propósito de la mala redacción que genera mucha confusión al momento de interpretar la figura, y las conductas inadecuadas como "diseñar, introducir, alterar,*

[64] Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 9 de enero 2018].

borrar y suprimir" que no encajan en el delito de fraude informático, estas conductas son propios del delito de daño- se clasifica como un *delito de resultado* porque no basta cumplir con el tipo penal para que se consume el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa. *Vgr. Clonar tarjetas bancarias, el fraude informático afecta los programa social JUNTOS, PENSIÓN 65, destinados a apoyo social.*

Este artículo es compatible con el Art. 8 del Convenio de Budapest[65], porque ambos artículos sancionan el empleo indebido de datos informáticos, la manipulación del funcionamiento del sistema mismo.

5. Delitos informáticos contra la fe pública (CAP. VI)

El Art. 9º de la ley (*suplantación de identidad*), sanciona la suplantación de identidad de una persona natural o jurídica, siempre que de esto resulte algún perjuicio.

> 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".

Este tipo penal sanciona el hecho se suplantar[66] *(ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba)* la identidad de una persona natural o jurídica causando algún perjuicio.

[65] Ver Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 2º, Art. 8º.- fraude informático.
[66] Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=suplantar (visto el 28 de marzo 2014).

La *suplantación de identidad* se puede calificar como un delito de resultado porque no basta con realizar la conducta típica de "*suplantar*" la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta que consiste en causar un perjuicio, caso contrario quedaría en tentativa. *Vgr. crear perfiles falsos en las redes sociales (correo electrónico, Facebook, twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros*[67].

6. Disposiciones comunes (CAP. VII)

El capítulo VII de la ley está integrado por las siguientes figuras penales: **Art. 10º** (*abuso de mecanismos y dispositivos informáticos*) y el **Art. 11º** *(agravantes*).

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

Se sanciona diversas conductas, entre ellas : fabricar *(producir objetos en serie, generalmente por medios mecánicos)*, diseñar *(hacer un diseño)*, desarrollar, vender *(traspasar a alguien por el precio convenido la propiedad de lo que uno posee*) , facilitar *(proporcionar o* entregar), distribuir *(entregar una mercancía a los vendedores y*

[67] "una abogada había sido suplantada en el Facebook y correo electrónico, por la pareja de su amiga, fingiendo ser lesbiana, para captar personas y ganarse la confianza a través del falso perfil y poder obtener materiales (fotos intimas) que luego eran utilizados para extorsionar a sus víctimas que ingenuamente creyeron estar en contacto con la persona suplantada, este acto trajo perjuicios económico, laboral, familiar, psicológico a la suplantada", CUARTO PODER REPORTAJE DE NOTICIA DE FECHA (02/12/13).

consumidores) , importa *(dicho de una mercancía: valer o llegar a cierta cantidad)*[68] *y* obtener *(alcanzar, conseguir y lograr algo que se merece, solicita o pretende),* para la utilización de mecanismos, programas informáticos, contraseñas, etc., diseñados específicamente para la comisión de los delitos previstos en esta ley. Este artículo es una expresión del adelantamiento de las barreras punitivas porque se sanciona la participación y más aún el sólo hecho de ofrecer un servicio que facilite la comisión de algún delito previsto en la presente ley.

Este tipo penal –*abuso de mecanismos y dispositivos informáticos*- se clasifica como un *delito de mera actividad*, porque la figura exige cumplir con la conducta mencionado en el tipo penal para la consumación del delito sin importar el resultado posterior. Aquí el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de fabricar, diseñar, vender, etc., mecanismos, programas orientados a cometer diversos delitos previstos en la ley. Esta figura penal poseería las características del llamado *derecho penal del enemigo* porque se sanciona actos preparatorios alegando la puesta en peligro de la seguridad informática. *Vgr. tráfico de datos de usuarios y contraseñas obtenidas ilícitamente para cometer fraudes informáticos, comercializar equipos especializados en capturar, interceptar información.*

Este artículo es compatible con el Art 6º de la Convención de Budapest, sin embargo hay una interpretación muy amplia, un vacío de este articulo por cuanto se extiende a toda gama de delitos previstos en la presente ley y que podría generar problemas en la interpretación judicial, debido a la extensión de ilícitos como : *interferencia telefónica, pornografía infantil, etc.*

[68] Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 9 de enero 2018].

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."

Se regulan las agravantes de los delitos previstos en la presente ley, y en base a esta norma el juez puede aumentar la pena hasta en un tercio por encima del máximo legal fijado; vgr: participación de integrantes de la organización criminal en la comisión de delitos informáticos, el acceso ilícito a la cuenta de correo electrónico a cambio de un pago*(los hackers de un centro comercial).*

Art. 12º.- "*Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos* "[69]

Este artículo incorporado por el Art. 3º de la Ley Nº 30171 "Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos", exime de responsabilidad penal a toda persona que realiza alguna de las conductas reguladas en los artículos 2º, 3º, 4º y 10º de la presente Ley. Esta cláusula de exención de responsabilidad se fundamenta en la

[69] Artículo 12º.- **EXENCIÓN DE RESPONSABILIDAD PENAL,** incorporado por el Art. 3º de la Ley N30171 "*Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos*", publicado el 10 de marzo del2014.

conducta legal – autorizada por la autoridad correspondiente- para realizar pruebas u otro procedimiento con el objetivo de proteger los sistemas y datos informáticos. Esta norma es compatible con el artículo 6°, inc. 2 del Convenio de Budapest.

2.3. Definiciones conceptuales.

- **Datos informáticos:** Toda representación de hechos, información o concepto expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

- **Deliberada:**Que es voluntario e intencionado fueron víctimas de un atropello de liberado, no se tratóde un accidente.

- **Ilegal:** Se conoce como ilegal a todo acto o circunstancia que no es permitido por la ley. El término ilegal se refiere a una circunstancia o hecho que colida o que se encuentra fuera del marco legal vigente o de la ley, es decir, no respeta lo que está establecido, y por el contrario, la violenta pudiendo acarrear una sanción o alguna pena por la realización de dicha actividad o hecho.

- **Ilícita:** Del latín illicĭtus, un ilícito es aquello que no está permitido legal o moralmente. Se trata, por lo tanto, de un delito (un quebrantamiento de la ley) o de una falta ética. Por ejemplo: “Hemos apresado a un hombre que acababa de cometer un ilícito en el centro comercial”, “El sospechoso tiene antecedentes por distintos ilícitos, desde robos hasta asesinatos”, “Es ilícito pensar que, con unos pocos gestos felices, subsanará años de injusticias”.

- **Indebida:**Que no se puede hacer por ser injusto o injustificado hacía un uso inde bido de supoder.

- **Sistema informático:** Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, será el tratamiento automatizado de datos en ejecución de un programa.

- **Tecnología de la información:** La frase tecnología de la información es proveniente del inglés "Information technology", y se hace conocido a través del administrador de computadoras Jim Domsic en el año de 1985, con la finalidad de darle un término más actualizado al procesamiento de datos. La tecnología de la información es un término que comprende todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones. Los avances tecnológicos como el Internet, las comunicaciones móviles, los satélites, etc. Han hecho significativos cambios en el sistema económico y social, influyendo en las relaciones sociales (conceptodefinicion.de, s.f.).

- **Tecnología de la comunicación:** la idea de tecnología se asocia a los conocimientos, las técnicas y los dispositivos que posibilitan la aplicación del saber científico. Comunicación, por su parte, se vincula a la transmisión de información entre un emisor y un receptor que comparten un mismo código.

CAPITULO III

RESULTADOS DE LA INVESTIGACIÓN

3.1. Trabajo de Campo

El trabajo empírico consistió en la aplicación de la técnica de la encuesta con su instrumento el cuestionario de encuesta para el estudio y análisis de las INCONSISTENCIAS Y AMBIGUEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY N°30096 Y SU MODIFICATORIA LEY N° 30171.

Los sujetos de la muestra estuvieron constituidos por los abogados, jueces y fiscales de la Provincia de Barranca del Distrito Judicial / Fiscal Huaura, a quienes se les suministro el cuestionario de encuesta, la cual fue hecha de forma anónima y tuvo por finalidad conocer la opinión sobre el tema motivo de investigación.

Tabla N° 1

¿Considera usted que la ley de delitos informáticos presenta una seria de inconsistencias normativas?	Frecuencia	Porcentaje
SI	25	83.3%
NO	5	16.7%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

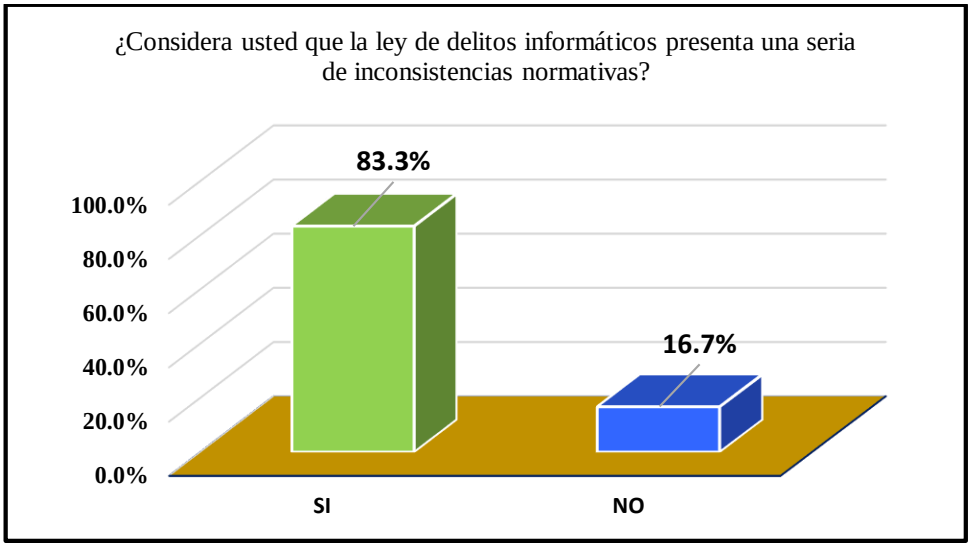

Figura 1

Fuente: Elaboración propia del autor.

De la figura 1, que representa a la siguiente pregunta ¿Considera usted que la ley de delitos informáticos presenta una seria de inconsistencias normativas?. Indicaron: un 83.3 % que SI, Considera usted que la ley de delitos informáticos presenta una seria de inconsistencias normativas y un 16.7 % señalaron que NO.

Tabla N° 2

¿Usted considera que Ley N° 30171 que modifica a la ley de delitos informáticos ha solucionado las inconsistencias normativas de la Ley N° 30096?	Frecuencia	Porcentaje
SI	18	60.0%
NO	12	40.0%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

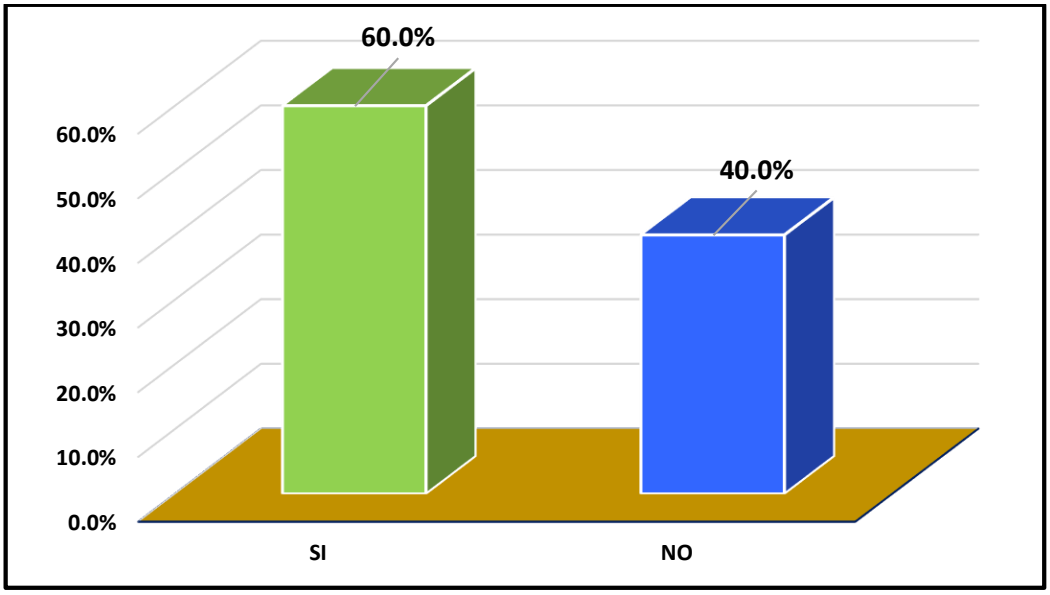

Figura 2

Fuente: Elaboración propia del autor.

De la figura 2, que representa a la siguiente pregunta ¿Usted considera que Ley N° 30171 que modifica a la ley de delitos informáticos ha solucionado las inconsistencias normativas de la Ley N° 30096?. Indicaron: un 60.0 % que SI, considera que Ley N° 30171 que modifica a la ley de delitos informáticos ha solucionado las inconsistencias normativas de la Ley N° 30096 y un 40.0% señalaron que NO.

Tabla N° 3

¿Cree usted que la falta de especialistas en materia de delitos informáticos es un problema para los legisladores pues no tienen un asesoramiento adecuado?	Frecuencia	Porcentaje
SI	16	53.3%
NO	14	46.7%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

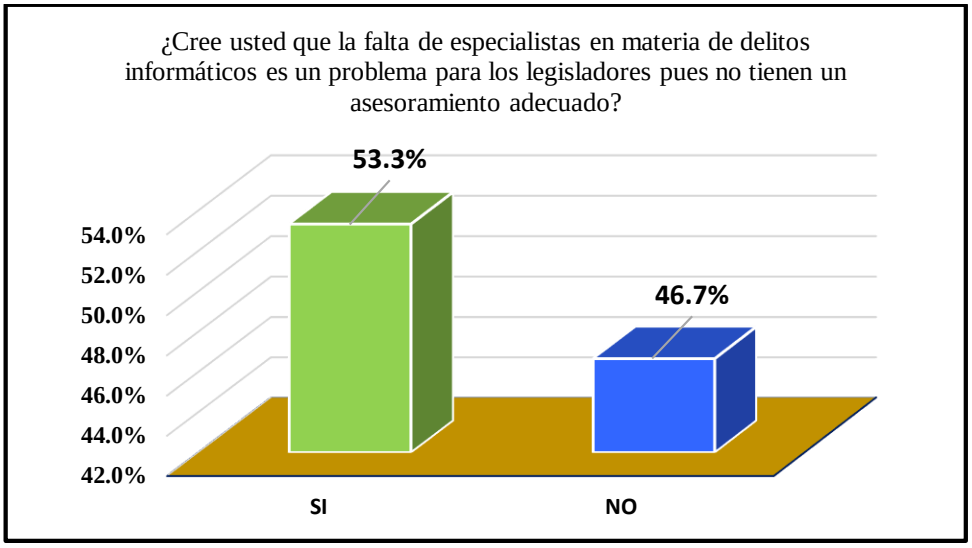

Figura 3
Fuente: Elaboración propia del autor.

De la figura 3, que representa a la siguiente pregunta ¿Cree usted que la falta de especialistas en materia de delitos informáticos es un problema para los legisladores pues no tienen un asesoramiento adecuado?. Indicaron: un 53.3% que SI, considera que la falta de especialistas en materia de delitos informáticos es un problema para los legisladores pues no tienen un asesoramiento adecuado y un 46.7 % señalaron que NO.

Tabla N° 4

¿Cree usted que los delitos informáticos necesitan regulación clara y precisa por parte del legislador?	Frecuencia	Porcentaje
SI	17	56.7%
NO	13	43.3%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

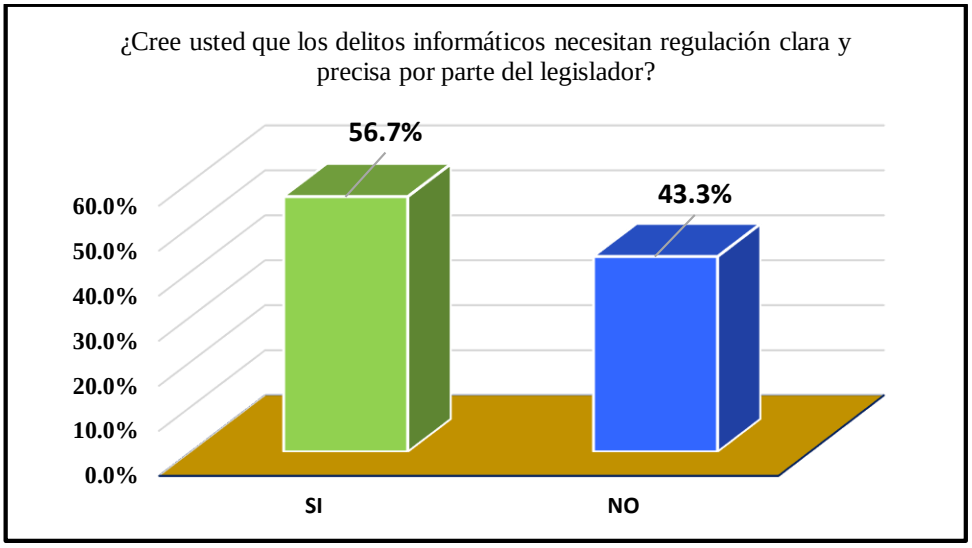

Figura 4
Fuente: Elaboración propia del autor.

De la figura 4, que representa a la siguiente pregunta ¿Cree usted que los delitos informáticos necesitan regulación clara y precisa por parte del legislador?. Indicaron: un 56.7 % que SI, considera que los delitos informáticos necesitan regulación clara y precisa por parte del legislador y un 43.3 % señalaron que NO.

Tabla N° 5

¿Considera que la inconsistencia normativa es un factor que afecta el principio de legalidad y principio determinación de la ley penal?	Frecuencia	Porcentaje
SI	14	46.7%
NO	16	53.3%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

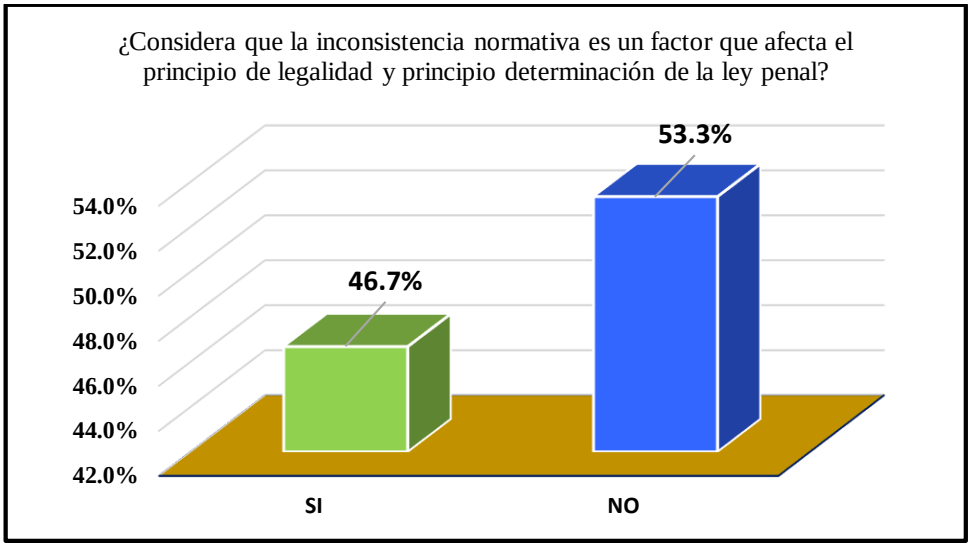

Figura 5
Fuente: Elaboración propia del autor.

De la figura 5, que representa a la siguiente pregunta ¿Considera que la inconsistencia normativa es un factor que afecta el principio de legalidad y principio determinación de la ley penal? Indicaron: un 46.7 % que SI, considera que la inconsistencia normativa es un factor que afecta el principio de legalidad y principio determinación de la ley penal y un 53.3 % señalaron que NO.

Tabla N° 6

¿Cree usted que la inconsistencia normativa en los delitos informáticos afecta el sistema jurídico?	Frecuencia	Porcentaje
SI	12	40.0%
NO	18	60.0%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

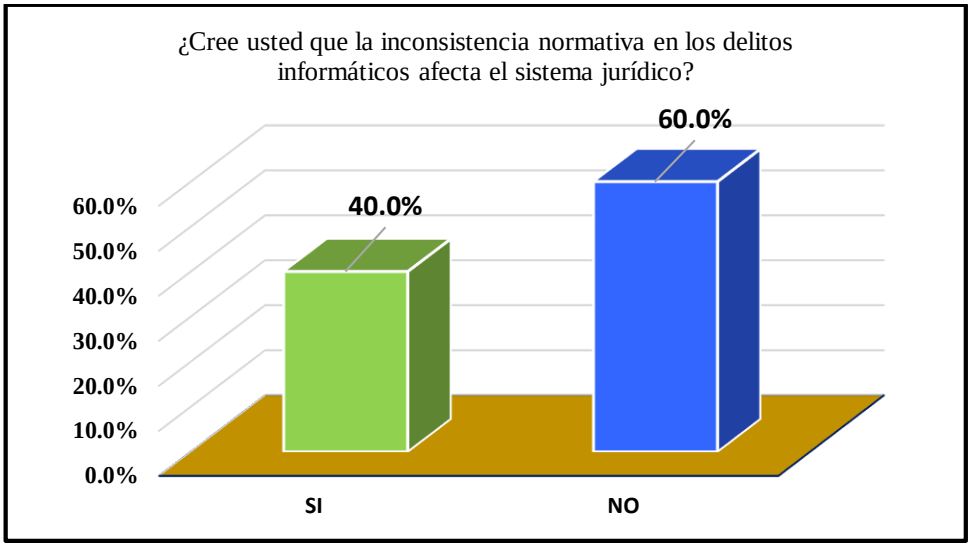

Figura 6
Fuente: Elaboración propia del autor.

De la figura 6, que representa a la siguiente pregunta ¿Cree usted que la inconsistencia normativa en los delitos informáticos afecta el sistema jurídico?. Indicaron: un 40.0 % que SI Considera que la inconsistencia normativa en los delitos informáticos afecta el sistema jurídico y un 60.0 % señalaron que NO.

Tabla N° 7

¿Cree usted que la ley N° 30096 y su modificatoria Ley N° 30171 presenta ambigüedades?	Frecuencia	Porcentaje
SI	20	66.7%
NO	10	33.3%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

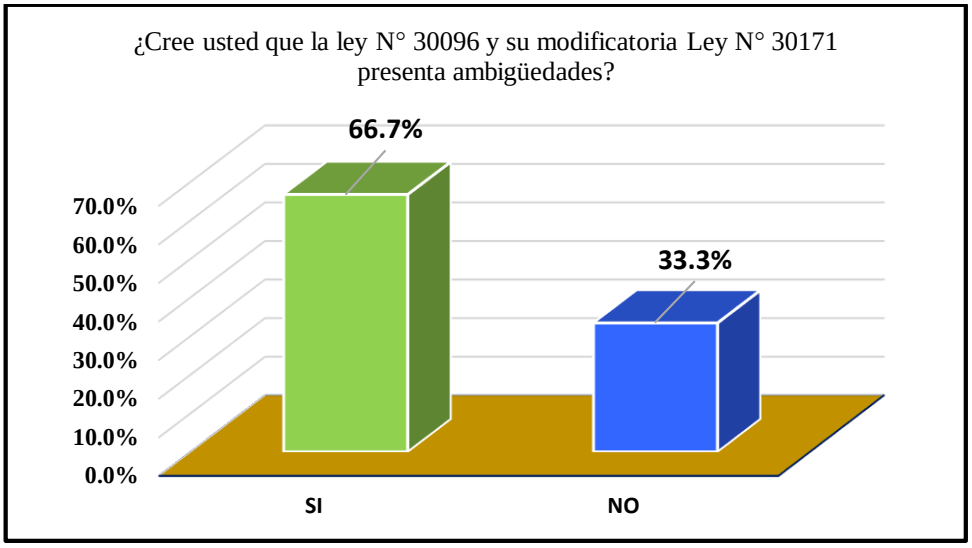

Figura 7
Fuente: Elaboración propia del autor.

De la figura 1, que representa a la siguiente pregunta ¿Cree usted que la ley N° 30096 y su modificatoria Ley N° 30171 presenta ambigüedades?. Indicaron: un 66.7 % que SI, considera que la ley N° 30096 y su modificatoria Ley N° 30171 presenta ambigüedades y un 33.3 % señalaron que NO.

Tabla N° 8

¿Considera usted que el legislador no ha hecho un estudio adecuado en la emisión de los tipos penales informáticos prescritos en la Ley N° 30096 y su modificatoria Ley N° 30171?	Frecuencia	Porcentaje
SI	13	43.3%
NO	17	56.7%
TOTAL	30	100.0%

Para efectos de mejor apreciación y comparación se presenta la siguiente figura:

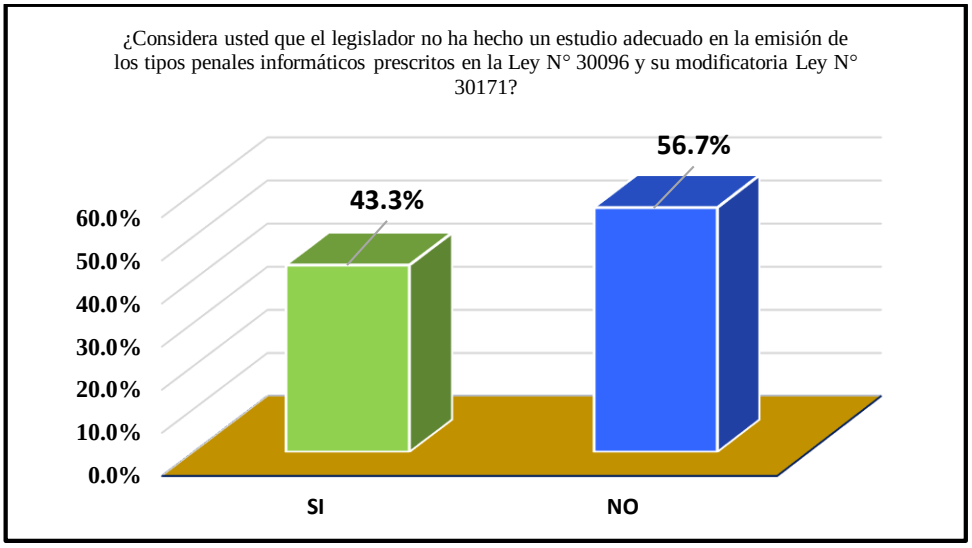

Figura 8
Fuente: Elaboración propia del autor.

De la figura 8, que representa a la siguiente pregunta ¿Considera usted que el legislador no ha hecho un estudio adecuado en la emisión de los tipos penales informáticos prescritos en la Ley N° 30096 y su modificatoria Ley N° 30171. Indicaron: un 43.3 % que SI, considera que el legislador no ha hecho un estudio adecuado en la emisión de los tipos penales informáticos prescritos en la Ley N° 30096 y su modificatoria Ley N° 30171 y un 56.7 % señalaron que NO.

3.2. Resultado normativo.

3.2.1. Derecho interno.

1. **Ley N° 27309 Ley que incorpora los delitos informáticos al código penal.**

   Durante el segundo lustro de los años 90´s, nuestro Código Penal Peruano no tenía artículos relacionados con los Delitos Informáticos específicamente. Es así que recién en el año 2000 (17 de julio) mediante la ley Nº 27309 se incorpora al título V un nuevo capítulo, el X-DELITOS INFORMÁTICOS en el Libro Segundo del Código Penal; cuyos artículos relacionados a delitos informáticos eran: los artículos Nº 207-A, 207-B y 207-C.

El artículo Nº 207-A está tipificado el Hacking o Intrusismo y/o Espionaje Informático; el artículo Nº 207-B tipificado el Sabotaje o Daño y el artículo Nº 207-C la Modalidad Agravada-Agravantes, siendo su contenido de tipificación lo siguiente:

Artículo 207º-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de 52 a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207º-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207º-C.- En los casos de los Artículos 207º-A y 207º-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

Después de 12 años, en mayo del 2012, se presenta una propuesta de Ley para modificar el artículo 207-C del Código Penal incorporando el delito de robo de identidad virtual, e incorporar un nuevo artículo el 207-D relacionado al delito informático agravado. Gracias a esta iniciativa de proponer una nueva Ley pero limitada a actualizar y adicionar un nuevo artículo, ingresa a un debate de tener en sí una Ley que este de acorde de contemplar penalidades de los nuevos delitos informáticos que se presenta en el Perú y el mundo.

2. **Ley Nº30096, Ley de delitos informáticos.**

   En los últimos tiempos, producto del desarrollo de las tecnologías informáticas se ha ido desarrollando una nueva forma de criminalidad denominada delitos informativos.

   En relación a esta nueva forma delictiva, en el Perú se ha emitido una Ley penal especial cuya finalidad es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, así como los secreto de comunicaciones, y los demás bienes jurídicos que resulte afectado con esta modalidad delictiva como son el patrimonio, la fe pública y la libertad sexual. La Ley N° 30096 "Ley de delitos informativos" fue promulgada el 21 y publicado el 22 de octubre del 2013 en el diario oficial "El Peruano". Luego fue parcialmente modificada por la Ley N° 30171 "Ley que modifica la Ley 30096, Ley de delitos informativos", promulgada el 9 y publicada el 10 de marzo del 2014.

3. **Ley 30171, Ley que modifica la Ley 30096, Ley de delitos informáticos.**

   La ley modificatoria 30171 de la Ley de Delitos Informáticos Nª 30096 ha realizado una serie de modificaciones con la finalidad de precisar los tipos penales, los cuales no se encontraban muy claros o eran muy amplios.

Asimismo, con la inclusión de la frase “deliberada e ilegítimamente” se hace mayor énfasis de que se trata de delitos dolosos tal como establece la parte general del Código Penal.

Además, se han precisado normas sobre coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros órganos especializados, tales como al centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-Cert), y la Oficina Nacional de gobierno Electrónico e Informática (ONGEI), los cuales no se encontraban nombrados en la antigua regulación.

Por otra parte, lo nuevo que ha traído esta regulación se establece en el caso de exención de responsabilidad penal para el hacking ético, cuya actividad se encuentra libre de persecución penal, por ser una práctica necesaria en el ámbito de las empresas que requieren resguardar sus datos informáticos.

A grandes rasgos podemos mencionar que esta nueva normativa ha intentado establecer un orden entre todas las modalidades típicas, modificando, derogando o incorporando los artículos que contenía la Ley Nº 30096, tanto en la misma norma como en el Código Penal; además, se ha intentado no dejar un espacio mínimo de impunidad en relación a las proposiciones a niños y adolescentes con fines sexuales.

3.2.2.1. Legislación en otros países

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

A. Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- ✓ Espionaje de datos (202 a)
- ✓ Estafa informática (263 a)
- ✓ Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- ✓ Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- ✓ Sabotaje informático (303 b. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- ✓ Utilización abusiva de cheques o tarjetas de crédito (266b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

B. Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987. Esta ley contempla los siguientes delitos:

- ✓ Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- ✓ Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

C. Francia.

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- ✓ Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- ✓ Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- ✓ Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

- ✓ Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- ✓ Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

D. Estados Unidos.

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Toya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

E. Holanda

El 1 de marzo de 1993 entró en vigor la Ley de los Delitos Informáticos, en la cual se penaliza el hancking, el preancking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

F. Reino Unido de la Gran Bretaña e Irlanda del Norte

Debido al caso de hancking en 1991, comenzó a regir la Computer Misuse Act, Ley de los abusos informáticos. Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Pena además la modificación de datos sin autorización donde se incluyen los virus.

3.2.3. Derecho comparado.

A. Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Esta ley reforma el Código Penal (art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202a).
- Estafa informática (263a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271,273).

- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Paises Escandinavos y en Austria.

B. España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999. La cual reemplaza una veintena de leyes anteriores de la misma Índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking. La introducción de virus, etc.: aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

C. Inglaterra.

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas.

El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

D. Chile.

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. SÍ esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hackíng. definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

3.3. Resultados jurisprudenciales

3.3.1. Tribunal constitucional

Por ser la ley de delitos informáticos de muy reciente regulación, esto es recién el año 2012 ha sido incorporado al código penal por la ley 27309 y recién en el año 2013 y 2014 se regula mediante una Ley especial. Es por ello que aún no se encuentra pronunciamiento del Tribunal Constitucional al respecto.

3.3.2. Poder judicial.

Por ser la ley de delitos informáticos de muy reciente regulación, esto es recién el año 2012 ha sido incorporado al código penal por la ley 27309 y recién en el año 2013 y 2014 se regula mediante una Ley especial. Es por ello que aún no se encuentra pronunciamiento del Poder Judicial al respecto.

3.4. Casos emblemáticos.

Caso1: Zinn, Herbert, Shadowhack..

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenía 16 y 17 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen[70].

Caso 2: Murphy Ian, Captain Zap.

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum. En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap," mostró la necesidad de hacer más clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenía acceso a órdenes de mercancías, archivos y documentos del gobierno. (..) el violar

[70]Quijada Tacuri, Victor Hugo. *Delitos informáticos en Perú* en: http://www.monografias.com/trabajos65/delitos-informaticos-peru/delitos-informaticos-peru3.shtml#xcasos.

accesos nos resultaba muy divertido". La Banda de hackers fue finalmente puesta a disposición de la ley". Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 ½ años de prueba.

Caso 3: Morris Robert.

En noviembre de 1988, Morris lanzo un programa "gusano" diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchisimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dolares. Se creo el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad[71].

[71] Quijada Tacuri, Victor Hugo. *Delitos informáticos en Perú* en: http://www.monografias.com/trabajos65/delitos-informaticos-peru/delitos-informaticos-peru3.shtml#xcasos.

CAPITULO IV

DISCUSIÓN Y VALIDACIÓN DE HIPÓTESIS.

4.1. Discusión doctrinaria

4.1.1. Posturas o argumentos a favor.

Si bien el Código Penal peruano (CP) fue promulgado el 03 de abril de 1991, este cuerpo normativo ya avizoraba la importancia de sancionar los delitos cometidos a través de medios electrónicos por lo que tipificó el delito de hurto telemático. Así, el artículo 186 CP, castigaba el hurto agravado con pena privativa de libertad no menor de 3 ni mayor de 6 años y con 180 a 365 días-multa, cuando el autor "usa[ba] sistemas de transferencia electrónica de fondos, de la telemática en general, o viola[ba] el empleo de claves secretas." Poco 6 tiempo después, mediante la Ley No. 26319 del 27 de mayo de 1994, la sanción fue incrementada a pena privativa de libertad no menor de 4 ni mayor de 8 años, manteniéndose sin modificación sustancial alguna hasta que fue derogada mediante la Ley 30096 del 22 de octubre de 2013. Sin embargo, pronto el legislador cayó en cuenta de que este tipo penal sólo castigaba un escaso número de conductas delictivas y dejaba impunes muchos ilícitos en los que se empleaban mecanismos informáticos.

En menos de una década, el problema del empleo indebido de las Nuevas Tecnologías ocasionó que el Congreso decidiera sancionar a quienes las empleaban con fines ilícitos. La primera respuesta de nuestro Legislador fue la tipificación de los Delitos Informáticos. Posteriormente, al no ser suficiente, se crearon nuevos delitos o se agravaron los ya existentes con la finalidad de perseguir a aquellos delincuentes que

empleaban este tipo de tecnologías como un medio para la perpetración de otros (turismo sexual, pornografía infantil, fraude electrónico, apología al terrorismo, etcétera)[72].

4.1.2. Posturas o argumentos en contra.

La ley 30096 y su modificatoria Ley N 30171, presenta más argumentos en contra que a favor, el especialista en Delitos Informáticos Erick Iriarte fue uno de los críticos más duros respecto a la regulación de los Delitos Informáticos "*se deben dar tres grandes pasos para consolidar la legislación Nacional contra el ciberdelito: 1. Adherirse al Convenio contra la Cibercriminalidad de Budapest (Hungría), suscrito en el 2001 por varios países; 2. Implementar los Equipos Preparados para Emergencias Informáticas (CERT, en ingles); y 3. Desarollar leyes destinadas a aplicar herramientas de informática forence".*

4.1.3. Posición o argumentos personales.

Pese a las posiciones y discusiones tomadas por diferentes autores ya sea en contra o a favor de la ley 30096 y modificatoria la ley 30171. Pensamos que los delitos electrónicos al ser el delito informático de reciente regulación aún hay vacíos en las cuales trabajar, somos uno de los países que más tempranamente adoptaron una regulación en tema de delitos informáticos (delitos que afectan al bien jurídico información) con la incorporación de los artículos 207A, 207B y 207C, de Nuestro Código Penal, enfocados en el intrusismo informático y en el cracking. Luego desarrollamos una legislación para fortalecer el combate contra la pornografía infantil, les dimos potestades a los fiscales para poder intervenir en comunicaciones (incluyendo comunicaciones digitales) pero no les dimos para temas de delitos por medio de TICs, y se han planteado diversos proyectos para adecuar los tipos penales existentes, pero no se han completado.

Es pues necesario adherirnos a un instrumento internacional, como el Convenio de Cybercrimen (Convenio de Budapest), que nos permita insertarnos en los esfuerzos

[72] PUELLES Ricardo Elías. Luces y sombras en la lucha contra la delincuencia informática en el Perú. P. 4. Lima. 2014.

internacionales y no quedar como una isla no regulada, esto a la vez nos serviría para implementar nuestra normativa en cuanto a Delitos Informáticos, y por supuesto contar con una cooperación internacional. El Convenio aparte de haber sido firmado por los países europeos, USA, Japón, Australia, Nueva Zelandia entre otros, presenta de la región Latinoamericana a Argentina, Chile, Costa Rica, Republica Dominicana y México que han firmado o ya están en proceso de ratificación del acuerdo. Mientras que otros países ya se encuentran en proceso de firmar el acuerdo. Este Convenio da instrumentos para la adecuación normativa, para la cooperación internacional y abre las puertas para el desarrollo de normativa sobre informática forense, necesaria para darle instrumento a la Policía y la Fiscalía para la persecución del delito.

Siendo de relevancia para el desarrollo de la Sociedad de la Información y con ello crear un marco normativo favorable al desarrollo de la industria TIC pero sobre todo para el desarrollo social, es necesaria el uso de Instrumentos Internacionales para poder seguir sus lineamientos en la lucha contra los Delitos Informáticos. Por todo lo antes expresado la Ley de Delitos Informáticos 30090 y su modificatoria Ley N° 30171 no puede continuar como se encuentra, debe volver a replantearse una propuesta dentro de un marco de respeto irrestricto a las libertades y derechos constitucionalmente protegidos, y en dicho marco plantear una legislación en materia de delitos informáticos.

4.2. Discusión normativa

4.2.1. Análisis o discusión de la normatividad interna.

La constante evolución tecnológica en las últimas décadas ha traído consigo las nuevas tecnologías de la información y de la comunicación que han producido un cambio necesario en las sociedades pasadas dando lugar a esta nueva sociedad digital, donde el hombre busca el desarrollo de su conocimiento y un mayor acceso a la información, lo que lleva a modificar y a producir cambios en el pensamiento humano.

Toda esta integración de la tecnología con la vida cotidiana se desarrolla de la mano con la aparición de un nuevo entorno digital, un medio en el que cada persona recibe, transmite y obtiene permanentemente información, dicho medio son las redes sociales en las que el espacio físico y el tiempo han sido modificados por redes de comunicación cibernética que permiten procesar información y transmitirla en tiempo real desde cualquier lugar del planeta generando grandes recursos de información en forma de imágenes, textos, gráficos y sonidos.

Todo esto tiene consecuencias en múltiples ámbitos puesto que estas redes se han convertido en un espacio social, una alternativa al mundo real donde se desarrollan actividades comerciales, formativas, de ocio, y también ilícitas.

La incorporación de los llamados delitos informáticos, en La legislación penal peruana, forma parte de las más recientes innovaciones al código penal de 1991. Las reformas, en materia penal, han sido de lo más variada (delitos contra la libertad sexual, contra el patrimonio, derechos de autor, terrorismo, etc.), lo que constituye una gran renovación a la materia penalista., pues las modificaciones empleadas, desde aquel entonces, han variado los lineamientos observados en el llamado "CODIGO DE BRAMONT ARIAS", de ahí que estos delitos se llaman los contra reformadores.

Es mediante la ley Nº27309, publicada el lunes 17 de julio de 2000, que se incorpora al título V los siguientes nuevos artículos: 207-A, 207-B, 207-C, lo que surge evidentemente como un intento de poner al día los nuevos avances tecnológicos, hechos que guardan concordancia con las normas relacionadas con la informática.

La incorporación del delito informático como antecedente más cercano en el Perú es el proyecto de ley Nº 5071/99, presentado por el congresista Jorge Muñiz, y proponía introducir en Delitos contra el patrimonio similares líneas con las ya anotadas en nuestro

código actualmente, sin embargo, ante observaciones derivadas del ejecutivo, se hicieron algunas variaciones que se plasman actualmente en el texto en los art. 208 A, B, C.

4.2.2. Análisis o discusión de la normatividad internacional.

Los Delitos Informáticos. es nuestro tema de análisis y uno de los aspectos doctrinales que avalan el sistema de protección mundial a esta nueva figura jurídica en la comunidad mundial de naciones, que ha insertado los principios de las Naciones Unidas en su política de protección y utilización a las nuevas tecnologías y servicios informáticos. El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Bajo esta perspectiva, los organismos internacionales que integran el engranaje de la comunidad mundial realizan mancomunados esfuerzos en aras de viabilizar proyectos que, en coordinación con la voluntad de los Estados nacionales, pueden materializarse.

4.2.3. Análisis o discusión del Derecho Comparado

A lo largo de la historia el ser humano ha necesitado transmitir y tratar la información de forma continua. Aún están en el recuerdo las señales de humo y los destellos con espejos y, más recientemente, los mensajes transmitidos a través de cables utilizando el código Morse o la propia voz por medio del teléfono.

La humanidad no ha cesado en la creación de métodos para procesar información. Con ese fin nació la informática como ciencia encargada del estudio y desarrollo de estas máquinas y métodos y con la idea de ayudar en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

Luego nació internet, como tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas en el mundo. Delincuentes diversos encontraron el modo de contaminarlo y, lo que es peor, hacerlo impunemente. La contaminación es de la más variada, entre los últimos ataques que pueden ser calificados como los más graves es el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, el terrorismo internacional y el narcotráfico.

Políticos de algunos países han pedido que se reglamente el uso de la red de modo que quienes prestan el servicio de internet registren a los clientes, cuándo y dónde llaman y para qué, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red protestaran enérgicamente.

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado posibilidades para el uso indebido de computadoras, lo que ha propiciado, a su vez, la necesidad de regulación por parte del Derecho. El espectacular desarrollo de la tecnología informática ha abierto las puertas a posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores por el lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información son algunos de los principales retos que cercan al mundo contemporáneo[73].

[73] Ramírez Bejerano, Egil Emilio - Aguilera Rodríguez, Ana rosa. *Los delitos informáticos. Tratamiento internacional.* 2015 En: http://www.la-razon.com/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional-gaceta_0_2216178537.html

4.3 VALIDACIÓN DE HIPÓTESIS

Pese a que se insistió en que se desarrolle un amplio debate sobre el tema y que especialistas en tecnologías de la información y comunicación participen en su modificación, el presidente Ollanta Humala promulgó la Ley de Delitos Informáticos [74]. Uno de los motivos por el cual vemos reflejados las falencias en esta cuestionada Ley de Delitos Informáticos. Encontramos artículos puntuales dentro de la Ley de Delitos Informáticos N° 30096 y su modificatoria Ley N° 30171 en los cuales presentan imprecisiones, que dificultan e imposibilitan su eficaz cumplimiento, y serán descritas de la siguiente manera:

- **Borrar archivos de otra persona.**

  Artículo 3. Atentado contra la integridad de datos informáticos

  El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

  Asimismo, la legislación castiga con hasta seis años de prisión a aquel que "introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos " de otra persona sin su consentimiento o permiso.

"No es lo mismo borrar un simple documento que acceder a la información de la defensa nacional, allí es cuando el juez tendrá que ver qué pena se pone. Con el Código Penal, ya se castiga esta acción. Lo dice Budapest y lo tienen varios países", refirió José Luis Medina del Ministerio de Justicia.

[74] La república. *Ley de Delitos Informáticos: estos son sus riesgos y peligros*. 2013 en: http://larepublica.pe/politica/746614-ley-de-delitos-informaticos-estos-son-sus-riesgos-y-peligros

Sin embargo, el especialista Erick Iriarte advirtió que se han cambiado términos del Convenio de Budapest, tratado internacional sobre cybercrimen al cual el Perú no ha logrado adherirse, y no existe un glosario para entender a qué se refiere la ley con tecnologías de la información o comunicación, porque hasta "para algunos, en TIC, se incluye el teléfono, el telégrafo o los dos".

Un ejemplo es el Cracker, que se da cuando una persona se introduce en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. A diferencia del Hacker, es aquella persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear su propio software para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso de apoya en un código ético.

•Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

Artículo 5. *El que, a través de las tecnologías de la información o de la comunicación, 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 artículo 36 del Código Penal.

En esta figura penal el legislador adelanta las barreras de punibilidad al sancionar el solo hecho de contactar con el menor de edad, sin importar si logra su objetivo el cual es obtener material pornográfico o llegar a tener actividad sexual, sin embargo este articulo tiene muchas falencias que podría violar el principio de legalidad, al no tener una redacción clara, y a consecuencia de este error se podría sancionar a personas que solo contactan con un menor de edad sin tener la finalidad de obtener material pornográfico y otro similar porque el término contactar no está delimitado, por consiguiente se estaría sancionando el solo hecho de establecer un "contacto" o comunicación con un menor de edad.

- **Utilización de una base de datos**.

  Artículo 6. Tráfico ilegal de datos: *El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.*

En este artículo de la ley, se condena con hasta cinco años de prisión a la persona que crea, ingresa, o utiliza indebidamente una base de datos. Sin embargo, el texto es ambiguo y hasta una simple lista de contactos puede verse involucrada.

Medina comentó que esta parte ya se encuentra en el Código Penal y lo único que se ha hecho es agruparla en este dictamen. Sin embargo, reconoció las inconsistencias.

"La redacción no es muy feliz, pudo ser mejor, yo la hubiera corregido, pero bueno, así fue, así lo plantearon en el Congreso", manifestó.

Artículo 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 resulta algún perjuicio material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años." De la misma manera, dentro de las Disposiciones Comunes (Capitulo VII) de la referida Ley, se reconoce el siguiente delito:*

Este tipo penal sanciona el hecho se suplantar (ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba), la identidad de una persona natural o jurídica causando algún perjuicio. La suplantación de identidad se puede calificar como un delito de resultado porque no basta con realizar la conducta típica de "suplantar" la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta que consiste en causar un perjuicio, caso contrario quedaría en tentativa. Ejemplos: crear perfiles falsos en las redes sociales (correo electrónico, Facebook, twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros. Citamos un caso: una abogada había sido suplantada en el Facebook y correo electrónico, por la pareja de su amiga, fingiendo ser lesbiana, para captar personas y ganarse la confianza a través del falso perfil y poder obtener materiales (fotos intimas) que luego eran utilizados para extorsionar a sus víctimas que ingenuamente creyeron estar en contacto con la persona suplantada, este acto trajo perjuicios económico, laboral, familiar, psicológico a la suplantada".

El artículo plantea que una suplantación sin perjuicio no configura delito. El mismo hecho de una suplantación ya configura un perjuicio y el tema de la protección de la identidad

ya se tiene en el espacio del derecho civil: "Artículo 28.- Nadie puede usar nombre que no le corresponde. El que es perjudicado por la usurpación de su nombre tiene acción para hacerla cesar y obtener la indemnización que corresponda." Sin embargo en la vía penal no había un artículo de suplantación de identidad, sea por medios digitales o por medios no digitales, siendo así nuevamente la oportunidad de regular una conducta al solo colocarle un tema tecnológico quita una oportunidad de adecuación normativa del código penal. Este artículo además no configura un delito informático sino un delito por medio informático, dado que el bien jurídico información no sería el vulnerado, sino la identidad personal.

Discriminación en internet.

Por otro lado, la discriminación de por sí es un delito establecido en el Código Penal, sin embargo, este legislación plantea añadir a la ley la modalidad a través de las tecnologías de la información o de la comunicación, llegando a castigar hasta con cuatro años de prisión, misma pena que la violencia por discriminación.

Nos encontramos otra vez frente a una regulación con medios Informáticos, resaltamos esto ya que éstos son solo instrumentos que facilitan el delito pero no determinan la comisión de las mismas, teniendo otra vez un exceso de regulación cuando esta conducta ya está regulada en nuestro Código Penal.

CONCLUSIONES.

1. Se evidencia, luego del análisis crítico de la ley de Delitos Informáticos Ley N° 3096 y su modificatoria Ley N° 30171, evidentes artículos que presentan imprecisiones en su redacción los cuales originan confusión tanto en los operadores de justicia como en los justiciables, ocasionando muchas veces que estos graves delitos no se denuncien o en su defecto que, posterior a ser denunciado, no se pueda hallar a los verdaderos culpables.

2. La superposición de tipos penales a los cuales se hace referencia en la presente tesis, solo demuestra que los legisladores están siguiendo una línea errada al pretender legislar los medios por los cuales se consuma un delito y no regular las CONDUCTAS. Cayendo equivocadamente en pretender regular conductas que ya están propiamente tipificadas en nuestro Código Penal.

3. Adherirnos al Convenio de Budapest que es el primer tratado en la lucha contra el cibercrimen serían un avance importantísimo que marcaría un antes y después en nuestra Legislación en temas de Delitos Informáticos. Hace falta que la intención de pertenecer a este Tratado se materialice y cambiemos nuestro normativa para poder proteger a los usuarios y poder navegar en la cuarta dimensión como es el Internet, con la seguridad de que no seamos victimas de delincuentes informáticos.

4. Las redes sociales propician el cambio de estructuras sociales dando paso al desarrollo humano, integral y comunitario, generando espacio de encuentro y reunión que sirve para compartir experiencias, para intercambiar información, para plantear problemas y generar sus respectivos proyectos de solución propagando información masivamente en instantes.

5. En el Perú no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa.

6. El derecho penal, siempre entendido como ultima ratio, resulta ser un arma fundamental en la lucha contra la delincuencia informática, no obstante, creer que constituye el único medio de control social capaz de solucionar el problema es en verdad iluso, de allí que el legislador deba orientar sus líneas político criminales a la luz del modelo de Estado Social y democrática de derecho que nos ilumina, sin creer que la sobre penalización y la sobre criminalización sean la solución a todos los problemas de criminalidad que existen en el Perú, la razón debe primar sobre la fuerza y la coerción, esos deben ser los pilares de cualquier reforma en materia penal.

7. Que debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

RECOMENDACIONES.

1. La recomendación básica en la cual se centró esta tesis es la INMEDIATA modificación los artículos observados en la Ley de Delitos Informáticos N° 30096 y su modificatoria Ley N° 30171, hace falta un debate a conciencia sobre los Delitos Informáticos para poder luego regularla.
2. Evitar que el poder Legislativo recaiga en las ambigüedades, imprecisiones, al redactar una norma, no confundamos Delitos Informáticos, en el cual el bien jurídico protegido es la Información tratada por medios Informáticos, con Delitos usando como medio la Tecnología.
3. En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general. Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, el presente proyecto ha sido dirigido a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países.

REFERENCIAS BIBLIOGRÁFICAS.

Fuentes bibliográficas

AZAOLA CALDERON, Luis; "Delitos informáticos y Derecho penal", UBIJUS, México 2010, pág. 70.BRAMONT - ARIAS, Luís. Delitos Informáticos. *Revista Peruana de Derecho de la Empresa, Derecho informático.2000.*

BRAMONT- ARIAS, Luis A.; "Delitos informáticos", en Revista Peruana de Derecho de la Empresa, DERECHO INFORMATICO Y TELEINFORMATICA JURIDICA, Nº 51, ASESORANDINA. Lima.2000.

CAMACHO LOSA, L; "El delito informático" GRAFICAS CONDOR, Madrid 1987, pág. 83- 84.

DE ALFONSO LASO, D; "El hackerin blanco. Una conducta ¿punible o impune?", en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial, Madrid, 2001, pág.110- 111.

ESTRADA GARAVILLA Miguel. Delitos informáticos. S/f.

GRAUW- HILL Interamericana Editores S.A. de C.V. 2003, P. 270

GUERRA VALDIVIA, Alicia Rubí. *Delitos Informáticos-Caso de estudio. Tesis.* Mexico.2011.

GONZÁLES HURTADO, Jorge Alexandre. *DELITOS INFORMÁTICOS: Daños informáticos del artículo 264 del código penal y propuesta de reforma. Tesis.* Madrid.2013.

GONZALES DE CHAVES CALAMITA, María E. El Llamado: Delitos informáticos. *Anales de la Facultad de Derecho de la Universidad de la Laguna, Nº 21. España*, PP.44-45.2004.

GUTIERRES FRANCES, M; “Fraude informático y estafa”/ RUIZ VADILLO, E; “tratamiento a la delincuencia informática”, en AZAOLA CALDERON, Luis; “Delitos informáticos y Derecho penal”, óp., cit., pág. 29.

HERNÁNDEZ, FERNÁNDEZ, & BAPTISTA. *Metodología de Investigación.* México: Mc

HIDALGO ÁVILA, Cesar Raúl. *Delincuentes Modernos en la Ciudad de la Oroya: En Delitos Informáticos. Tesis.* Oroya - Peru.2011

Convenio sobre la ciberdelincuencia – Budapest, 23.XI.2001: Cap. II, sección 1º, titulo 1º, Art. 4º.Ataques a la integridad de los datos.

LANDA ARROYO. César y Ana VELAZCO LOZADA Constitución política del Perú 1993 Lima Pontificia Universidad Católica del Perú. 1994 p.31-32

Ley Nº 30096, Ley de Delitos Informáticos; fue derogado por la UNICA DISPOSICION COMPLEMENTARIA DEROGATORIA de la Ley Nº 30171 “Ley que modifica la Ley Nº 30096, Ley de Delitos Informáticos”

Ley 30171, Ley que modifica la Ley 30096, Ley de delitos informáticos publicado en el diario Oficial el Peruano el 10 de marzo de 2014.

Ley Nº 30096, Ley de delitos informáticos publicado el 22 de octubre de año 2013 en el diario oficial el peruano.

Ley Nº 30096, Ley de Delitos Informáticos. 22 de octubre de 2013.

Ley Nº 30171, *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. 10 de marzo de 2014.

Ley 27309. Ley que Incorpora los Delitos Informáticos al código penal. 17 de julio de 2000

MARCHENA GOMEZ, M; “El sabotaje informático: entre los delitos de daños y desordenes públicos”, en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid 2001, pág. 356.

MARAVÍ SUMAR. Milagros Las instituciones de la democracia directa en la Constitución de 1993. p.122 En La Constitución de 1993. Análisis y comenta nos Lima CAJ, 1994. 296p

MARCHENA GOMEZ, M; “El sabotaje informático: entre los delitos de daños y desordenes públicos”, en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid 2001, pág. 356.

MATA BARRANCO, Norberto J/ HERNÁNDEZ DÍAZ, Leyre; “El delito de daños informativos: una tipificación defectuosa”; **en**, Revista de Estudios Penales y Criminológicos, Vol. XXIX, España, 2009, pág. 311- 362.

MINISTERIO DE JUSTICIA Código Civil Edición Oficial 2a.ed Lima W G 1994 p 8

MORANT VIDAL, J; “protección penal de la intimidad frente a las nuevas tecnologías”, Ed. PRACTICA DE DERECHO, Valencia, 2002, pág. 44.

MORANT VIDAL, J; “Protección penal de la intimidad frente a las nuevas tecnologías”, Ed. RACTICA DE DERECHO, Valencia 2003, pág. 46- 47.

MORON LERMA, ESTHER; “Internet y Derecho Penal: hacking y otras conductas ilícitas en la red”, ED. ARANZADI, Navarra, 2002, 2° ed., pág. 51.

NORTHCOTE, C. (2013). Cometarios a la Ley de Delitos Informáticos. *Actualidad Empresarial,* 4(p. VIII-4).

ORTS BERENGUER, Enrique/ ROIG TORRES, Margarita; “Delitos informáticos y delitos comunes cometidos a través de la informática”, TIRANT LO BLANCH, Valencia 2001, pág. 129.

PUELLES Ricardo Elías. Luces y sombras en la lucha contra la delincuencia informática en el Perú. P. 4. Lima. 2014.

REYES SÁNCHEZ, Yuridia & FERNANDEZ ARAMBURO, Ever. *Proyecto de Investigación: Delitos Informáticos.* Durango.2009.

RUMICHE PAZO, José Alfonso. *Sombras de la Normatividad que regula el incremento de la ciberdelincuencia en Lima 2015. Tesis.* Huacho- Peru. 2015.

SÁNCHEZ CASTILLO, ZULAY NAYIV (2017). *Análisis de la Ley 1273 de 2009 y la evolución de la Ley con relación a los delitos Informáticos en Colombia. Tesis.* Chichinquirà. Colombia. 2017.

SIEBER, Ulrich: "Criminalidad informática: peligro y prevención", pág. 77, MIR PUIG, S; "Delincuencia informática".

VILLAVICENCIO Terreros, Felipe. *Revista IUS ET VERITAS, N° 49, Diciembre.*, P.289. 2014.

VILLAVICENCIO TERREROS, Felipe; "Derecho Penal- Parte General", 3° reimpresión de la 1° ed., GRIJLEY, Lima 2010 pág. 375

VIVES ANTÓN y GONZÁLES CUSSAC, "Comentarios al código Penal 1995", Ed. TIRONT BLANCH, Valencia 1996, pág. 1238.

Fuentes electrónicos

Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 9 de enero 2018].

Diccionario de la Real Academia Española http://www.rae.es/recursos/diccionarios/drae [visto el 9 de enero 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=inutilizar [visto el 9 de enero marzo 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=suprimir [visto el 09 de Enero 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 9 de Enero de 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=imposibilitar [visto el 9 de enero 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 9 de Enero de 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 9 de Enero de 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=entorpecer [visto el 9 de Enero de 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=imposibilitar [visto el 9 de enero 2018].

Diccionario de la Real Academia Española http://lema.rae.es/drae/?val=acceder [visto el 8 de enero 2018].

MANSON, Marcelo; "Legislación sobre delitos informáticos", **en** https://dl.dropbox.com/u//dl. legislacioncomparada.pdf. [visto el 27 de diciembre 2013].

Quijada Tacuri, Víctor Hugo. *Delitos informáticos en Perú* en: http://www.monografias.com/trabajos65/delitos-informaticos-peru/delitos-informaticos-peru3.shtml#xcasos.

La república. *Ley de Delitos Informáticos: estos son sus riesgos y peligros*. 2013 en: http://larepublica.pe/politica/746614-ley-de-delitos-informaticos-estos-son-sus-riesgos-y-peligros

Ramírez Bejerano, Egil Emilio - Aguilera Rodríguez, Ana rosa. *Los delitos informáticos. Tratamiento internacional.* 2015 En: http://www.la-razon.com/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional-gaceta_0_2216178537.html

ANEXO

Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENCIONES	INDICADORES	METODOS Y TECNICAS
Problema General ¿De qué manera se muestran las inconsistencias y ambigüedades en la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171?	**Objetivos General** Determinar de qué manera se muestran las inconsistencias y ambigüedades en la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171.	**Hipótesis General** Existe significativamente inconsistencias y ambigüedades en la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171.	***(VD)*** ***INCONSISTENCIAS Y AMBIGUEDADES***	**X.1.**Inconsistencia **X.2**.Ambigüedad	X.1.1. Falta de especialistas en la materia. X.1.2. Escasos antecedentes normativas X.1.3. Un tema nuevo X.2.1. Concepciones diferentes X.2.2. Libertada de interpretación normativa.	. **Técnicas :** **Para el acopio de Datos:** Encuesta Análisis Documental y Bibliográfica. **Instrumentos de recolección de datos:** Guía de observación. Fichaje. Guía de entrevista. Cuestionario de encuesta. Análisis de contenido y Fichas. **Para el Procesamiento de datos.** Argumentación Jurídica. **Plan de recolección de la información**: Técnica Documental **Para presentación de datos** gráficos y figuras estadísticas. **Para el informe final:** **Tipo de Investigación:** **Diseño de Investigación** No experimental
Problemas Específicos: 1. ¿Existe superposición de tipos penales por las inconsistencias y ambigüedades de la Ley de delitos	**Objetivos Específicos:** 1. Determinar de qué manera Existe una superposición de tipos penales por las inconsistencias y ambigüedades de la	1. Existe significativamente superposición de tipos penales por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley nº 30096 y su modificatoria Ley nº 30171.	***(VI)***	**Y.1.**Superposición de tipos penales entre la Ley 30096 y el código penal.	Y.1.1. Artículo 5 de la ley 30096 con art. 175, 176 y 176-A del C. penal. Y.1.2. Artículo 7 de la ley 30096 con art. 162 del C. penal Y.1.3. Artículo 8 de la ley 30096 con art. 196, 196-A y 197 del C. penal	

informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171? 2. ¿Existe exceso de regulación normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171?	Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171. 2. Determinar de qué forma Existe un exceso de regulación normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171?	2. Se determina significativamente el exceso de regulación Normativa por las inconsistencias y ambigüedades de la Ley de delitos informáticos Ley nº 30096 y su modificatoria Ley nº 30171?	***LEY DE DELITOS INFORMATICOS.***	**Y.2.**Excesos en la regulación de la Ley 30096 y su modificatoria la Ley 30171.	Y.1.4. Artículo 9 de la ley 30096 con art. 438 del C. penal. Y.3.1. Convenio de Budapest Y.3.2. Ley 27309. (17 de Julio de 2000). Ley que Incorpora los Delitos Informáticos al código penal. Y.3.3. Ley 30096 y su modificatoria la ley 30171	

Instrumento de recolección de datos

INCONSISTENCIAS Y AMBIGÜEDADES		
I. Inconsistencia (Marcar con una "X" en el recuadro apropiado)	**Calificación**	
	1	**2**
1. ¿Considera usted que la ley de delitos informáticos presenta una seria de inconsistencias normativas?		
2. ¿Usted considera que Ley N° 30171 que modifica a la ley de delitos informáticos ha solucionado las inconsistencias normativas de la Ley N° 30096?		
3. ¿Cree usted que la falta de especialistas en materia de delitos informáticos es un problema para los legisladores pues no tienen un asesoramiento adecuado?		
4. ¿Cree usted que los delitos informáticos necesitan regulación clara y precisa por parte del legislador?		
5. ¿Considera que la inconsistencia normativa es un factor que afecta el principio de legalidad y principio determinación de la ley penal?		
6. ¿Cree usted que la inconsistencia normativa en los delitos informáticos afecta el sistema jurídico?		
II. Ambigüedades (Marcar con una "X" en el recuadro apropiado)	**Calificación**	
	1	**2**
7. ¿Cree usted que la ley N° 30096 y su modificatoria Ley N° 30171 presenta ambigüedades?		
8. ¿Considera usted que el legislador no ha hecho un estudio adecuado en la emisión de los tipos penales informáticos prescritos en la Ley N° 30096 y su modificatoria Ley N° 30171?		

UNIVERSIDAD NACIONAL DE ANCASH

"SANTIAGO ANTUNEZ DE MAYOLO"

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS DE INVESTIGACIÓN PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO.

Estimados Abogados, Jueces y Fiscales, esperamos tu colaboración respondiendo con responsabilidad y honestidad, el presente cuestionario. Se agradece no dejar ninguna pregunta sin contestar.

Instrucciones: Lea cuidadosamente las preguntas y marque con una aspa**(x)** la escala que crea conveniente.

Escala valorativa.

1	**2**
SI	**NO**