FACULTAD DE DERECHO

ESCUELA ACADÉMICO PROFESIONAL DE DERECHO

TESIS

LA INSEGURIDAD AL UTILIZAR LOS SERVICIOS DE REDES SOCIALES Y LA PROBLEMÁTICA JUDICIAL PARA REGULAR LOS DELITOS INFORMÁTICOS EN EL PERÚ-2015

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

Autor:

Morales Delgado Deivid Yuly

Abg. Bernal Marchena Maryluisa Guadalupe

Asesor Metodológico

Mg. Chávez Reyes Mario Vicente

Asesor Temático

Pimentel, Abril del 2016

LA INSEGURIDAD AL UTILIZAR LOS SERVICIOS DE REDES SOCIALES Y LA PROBLEMÁTICA JUDICIAL PARA REGULAR LOS DELITOS INFORMÁTICOS EN EL PERÚ-2015

Aprobación de la Tesis

Bachiller Morales Delgado Deivid Yuly
Autor

Abg. Bernal Marchena Maryluisa Guadalupe
Asesor Metodológico

Mg. Chávez Reyes Mario Vicente
Asesor Temático

Mg. Cabrera Leonardini Daniel Guillermo
Presidente del Jurado

Mg. Uchofen Urbina Ángela Katherine
Secretario del Jurado

Mg. Chávez Reyes Mario Vicente
Vocal del Jurado

DEDICATORIA

A Dios

Por haberme permitido llegar hasta este punto, dado salud para lograr mis objetivos y por su infinita bondad y amor.

A mis Padres

Porque en todo momento me apoyaron, aconsejaron y porque son parte esencial de mi existencia, su constante motivación que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mi esposa Lucía.

Por su amor y que nunca puso en tela de juicio mi capacidad, soportar estos años de estudios, apoyarme y comprender los esfuerzos realizados para nuestro bienestar familiar y así obtener una carrera profesional.

A mis hijos Ariana y Fernando.

Porque a su corta edad comprenden que a veces tenemos que sacrificar un poco de nuestro tiempo para lograr nuestros objetivos y metas.

AGRADECIMIENTO

Agradecer a **Dios**, por darme la oportunidad de vivir, estar conmigo en cada paso que doy, por fortalecer mi corazón, iluminar mi mente y por haber puesto en mi camino a las personas idóneas que han sido mi soporte y compañía durante todo el periodo de estudio.

A la **Universidad Señor de Sipán**, a los docentes por sus enseñanzas y experiencias impartidas en todos estos años de estudios.

ÍNDICE **DEDICATORIA ..... i**

RESUMEN

La evolución de las tecnologías y la informática, plantea al legislador nuevos y complejos problemas, y es evidente la dificultad para encarar un adecuado enfoque y solución de todas las implicancias de este tema. Pues la información es uno de los activos más valiosos y por ello que se exige tener un control sobre la misma, pues resulta demasiado sencillos los métodos con los que se puede extraer información y cometer un delito al obtener, modificar o eliminar información sin previa autorización del propietario, así como irrumpir en la privacidad de las personas de manera física y virtual. En la investigación abordaremos la legislación peruana y un poco más a fondo las especificaciones que se deben contemplar respecto a determinados artículos de nuestro ordenamiento jurídico, pues la jurisprudencia debe ayudar a una mejor legislación en cuanto a vacíos legales y no es posible seguir 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 como es lograr una correcta relación entre los miembros de la sociedad.

Palabras Clave: Evolución de las tecnologías; ordenamiento jurídico; irrumpir en la privacidad.

ABSTRACT

The evolution of technology and computing stalls the new legislature and complex problems, and it is clear the difficulty in addressing an appropriate approach and solution of all the implications of this issue. For information, it is one of the most valuable assets and why it is required to have a control over it, because it is too easy methods with which you can extract information and commit a crime to obtain, modify or delete information without prior authorization owner and breaking into the privacy of individuals physically and virtually. In research board Peruvian law and a little further specifications should look for certain items of our legal system, the case law should help better legislation regarding legal loopholes and can no longer sticking to figures typical not solve a specific problem, because since its formation can be seen if these figures comply with the primary object of law as is to achieve a correct relationship between members of society.

Keywords: Evolution of technologies; legal system; break into privacy.

INTRODUCCIÓN

En todo el mundo y en especial en nuestro Perú, han surgido muchos problemas, que deben de afrontarse con la adecuada interpretación de la leyes, como es el caso de la delincuencia informática que hoy por hoy se practica como el pan de cada día y que producto de estos actos delictivo, se van perfeccionando las formas de operar, inclusive utilizando recursos de procedencia lícita que mediante su utilización las organizaciones se van lucrando hasta el punto de ampliar sus conocimientos en este campo tecnológico y en donde los sujetos activos son personas expertas en la materia y que se valen de todos los recursos existentes para operar.

En este aspecto, la delincuencia al utilizar estos medios informáticos, para alcanzar sus fines lucrativos de manera ilegal en nuestro Perú se ha constituido el denominado Delito Informático, este nuevo fenómeno se convertido en una preocupación más para los legisladores, porque son ellos los que tiene que establecer patrones de comportamiento dentro de nuestra sociedad .

Dentro de la presente investigación se estudiarán los delitos informáticos, analizando primero la historia de la informática sus inicios, evoluciones y diversos cambios a los cuales se ha visto afectado, el cual implica desde el surgimiento de las computadoras hasta la evolución más sofisticada de la

misma, pero también se detalla las diversas situaciones que enfrenta el legislador para su adecuada tipificación y aplicación, y que posiblemente estemos ante una regulación ya establecida pero no muy bien aplicada como lo es el derecho a la intimidad y su inseguridad para utilizar estos mismos medios informáticos que día a día evolucionan y se convierten en las herramientas delictivas más sofisticadas y más utilizadas por las organizaciones delictivas que existen en nuestro país.

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1. El Problema

En la actualidad la informática está implantada en casi todos los países, por no decirlo en todo el globo terráqueo, tanto en las administraciones públicas y privadas, en la misma investigación científica, en las industrias, en el estudio e incluso en el ocio, gracias a estos logros se ha sistematizado el trabajo manual y en ocasiones el uso de la informática es indispensable, pero ante este incuestionable y muy importante avance surgen algunas facetas negativas como los ya conocidos delitos informáticos o ciberdelitos.

Este espectacular mundo cibernético y los constantes avances en la tecnología de la información, han abierto innumerables puertas a nuevas técnicas delictivas que en años atrás eran impensables, las manipulaciones de los diversos ordenadores ahora con fines de lucro, la creación de nuevos programas destructores de bases de datos el ingreso clandestino y la utilización indebida de la información que afecta directamente la privacidad de las organizaciones y especialmente de las personas, que con su utilización indebida se pueden ocasionar graves daños, no solo materiales y económicos sino también daños morales. Pero no solo la cuantía de los perjuicios ocasionados usualmente por la delincuencia tradicional está en juego sino también elevadas posibilidades

que estos delitos queden impunes o no lleguen a descubrirse, pues como sabemos nos enfrentamos a delincuentes especialistas en ocasiones profesionales en la materia que son capaces de borrar toda huella de los actos cometidos.

Con la aparición de Internet y de los delitos informáticos, los criminólogos han comenzado a anunciar que la concepción del delito debe replantearse pues estos nuevos crímenes vienen siendo cometidos en determinados lugares virtuales logrando abrir nuevas líneas de estudio.

Mientras que el miedo al delito tradicional se asociaba a experiencias emocionales, el miedo al delito informático está vinculado a un componente cognitivo, ya que el usuario de Internet hace una valoración puramente racional del riesgo que corre con determinadas conductas en la red. Sin embargo, es poco probable que navegar por la red le genere la misma sensación que cuando pasa por una calle oscura, por un lugar inhóspito o poco controlable. El problema del uso indebido de las Nuevas Tecnologías ocasionó que el Congreso decidiera sancionar a quienes las empleaban con fines ilícitos, siendo las primeras respuestas de nuestro Legislador la tipificación de los Delitos Informáticos. Pero Posteriormente, al no ser suficiente, se crearon nuevos delitos o se agravaron los ya existentes con la finalidad de perseguir a aquellos delincuentes que

emplean este tipo de tecnologías como un medio para la perpetración de otros como lo es el turismo sexual, la pornografía infantil, fraude electrónico, apología al terrorismo, que si bien es cierto está tipificados, se considera que no están regulados en su totalidad, por ejemplo el Artículo 2º de la Ley de Delitos Informáticos; el Delito de Acceso Ilícito, se puede ver que se sanciona el intrusismo, pues sólo se requiere el acceso ilícito a través de la vulneración de las medidas de seguridad para su configuración así tenemos que si algún estudiante de Ingeniería de Sistemas e Informática requiere poner en práctica sus conocimientos para descubrir los puntos vulnerables de algún sistema de información y poder mejorar, estaría cometiendo un delito sin tener en cuenta que no se persigue una finalidad ilícita. De otro lado, el Artículo 3º de la LDI tipifica el Delito de atentado a la integridad de datos informáticos en las modalidades sugeridas en el Convenio de Budapest. Sin embargo, se aparta de este instrumento al incorporar los términos “introduce” y “hace inaccesible” a la redacción del tipo penal. Al sancionarse otro tipo de conductas como “daña”, “borra”, “deteriora”, “altera” o “suprime” las cuales sí fueron recomendadas por el Convenio, la incorporación de las dos modalidades antes mencionadas se convierten en inútiles, pues, ¿cuándo debería castigarse penalmente la “introducción” de datos informáticos? La respuesta está vinculada a una carencia de la norma: cuando se

produzcan daños graves. Nuestra norma actual no lo prevé por lo que no tiene sentido y, de hecho, atenta contra el principio de lesividad del Derecho Penal, pues dicha modalidad per se no ocasiona daño alguno. Asimismo, sostengo que el término “hace inaccesible” es inútil por cuanto es una consecuencia de la modalidad “daña”. (Ricardo. 2014, p 36).

1.1.1 Selección del Problema

El problema fue seleccionado teniendo en cuenta los siguientes criterios:

a) Se tiene acceso a los datos.

b) La solución contribuye a solucionar otros problemas.

c) Es un problema que tiene incidencia social.

d) El problema afecta en forma negativa a la comunidad jurídica.

e) En su solución están interesados varios sectores de la sociedad.

1.1.2 Antecedentes del Problema

A. ¿Desde cuándo se tiene referencias sobre este tipo de problemas?

Estados Unidos

Herbert Zinn; fue el primer sentenciado bajo el cargo de fraude computacional y abuso en 1986, a la edad de 16 años violó el acceso de

AT&T y los sistemas del departamento de defensa. Sentenciado a 9 meses de prisión y a una fianza de 10.000 dólares.

David Smith; programador acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo.

Wau Holland y Steffen Wenery; ingresaron al Sistema de las instalaciones VAX del cuartel general de la NASA.

Poulsen Kevin, Dark Dante, diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de "Dark Dante" en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.

Ian Murphy; ingreso a los sistemas de la casa blanca, el pentágono, Bellsouth Corp., sentenciado a dos años y medio.

Robert Morris; lanzó un gusano encargado de consumir los recursos de las computadoras, sentenciado bajo el cargo de fraude a tres años de prisión.

En el Perú

En el Perú el legislador del Código Penal de 1991, pretendió hacer frente al problema desde una visión patrimonialista, incorporando delitos que estén acordes con las nuevas formas de criminalidad informática

En efecto el legislador peruano considerando que con las acciones de los delincuentes informáticos se afectaba el bien jurídico patrimonio de la víctima, en el inciso 3 del artículo 186 del CP, reguló como agravante el uso de los conocimientos y máquinas de la informática.

Este dispositivo prevé que se configura el delito de hurto agravado cuando el agente actúa mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas.

Allí se regularon tres supuestos que en doctrina se conocen como delitos informáticos. Al respecto el escritor peruano Bramont Arias Torres, considera que con los delitos informáticos en realidad no se protege ningún bien jurídico, porque en realidad no hay, como tal un “delito” informático. Esta postura asumió el legislador y optó por introducir a los mal llamados delitos informáticos como modalidades de comisión de conductas delictivas ya tipificadas. Luego, el legislador peruano al percatarse que lo previsto en el inciso 3 del artículo 186 del Código Penal, sólo servía para sancionar a un reducido grupo de conductas

patrimoniales, dejando sin sanción punitiva gran número de conductas dañosas, es decir no servía para hacer frente a los típicos delitos informáticos que sin duda causan enorme perjuicio a los intereses patrimoniales de los propietarios de las máquinas u ordenadores y redes informáticas.

La posibilidad de que no llegue a descubrirse a los autores se torna elevada, debido a que los delincuentes informáticos son especialistas capaces de borrar toda huella de sus actos ilícitos.

Asimismo, se plantean los antecedentes relacionados cuando se presentó a la Comisión de Reforma de Códigos del Congreso de la República del Perú los proyectos N°s. 5071/99-CR y 5132/99-CR del Dr. Jorge Muñiz Ziches y la Sra. Ivonne Susana Díaz Díaz respectivamente, los cuales propusieron se incorporen los Delitos Informáticos al Código Penal, las mismas que se materializan gracias a las facilidades que proporciona la informática en General.

Posteriormente se analizan las características del Delincuente informático, el mismo que está en constante evolución y perfeccionamiento. Seguidamente se presenta aspectos vinculados al Delito Informático y su relación con las otras figuras delictivas tipificadas en el Código Penal Peruano.

B. Estudios Anteriores

En Colombia

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en

Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

En Venezuela

Recientemente se publicó la Ley sobre Delitos Informáticos ("la Ley"), cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías (Gaceta Oficial N° 37.313 del 30 de octubre de 2001). Se trata de una ley especial que descodifica el Código Penal y profundiza aún más la incoherencia y falta de sistematicidad de la legislación penal, con el consecuente deterioro de la seguridad jurídica.

La Ley define los términos tecnología de la información, sistema, data, documento, computadora, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos.

La ley presenta varias deficiencias y problemas, entre los que podemos mencionar los siguientes:

Utiliza términos en el idioma inglés, cuando la Constitución sólo autoriza el uso del castellano o lenguas indígenas en documentos oficiales; no tipifica delito alguno relativo a la seguridad e integridad de la firma electrónica y a su registro; la terminología utilizada es diferente a la de la Ley de Mensaje de Datos y Firmas Electrónicas, tal como se observa en la definición que hace del mensaje de datos con lo que se propicia un desorden conceptual de la legislación en materia electrónica; repite delitos ya existentes en el Código Penal y en otras leyes penales, a los cuales les agrega el medio empleado y la naturaleza intangible del bien afectado; tutela los sistemas de información sin referirse a su contenido ni sus aplicaciones; no tutela el uso indebido de Internet; y establece principios generales diferentes a los establecidos en el libro primero del Código Penal, con lo cual empeora la descodificación.

La Ley, que pretende ser un Código Penal en miniatura, pero carece de la sistematicidad y exhaustividad propias de tal instrumento, elabora cinco clases de delitos:

Contra los sistemas que utilizan tecnologías de información; contra la propiedad; contra la privacidad de las personas y de las comunicaciones; Contra niños y adolescentes y Contra el orden económico.

En Panamá

De acuerdo con estadísticas de la fiscalía en mención, hasta el 30 de abril pasado, en el país se habían tramitado 21 delitos informáticos. Sobresalen los casos que tienen que ver con el ingreso ilegal a redes y bases de datos. Pero desde que en 2007 el delito informático se incluyó en el Código Penal, en Panamá se han reportado 359 investigaciones relacionadas a este hecho, pero solo ha habido tres condenas.

Aunque el Código Penal incluye al delito informático, hay aspectos sobre el tema que no están contemplados. Por ejemplo, la usurpación de identidad en redes sociales como Facebook, Twitter o Instagram, no se abordan en el presente código a pesar de los delitos están tipificados bajo la Ley 14 de 2007, Título VIII denominada Delitos contra la Seguridad Jurídica de los Medios Electrónicos Capítulo 1 “Delitos contra la Seguridad Informática” que abarca desde el artículo 289 hasta el Artículo 292.

En Ecuador

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, publicada en el R.O. / Sup.557 del 17 de Abril

del 2002, tiene un avance muy importante en el sentido de incluir figuras penales que castiguen los ilícitos informáticos, con lo cual junto al Código Penal integran normas creadas para la Sociedad de la Información.

Dentro de estas normas promulgadas en la Ley 67 para posteriormente ser transcritas al Código Penal, constan los siguientes ilícitos informáticos:

Art.57 CEFEMD: Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Art.58 LC EFEMD, Conc. Art.202.1 CP: Contra la Información Protegida.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

En México

En México, la Cámara de Diputados aprobó modificaciones legales para identificar los tipos de delitos informáticos, con lo que se pretende condenar a aquellos que hagan mal uso de la tecnología.

Los posibles delitos que podrían entrar pronto en vigor, van desde el ciberbullying, hasta el hacking y cracking, ya que si un individuo acceda a un sistema ajeno, aunque no haga daños ni modificaciones, sino que sea una simple práctica educativa, será considerado como delito en la reforma al artículo 211 del código penal.

1.1.3 Formulación del Problema

1.1.3.1 Formulación Proposicional del Problema.

La primera parte de esta investigación, comprende la existencia de Discrepancias Teóricas; que lo identificamos en la existencia de diferentes planteamientos teóricos, principios, derechos y posiciones desarrollados por la doctrina y Normas nacional (LEY 30171 Ley de los Delitos Informáticos) e internacionales, relacionados con los diversos delitos informáticos.

1.1.3.2 Formulación Interrogativa del Problema.

La segunda parte del problema consiste en la existencia de Empirismos Normativos; que lo identificamos en el deber del Estado de cautelar los

derechos informáticos de los individuos públicos, al no regular de manera eficaz mediante la derogación de artículos en la promulgación de dos leyes en relación con los delitos informáticos.

1.1.4 Justificación de la Investigación

El presente trabajo se justifica en la inadecuada legislación peruana no solo basta contemplar reformas al código penal o adecuaciones en sus apartados sino también delimitar muy bien los bienes jurídicos que deben ser protegidos por los delitos informáticos.

Dar a conocer las diferentes áreas propensas a ser víctimas de estos ilícitos y los beneficiados con este proyecto serán estudiantes, empresarios y personas comunes que hacen uso de las nuevas tecnologías en su quehacer diario.

1.1.5 Limitaciones y Restricciones de la Investigación

Limitaciones:

a) De tiempo: la presente investigación sólo comprende 4 meses.

b) De alcance: La investigación se limita a la reglamentación actual.

c) El presupuesto: Se limita al alcance de la disposición económica del investigador.

Restricciones:

a) Dedicación: el investigador sólo pueden dedicar 3 horas diarias.

b) Horarios: el investigador por tener que cumplir horarios de trabajo, solo tiene acceso en horas de la noche y fines de semana.

1.2 Objetivos de la Investigación

1.2.1 Objetivo General

Explicar la razón de ser de los delitos informáticos, como ha ido evolucionando hasta nuestros días, dar un acercamiento sobre la realidad que acontece en nuestro medio sobre la problemática que afecta a nuestra sociedad y la relación con el uso de la informática computacional como medio o fin, para la comisión de delitos, así mismo otorgar los elementos de información necesarios, para lograr una percepción social conveniente a fin de poder desarrollar una política de seguridad informática en nuestro medio. Dar una propuesta real de acción para el Legislador, con el fin que sus recursos humanos y materiales se aboquen al estudio, análisis y evaluación de esta problemática delictual, desarrollando los cursos necesarios para no ser sorprendidos y sobrepasados por esta nueva realidad nacional e internacional.

1.2.2 Objetivos Específicos

1.- Proponer un proyecto con alternativas de solución para los vacíos legales.

2.- Analizar los diferentes tipos de delitos informáticos regulados en nuestra legislación.

3.- Explicar las muchas consecuencias que pueden ocasionar así como también daños económicos y emocionales que pueden causar.

1.3. Hipótesis

1.3.1. Hipótesis global

La falta de algún fundamento teórico y estudio más detallados de los elementos que integran un tipo penal concreto, regulados en la Ley 30096 Ley de los Delitos Informáticos, la cual ha conducido al fracasar en el intento por regular de manera eficaz los actos delictivos, para proteger a los sujetos pasivos de la comisión de estos delitos; y las modificatorias establecidas en la Ley Nº 30171 Ley que regula, modifica y deroga algunos de los artículos de la mencionada norma.

1.3.2. Sub- Hipótesis

1.- Existen Discrepancias teóricas al aplicar las regulaciones establecidas en los ordenamientos jurídicos actuales.

Fórmula: - X1; A1; -B1, B2

Arreglo: -X, -A; -B

2.- Comunidad Jurídica la falta regulación o mala regulación de las leyes para tipificar los delitos informáticos.

Fórmula: A2; -X1,--B1,- B2, B3

Arreglo: -X, -A; -B

3.- Responsabilidad del Congreso de la República, al aprobar el proyecto de Ley con vacíos legales.

Fórmula: -X2; A1,- B1, B2

Arreglo: -X, -A; -B

4.- Se aprecian empirismos normativos, al tipificar los determinados delitos.

Fórmula: -X2; A2,- B1, B3

Arreglo: -X, -A; -B

1.4 Variables

1.4.1 Identificación de las Variables

Dados los cruces que consideran las sub-hipótesis en la presente investigación, para poder contrastarlas; se requerirá obtener los datos de los siguientes valores:

A = Variables de la Realidad:

A1 = Operadores de Derecho

A2 = Comunidad Jurídica

- B = Variables del Marco Referencial:

- B1 = Planteamientos Teóricos

- B2 = Normas

- B3 = Legislación Comparada

- X = Variables del Problema:

- X1 = Discrepancias Teóricas.

- X2 = Empirismos Normativos.

1.2.4.2 Definición de las Variables

A = Variables de la Realidad

-A1 = Operadores de Derecho

Pertenecen al dominio de esta variable, todos los datos que en común tienen la propiedad de explicar lo referente a “Toda persona que labora en relación a la jurisprudencia nacional, Magistrados, Abogados, Docentes Universitarios manifestándose como operadores de Derecho a través de su rutina ”

-A2 = Comunidad Jurídica

Pertenecen al dominio de esta variable, todos los datos que en común tienen el atributo de explicar porque la colectividad está interesada en esta temática jurídica nacional.

-B1= Conceptos básicos

Pertenecen al dominio de esta variable, todos los datos que en común tienen el atributo de explicitar... “Una imagen mental de cualquier cosa que se forma mediante la generalización a partir de casos particulares como por ejemplo, una palabra o un término”…; referidos a lo básico, es decir...“perteneciente a la base o bases sobre la que se sustenta algo fundamental”.

-B2= Normas

Los datos que en común tienen el atributo de explicitar “la norma o regla jurídica como un esquema o programa de conducta que disciplina y

castiga los delitos informáticos conforme a Ley y como lo dispone el la (LEY 30171 Ley de los Delitos Informáticos)".

-B3= Legislación Comparada

Pertenece al dominio de esta variable, todos los datos que en común tienen el atributo de explicitar la "Ciencia cuyo objeto es el estudio de las semejanzas y diferencias entre los ordenamientos jurídicos de dos o más países"; referido a legislación "Se entiende por tal, según la definición de la Academia de la Lengua, "el conjunto o cuerpo de leyes por las cuales se gobierna un Estado o una entidad determinada, y también la ciencia de las leyes". Con un sentido amplio, debe entenderse por leyes, todas las normas rectoras del Estado y de las personas a quienes afectan; dictadas por la autoridad a quien esté atribuida esa facultad.

-X1= Discrepancias Teóricas

Los identificamos cuando algunos conocen y propugnan la aplicación de un planteamiento teórico, tal que (A), y otros hacen lo mismo pero con otro planteamiento teórico tal que (B).

-X2= Empirismos Normativos

Los identificamos cuando alguna norma interna que rige en esa realidad, entidad o empresa no ha incorporado en su enunciado, no está

actualizado o no considera un planteamiento teórico directamente relacionado.

1.4.2 Definición de las Variables

A = Variables de la Realidad

-A1 = Operadores de Derecho

Pertenecen al dominio de esta variable, todos los datos que en común tienen la propiedad de explicar lo referente a “Toda persona que labora en relación a la jurisprudencia nacional, Magistrados, Abogados, Docentes Universitarios manifestándose como operadores de Derecho a través de su rutina ”

-A2 = Comunidad Jurídica

Pertenecen al dominio de esta variable, todos los datos que en común tienen el atributo de explicar porque la colectividad está interesada en esta temática jurídica nacional.

-B1= Conceptos básicos

Pertenecen al dominio de esta variable, todos los datos que en común tienen el atributo de explicitar... “Una imagen mental de cualquier cosa que se forma mediante la generalización a partir de casos particulares como por ejemplo, una palabra o un término”…; referidos a lo básico, es

decir...“perteneciente a la base o bases sobre la que se sustenta algo fundamental”.

-B2= Normas

Los datos que en común tienen el atributo de explicitar “la norma o regla jurídica como un esquema o programa de conducta que disciplina y castiga los delitos informáticos conforme a Ley y como lo dispone el la (LEY 30171 Ley de los Delitos Informáticos)”.

-B3= Legislación Comparada

Pertenece al dominio de esta variable, todos los datos que en común tienen el atributo de explicitar la “Ciencia cuyo objeto es el estudio de las semejanzas y diferencias entre los ordenamientos jurídicos de dos o más países”; referido a legislación “Se entiende por tal, según la definición de la Academia de la Lengua, “el conjunto o cuerpo de leyes por las cuales se gobierna un Estado o una entidad determinada, y también la ciencia de las leyes”. Con un sentido amplio, debe entenderse por leyes, todas las normas rectoras del Estado y de las personas a quienes afectan; dictadas por la autoridad a quien esté atribuida esa facultad.

-X1= Discrepancias Teóricas

Los identificamos cuando algunos conocen y propugnan la aplicación de un planteamiento teórico, tal que (A), y otros hacen lo mismo pero con otro planteamiento teórico tal que (B).

-X2= Empirismos Normativos

Los identificamos cuando alguna norma interna que rige en esa realidad, entidad o empresa no ha incorporado en su enunciado, no está actualizado o no considera un planteamiento teórico directamente relacionado.

1.4.3 Clasificación de las Variables por la relación causal, cantidad o cualidad y jerarquía.

Clasificación de las variables

Variables	*Clasificaciones*						
	Por la relación causal	*Por la cantidad o cualidad*	*Por la jerarquía o escalas*				
			4	*3*	*2*	*1*	*0*
Del Marco Referencial							
Teóricas (Planteamientos Teóricos)							
-B1= Conceptos Básicos	Independiente	Cualitativa	*TA*	*MA*	*A*	*PA*	*NA*
Normativas							
-B2= Normas	Independiente	Cualitativa	--	--	--	--	--
-B3= Legislación Comparada	Independiente	Cualitativa	T AP	*M AP*	*AP*	*P AP*	*N AP*
Entorno – Ámbito							
-B4= Jurisprudencia	Independiente	Cualitativa	*TA*	*MA*	*A*	*PA*	*NA*
De la Realidad							
A1= Responsables	Interviniente	Cualitativa	--	--	--	--	--
A2= Comunidad Jurídica	Interviniente	Cualitativa	T E	*M*	*E*	*P E*	*N E*
Del Problema							
X1= Discrepancias Teóricas	Dependiente	*Cantidad Discreta*	--	--	--	--	--
-X2= Empirismos Normativos	Dependiente	*Cantidad Discreta*	--	--	--	--	--

Leyenda:

T= Totalmente P= Poco A= Aplicable AC= Actualizado

E= Eficiente M= Muy N= Nada C= Cumplible

Ad= Adecuado AP= Aprovechó

Figura 1: Clasificación de las Variables por la relación causal cantidad y jerarquía

1.5 Diseño de la Ejecución del Plan y desarrollo de la Investigación

1.5.1 Universo de la Investigación

El universo de la presente investigación comprende la sumatoria de todos los datos, de los dominios de todas las variables, que se cruzan en todas las sub-hipótesis en el anexo 04, que se han identificado como (Operadores de Derecho, Comunidad Jurídica, Conceptos Básicos, Normas, Legislación Comparada, Discrepancias Teóricas y Empirismos Normativos).

1.5.2 Selección de Técnicas, Instrumentos y Fuentes de Investigación de Datos

De acuerdo a las variables presentes en la investigación, y la forma en cómo se realizaron las cruces para la obtención de las sub hipótesis, se requerirá recurrir, a las siguientes técnicas de recolección:

a. La Técnica del Análisis Documental; utilizando como instrumentos de recolección de datos de las fuentes documentales, Fichas Textuales y de Resumen, recurriendo como fuentes a libros especializados, documentos oficiales e internet, que aplicaremos para obtener los datos de los dominios de las variables: Conceptos Básicos, Normas y Legislación Comparada.

b. La Técnica del cuestionario; utilizando como instrumento para la recopilación de datos de campo un rol de preguntas y recurriendo como informantes a los responsables para obtener los datos de los dominios de las variables: Operadores de Derecho, Comunidad Jurídica.

1.5.3 Población y Muestra de Informantes

La población y la muestra está integrada por las normas y documentos objeto de las mismas que son:

Constitución Política del Perú (artículos pertinentes).

Ley Nº 26301 Acción Constitucional de Habeas Data.

Ley Nº 30096, Ley de los Delitos Informáticos.

Ley Nº 30171, Ley que Modifica la Ley Nº 30096 Ley de los Delitos Informáticos.

Decreto Legislativo Nº 822 Ley de Derechos de Autor.

Resolución Ministerial Nº 622-96-MTC/ Secreto de las Telecomunicaciones y Protección de Datos.

Código Penal.

Ley Nº 27309, que incorpora los Delitos Informáticos al Código Penal Peruano

1.5.4 Forma de Tratamiento de Datos

Los datos obtenidos mediante la aplicación de las técnicas e instrumentos antes mencionados serán incorporados a programas computarizados, como los aplicativos de Ms Office y SPSS de ser el caso necesario, con precisiones porcentuales y prelaciones u ordenamientos de mayor a menor, los promedios o sumas serán presentados como informaciones en forma de figuras, gráficos, cuadros o resúmenes.

1.5.5 Forma de Análisis de las Informaciones

Con respecto a las informaciones presentadas como figuras, gráficos, cuadros o resúmenes, etc; se formularán apreciaciones objetivas. Las apreciaciones correspondientes a informaciones del dominio de variables que han sido cruzadas en una determinada Sub-Hipótesis, son premisas para contrastar esa Sub-Hipótesis.

En el capítulo 4: “Conclusiones”; las apreciaciones resultantes del análisis directamente relacionadas con una determinada sub hipótesis se usarán como premisas para contrastar esas sub hipótesis; se procederá igual con cada una de ellas. El resultado de la contratación de cada sub hipótesis dará la base para formular una conclusión parcial. En el Capítulo 5: “Recomendaciones”, cada conclusión dará base para formular una recomendación parcial. Los resultados de las contrataciones de las sub hipótesis, a su vez, se usarán como premisas para contrastar la hipótesis global. El resultado de la contratación de la hipótesis global nos dará la base para formular la Conclusión General.

Cada resultado de una contrastación, que puede ser:

a) Prueba total

b) Disprueba total

c) Prueba y disprueba parciales.

El que resulte, cualquiera de ellos, será considerado al formular las conclusiones parciales o la conclusión general.

Las conclusiones fundamentarán las recomendaciones de la investigación.

CAPÍTULO II

MARCO

REFERENCIAL

2.1. Planteamientos Teóricos

2.1.1 Conceptos Básicos

La realidad del mundo jurídico es fiel testigo de los cambios que se han generado en los aspectos económicos, administrativos, sociales, culturales y sobre todo tecnológicos lo cual ha llevado mejorar la calidad de vida de las personas pues facilitan las herramientas que se son necesarias para agilizar el trabajo diario tanto en casa, el trabajo así como en los estudios, porque en todos nuestros actos cotidianos se ha hecho indispensable el uso de INTERNET. Las redes sociales ya forman parte de nuestra vida no solo en nuestro país sino en el mundo y el cual desempeña un papel fundamental.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:

a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.

b. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.

c. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.

d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos. Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.

Es necesario mencionar que el hecho de criminalizar algunas conductas desplegadas en el mundo informático, no implica desconocer las ventajas y facilidades brindadas por estos sistemas. Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el uso de la tecnología informática y comunicación.

Como señala Camacho Losa, “En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de

venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia.” Entonces el autor se pregunta **¿y por qué la informática habría de ser diferente?**

2.1.2 Derecho Informático

Bajo la égide de Derecho Informático, se encuentra la relación conceptual existente entre la Ciencia Jurídica y la Informática. El 30 de abril de 1980, el Comité de los ministros de los Estados miembros del Consejo de Europa aprobó una recomendación sobre “la enseñanza, la investigación y la formación en materia de Informática y Derecho”, a través de la cual se dio a conocer la importancia y utilidad de fomentar en el ámbito universitario el estudio de los temas. (Davara, 1993, p. 30).

2.1.3 Concepto.

El derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre EL Derecho y la Informática. (Flores Salgado, 2014, p. 17).

Para Julio Téllez Valdés, el Derecho Informático es... “Una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática).

El Derecho Informático como rama del Derecho tiene una incipiente y corta evolución, la cual data a partir del año de 1949, en el que Norbert Wiener, con su obra, consagra al derecho y las comunicaciones, al expresar la influencia que ejerce la cibernética respecto de la ciencia jurídica, al afirmar... “Así los problemas de la ley deben considerarse como comunicativos y cibernéticos, es decir, son problemas de regulación ordenada y reproducible de ciertas situaciones críticas.” (Armando, 2008, p. 80).

Para nuestra investigación diremos que el Derecho informático, como rama de Derecho s una interdisciplina que se encarga de estudiar el uso y desarrollo de las tecnologías informáticas, encaminadas a la investigación científica de los problemas jurídicos y como un factor de estrategia para el desarrollo de la sociedad, con el fin de lograr su pleno aprovechamiento, y como instrumento de apoyo para elevar la productividad, competitividad, eficiencia, administración y procuración del derecho en los sectores público, social y privado para propiciar el bienestar común.

2.1.4 Los Delitos Informáticos en la Historia

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las

computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Los primeros casos fueron reportados en 1958. Para el profesor Manfred Mohrenschlager, este fenómeno ha obligado al surgimiento de medidas legislativo penales en los Estados Industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo informático.

En nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía su máximo nivel, esto por cuanto no se conoce en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta o tomada en cuenta a medias, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual. (Problema que no solo es en el área Penal sino en todo el ordenamiento jurídico nacional). A continuación se intentará dar una delimitación de este fenómeno de la criminalidad informática.

2.1.5 Naturaleza Jurídica del Delito Informático

1. Dentro del Derecho Positivo, necesariamente optamos por seguir la rama del Derecho Público.

2. Dentro del Derecho Público, ubicamos a los “delitos Informáticos” en la rama del Derecho Penal, dado que su función es la protección de un bien jurídicamente tutelado de importancia, tal que puede eventualmente coartar la libertad de aquel que pudiera atentar en su contra, previendo en distintos ordenamientos jurídicos. (Pérez Luño, 1996, p. 17).

2.1.6 Delimitación del Fenómeno Informático

El aspecto más importante de la informática radica en que la información se ha convertido en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después.

A decir de **Claudio Magliona y Macarena López**, una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales, es por eso que es menester desentrañar el intrincado debate doctrinario acerca del real contenido de lo que se ha dado en llamar los delitos informáticos. Desde esta perspectiva, debe reinar la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del estado.

2.1.7 Características

1. Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos pueden llegar a cometerlas.

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

3. Ofrecen facilidades de tiempo y espacio, puesto que en milésimas de segundos y sin necesidad de presencia física pueden llegar a cometerse.

4. Son muchos los casos y muy pocas denuncias, y todo ello debido a la misma falta de regulación jurídica a nivel nacional.

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

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

7. Provocan serias pérdidas económicas para los afectados, pero siempre producen beneficios de más de cinco cifras para quienes lo realizan.

8. Son muy sofisticados.

9. Ofrecen facilidades para su comisión los menores de edad.

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

En algunos casos siguen siendo ilícitos e impunes ante la Ley. (Rodríguez, 2033, p. 52).

2.1.8 Delincuencia Informática

La define **Gómez Perals** como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

La misma definición aporta **Correa** incidiendo en la Recomendación. Del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador.

2.1.9 Definición y Concepto de Delito Informático

Podemos indicar que los delitos informáticos son todas aquellas conductas ilícitas susceptibles de sanción por el derecho penal, por hacer uso indebido de cualquier medio informático. (García de la Cruz, 2009, p. 37).

De otro al profesor **TELLES VALDEZ**, nos ilustra con una definición de los delitos informáticos, señalando que son actitudes ilícitas en que se tiene a la computadora como instrumento o fin; y agrega, citando al italiano Carlos Sarzana que los delitos informáticos son cualquier comportamiento criminógeno en que la computadora está involucrada, como material, objeto o mero símbolo. De las definiciones dadas, se tiene que los delitos informáticos, son pues todas aquellas conductas ilícitas, que emplean para su comisión elementos o medios informáticos, y que dichos comportamientos se encuentran regulados de manera explícita en la norma penal.

El delito informático, en un inicio se encontraba tipificado en el Art. 186° inc. 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. En la actualidad, los delitos informáticos están previstos en el Capítulo X

13 del CP: los artículos 207°-A (interferencia, acceso o copia ilícita contenida en base de datos), 207°-B (alteración, daño o destrucción de base de datos), 207°-C (circunstancias calificantes agravantes), 207°-D (tráfico ilegal de datos), y en las leyes penales especiales.

2.1.10 Sujetos del Delito Informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo. (Pérez Luño, 1996, p. 18).

2.1.10.1 Sujeto Activo

De acuerdo al profesor chileno Mario Garrido Montt, se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal. 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. (Davara, 1993, p. 46).

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencian entre sí, es la naturaleza de los delitos cometidos. De esta forma, la persona que “entra” en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que “desvía fondos” de las cuentas de sus clientes.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nro. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (Insiders). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran

atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (Outsiders).

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 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”.

Respecto a esto el jurista mexicano Jorge Lara Rivera, en un artículo publicado en Internet nos dice que “Tradicionalmente se ha considerado que este tipo de delitos se encuadra dentro de los llamados “delitos de cuello blanco” debido a que se requiere que el sujeto activo tenga un conocimiento especializado en informática. Ahora bien, no podemos negar que la especialización informática facilita a los sujetos a incidir

criminalmente por medio de las computadoras. Sin embargo, el mundo de la computación se va convirtiendo paulatinamente en un área común y corriente, gracias a la facilidad con la que los modernos sistemas y programas pueden ser controlados.

Dentro de poco tiempo la operación de un sistema electrónico será tan fácil como manejar una televisión, por ejemplo. De esta manera, se puede ubicar como sujeto activo de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación. Por no hablar del problema que se plantea con los llamados “niños genio” que son capaces no sólo de dominar sistemas electrónicos básicos, sino que pueden incluso intervenir exitosamente en operaciones de alto grado de dificultad técnica, acarreando más problemas al tambaleante concepto de la impunidad para el caso de que algunos de estos menores logre cometer estragos importantes a través de los medios computacionales que maneje”.

2.1.10.2 Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

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, etcétera 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. (Armando, 2008, p. 29).

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 y la 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”.

2.1.2 Principios más Relevantes

2.1.2.1 Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir ya que constituye la razón de

ser del delito y no suele estar expresamente señalado en los tipos penales.

2.1.2.2 Bien Jurídico Protegido en los Delitos Informáticos

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda, da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente. (Jijena Leiva, 1993, p. 76).

Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales.

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

2.1.2.3 Tipos de Delitos Informáticos

2.1.2.3.1 Delitos Contra Datos y Sistemas Informáticos

Este apartado 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" 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 "vulnerar" se entiende como "transgredir, quebrantar, violar una ley o precepto" que se entiende al hecho de transgredir las barreras de protección diseñados por el sistema.

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"36 de la acción contenida en el texto del Convenio de Budapest guarda cierta identidad con el dolo (conocimiento y voluntad). (Ley Nº 30096, Ley de los Delitos Informáticos).

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".

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 (hacer cesar, hacer desaparecer) y hacer accesible 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 accesible 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 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".

Esta figura penal sanciona las conductas que están dirigidas a inutilizar (hacer inútil, vano o nulo algo) total o parcialmente un sistema informático, entorpecer (retrasar, dificultar) imposibilitar (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 sólo dará lugar a la tentativa. (Ley Nº 30096, Ley de los Delitos Informáticos, 2014)

Este artículo guarda cierta relación de compatibilidad con el Art. 5º del Convenio de Budapest 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 Daños; 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. El modus operandi se viene perfeccionando con el tiempo: virus, cáncer routine. Estos actos deben causar un perjuicio patrimonial.

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”. Marchena Gómez señala que el “sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños”. Morant Vidal señala que “el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas”.

Las técnicas que permiten cometer sabotaje informático son las siguientes:

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.

Gusanos; 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 con la finalidad de borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente; cambiar la clave secreta o eliminar la cuenta electrónica (correo, twitter, Facebook) para impedir al titular el acceso a su cuenta.

2.1.2.3.2 Delitos Contra la Identidad y Libertad Sexual

Que sanciona la propuesta sexual (solicitar u obtener material pornográfico, llevar a cabo actividades sexuales) a niños, niñas y adolescentes utilizando los medios tecnológicos.

2.1.2.3.3 Proposiciones a Niños, Niñas y Adolescentes con Fines Sexuales con 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 involucran el quebrantamiento de la indemnidad o libertad sexual del menor (violación sexual o actos contra el pudor). (Código Penal, 1991)

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 artículo 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.

2.1.2.3.4 Delitos Contra la Intimidad y el secreto de las Comunicaciones

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 transporte dichos datos informáticos, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.

La figura penal sanciona la conducta que deliberada e ilegítimamente intercepta (Interrumpe, obstruye una vía de comunicación) datos

informáticos y las emisiones electromagnéticas que transportan estos datos en las transmisiones privadas.

2.1.2.3.5 Delitos informáticos contra el Patrimonio

Que sanciona la acción de diseñar, introducir, alterar, borrar, suprimir y clonar datos informáticos en perjuicio de tercero.

2.1.2.3.6 Fraude Informático

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

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), 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) 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, 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. 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, porque ambos artículos sancionan el empleo indebido de datos informáticos, la manipulación del funcionamiento del sistema mismo.

2.1.2.3.7 Delitos informáticos contra la Fe Pública

Sanciona la suplantación de identidad de una persona natural o jurídica, siempre que de esto resulte algún perjuicio.

2.1.2.3.8 Suplantación de Identidad

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

Este tipo penal sanciona el hecho se suplantar (ocupar con malas artes el lugar de alguien, defraudando 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. Crear perfiles falsos en las redes sociales (correo electrónico, Facebook, twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros.

2.1.2.3.9 Abuso de Mecanismos y Dispositivos Informáticos

Está dirigido al que fabrique, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas,

dispositivos, contraseña, códigos de acceso o cualquier otro dato informático para la comisión de los delitos antes mencionados.

2.2 Normas

2.2.1 Constitución Política del Perú de 1993

La Constitución Política del Perú, regula el estado de derecho del país, es el más alto nivel en normas legales y de allí se desarrollan las demás leyes puede estar en contra de la constitución, pues se podría declarar inconstitucional.

Los temas legales con respecto a la informática son novedosos en el país, a pesar que en países más avanzados ya existen gran cantidad de normas.

En esta sección se analizarán los artículos insertados en la constitución que están relacionados a la informática y que nos pueden guiar para comprender el derecho informático en otros campos.

En la constitución vigente desde el año de 1993, encontramos los siguientes artículos:

TÍTULO I DE LA PERSONA Y LA SOCIEDAD

Artículo 2º.- Toda persona tiene derecho:

1. A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de derecho en todo cuanto le favorece.

2. A la igualdad ante la ley. Nadie debe ser discriminado por motivo de origen, raza, sexo, idioma, religión, opinión, condición económica o de cualquiera otra índole.

A la libertad de conciencia y de religión, en forma individual o asociada. No hay persecución por razón de ideas o creencias. No hay delito de opinión. El ejercicio público de todas las confesiones es libre, siempre que no ofenda la moral ni altere el orden público.

En el derecho informático, al igual que en las demás ramas del derecho, no se puede legislar contra la vida humana o el desarrollo físico y psicológico.

Todos son iguales, no va a interesar que tanta tecnología informática tenga en su poder, ni ningún otros rasgos que puedan diferenciarlo de otra persona.

Las personas, tendrán diferentes enfoques o ideas relacionadas con la informática (por ejemplo el software debe ser libre o no), pero no se les

puede perseguir, sino se está de acuerdo a esas ideas, hay libertad. La única restricción es que no contravenga la moral o el orden público.

3. A las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley.

Las personas tienen libertad para difundir información como opiniones, ideas, etc., por los diferentes medios de comunicación social, en este caso por Internet; esto se puede comprobar por la existencia de distintos sitios web donde se da opinión (foros), se consulta y absuelve preguntas (listas de interés), se conversa en línea (Chat), se da noticias sobre intereses particulares (blogs), o se comparten videos propios. Esto tiene que seguir no siendo restringido, teniendo en cuenta de respetar las demás leyes.

Los delitos cometidos por medio del libro, la prensa y demás medios de comunicación social se tipifican en el Código Penal y se juzgan en el fuero común.

Es delito toda acción que suspende o clausura algún órgano de expresión o le impide circular libremente. Los derechos de informar y opinar comprenden los de fundar medios de comunicación.

4. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

Con la ayuda de Internet, muchas instituciones públicas dan servicios en línea a sus usuarios, por lo cual los costos de acceso se están reduciendo y asimismo el tiempo. El usuario puede solicitar cualquier información pública, sin necesidad de expresar la causa. Hay algunas excepciones: como las que afecten la intimidad de las personas, las que estén prohibidas por ley o por razones de seguridad.

El derecho al acceso a la información pública es un derecho humano. Es decir que por nuestra simple condición de seres humanos, todos nosotros lo poseemos. Por ello, recibe especial protección por parte del Estado.

5. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Aquí, debe aclararse hasta qué punto la información personal se puede compartir o distribuir, no depende del tipo de institución, ya que es igual

para las públicas y privadas. La controversia es ¿Cuándo se puede decir que afectan la intimidad personal o familiar? El dar el nombre, la dirección, el correo electrónico, el centro de trabajo, etc. Para distintas personas afectará de diferente manera esta información.

6. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias.

Toda persona afectada por afirmaciones inexactas o agraviantes en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

Hay que tener presente, para el caso de los conocidos blogs, en los cuales con exceso se califica a personas o instituciones. Como se aprecia está prohibido y existen leyes penales que castigan estos abusos en los medios de comunicación como Internet.

7. A la libertad de creación intelectual, artística, técnica y científica, así como a la propiedad sobre dichas creaciones y a su producto. El Estado propicia el acceso a la cultura y fomenta su desarrollo y difusión.

Existe una protección a toda creación intelectual, artística, técnica y científica, y a disfrutar de su propiedad. En este caso, la creación de

software y su comercialización es libre, y ninguna otra persona puede hacer uso o compartirla sin el consentimiento del autor. Existen entidades como Indecopi, que defienden a los autores y sancionan a las personas o empresas que usan software no autorizado por las licencias respectivas.

8. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.

Los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial.

Con la tecnología actual, se va a hablar muy poco del domicilio físico, y más del domicilio virtual o web. Como el artículo es general, también se restringen los ingresos a estos sin el consentimiento del propietario.

En el caso de las correspondencias, se debe seguir manteniendo, como una forma de asegurar que los correos electrónicos o mensajes a través de la red, no sean interceptados y utilizados por personas ajenas. Sólo la autoridad competente puede revisar la correspondencia, pero respetando la intimidad de la persona.

TÍTULO V DE LAS GARANTÍAS CONSTITUCIONALES

Artículo 200º de las Garantías Constitucionales

3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2º, incisos 5) y 6) de la Constitución.

2.2.2 Código Penal

TÍTULO IV DELITOS CONTRA LA LIBERTAD

Artículo 154º, El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres años y de treinta a ciento

veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista. Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

Violación de la intimidad en el ejercicio del cargo

Artículo 155º Si el agente es funcionario o servidor público y, en ejercicio del cargo, comete el hecho previsto en el artículo 154º, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36º, incisos 1, 2 y 4.

Revelación de la intimidad

Artículo 156º; El que revela aspectos de la intimidad personal o familiar que conociera con motivo del trabajo que prestó al agraviado o a la persona a quien éste se lo confió, será reprimido con pena privativa de libertad no mayor de un año.

Organización entrega y uso indebido de archivo político o religioso.

Artículo 157º; El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas será

reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36º incisos 1, 2 y 4.

Acción privada

Artículo 158º Los delitos previstos en este apartado son perseguibles por acción privada

CAPÍTULO IV VIOLACIÓN DEL SECRETO DE LAS COMUNICACIONES

Artículo 161º Violación de correspondencia

El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa.

Interferencia telefónica

Artículo 162º El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de

libertad no menor de uno ni mayor de tres años. Si el agente es funcionario público, la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación conforme al artículo 36º incisos l, 2 y 4.

Frustración de correspondencia

Artículo 163º El que, indebidamente, suprime o extravía de su destino una correspondencia epistolar o telegráfica, aunque no la haya violado, será reprimido con prestación de servicio comunitario de veinte a cincuenta y dos jornadas.

Publicación indebida de correspondencia

Artículo 164º El que publica, indebidamente, una correspondencia epistolar o telegráfica, no destinada a la publicidad, aunque le haya sido dirigida, será reprimido, si el hecho causa algún perjuicio a otro, con limitación de días libres de veinte a cincuenta y dos jornadas.

CAPÍTULO V VIOLACIÓN DEL SECRETO PROFESIONAL

Violación del secreto profesional

Artículo 165º El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revela sin consentimiento del interesado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a ciento veinte días-multa

TÍTULO V DELITOS CONTRA EL PATRIMONIO

CAPÍTULO I

HURTO

Hurto Simple

Artículo 185º El que, para obtener provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayendo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equiparan a bien mueble la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético.

Hurto agravado

Artículo 186º El agente será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años si el hurto es cometido:

1. En casa habitada.

2. Durante la noche.

3. Mediante destreza, escalamiento, destrucción o rotura de obstáculos.

4. Con ocasión de incendio, inundación, naufragio, calamidad pública o desgracia particular del agraviado.

5. Sobre los bienes muebles que forman el equipaje de viajero.

6. Mediante el concurso de dos o más personas. La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

1. Por un agente que actúa en calidad de integrante de una organización destinada a perpetrar estos delitos.

2. Sobre bienes de valor científico o que integren el patrimonio cultural de la Nación.

3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.

4. Colocando a la víctima o a su familia en grave situación económica.

5. Con empleo de materiales o artefactos explosivos para la destrucción o rotura de obstáculos. La pena no será menor de ocho ni mayor de quince años cuando el agente actúa en calidad de jefe, cabecilla o dirigente de una organización destinada a perpetrar estos delitos.

2.2.3 Ley Nº 27309 que incorpora los Delitos Informáticos al Código Penal

CAPITULO X

Delitos Informáticos

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 cincuentidos 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 o 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.

2.2.4 Ley Nº 30096 Ley de los Delitos Informáticos

CAPÍTULO II

Delitos contra datos y Sistemas Informáticos

Artículo 2º. Acceso Ilícito

El que accede sin autorización 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.

Artículo 3º. 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.

Artículo 4º Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, Inutiliza, total o parcialmente, un sistema Informático, Impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus

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

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

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 su persona material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro no mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36º 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 36º del Código Penal.

Artículo 6º 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.

Artículo 7º Interceptación de datos informáticos

El que, a través de las tecnologías de la Información o de la comunicación, 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 transporte dichos datos informáticos, será reprimido con 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 las normas de la materia.

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.

2.2.5 Ley Nº 30171 Ley que Modifica la Ley Nº 30096 Ley de los Delitos Informáticos

Artículo 1º Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10

Artículo 2º Acceso Ilícito (….)

Artículo 3º Atentado a la Integridad de Datos Informáticos (….)

Artículo 4º Atentado a la Integridad de Sistemas Informáticos (….)

Artículo 5º Proposiciones a adolescentes, Niños y Niñas con fines Sexuales con fines a la Integridad de Datos Informáticos (….)

2.3 Contexto Internacional

2.3.1 Estados Unidos

El Acta Federal de Abuso Computacional de 1994, que modificó el Acta Fraude y Abuso Computacional de 1986, diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de estragos. El Acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan daño por la trasmisión de ese virus, el castigo de hasta 10 años en prisión más una multa y para aquellos que lo

trasmiten, solo de manera imprudencial la sanción consiste de entre una multa y un año en prisión.

Con la finalidad de eliminar los argumentos híper técnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en qué difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Los legisladores estadounidenses, la nueva Ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delito, la nueva Ley da lugar a que se contemple que se debe entender como acto delictivo.

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.

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

2.3.2 Colombia

Andrés Velásquez, presidente y fundador de la compañía de cibert seguridad Informática, explica que hay dos tipos de cibert delincuentes a distinguir: aquellos que saben cómo utilizar la tecnología para cometer un delito y quienes no son expertos, pero conocen las vulnerabilidades en las plataformas corporativas y las aprovechan para obtener un beneficio.

En el segundo grupo se encuentran los llamados "insiders", que generalmente son empleados que roban, borran o dañan información sensible de la empresa. Un ejemplo puede ser el ejecutivo que se va a trabajar a otra empresa y sustrae en una memoria USB bases datos de clientes o información confidencial de la organización para la cual trabajaba con el fin de utilizarla en su beneficio. Ahora bien, aunque los hackers tal como los muestran los medios de comunicación solo existan en Hollywood y la ciberguerra sea un tema restringido a las potencias

mundiales, en el país, los delitos informáticos son una realidad. Dentro de los que más aquejan a la población colombiana están: suplantación de identidad, difamación por Internet, fraude cibernético, denegación de servicio, fuga de información, phishing, divulgación indebida de contenido, pornografía infantil, uso de software espía, violación de derechos de autor, piratería en Internet, entre otros.

Ante este panorama, el Congreso de la República de Colombia sancionó la Ley 1273 del 5 de enero de 2009, "por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado De la Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

A partir de dicha normativa, la información se convirtió en un bien titulado y de esta manera se logró establecer un marco regulatorio para conductas delictivas relacionadas con la tecnología o que son perpetradas desde medios informáticos. Así, el país pasó a ser pionero a nivel mundial en materia de legislación de delitos informáticos.

"Algo que se hizo muy bien en Colombia al momento de legislar sobre esta materia es que no se utilizó tanto tecnicismo. Cosa que no sucedió en países como México cuando se tipificó el phishing. En ese país, tres

meses después de sancionada la norma esa conducta criminal pasó a llamarse 'Drive by Pharming', lo que hizo que las autoridades ya no pudieran castigarla con las normas existentes", señala, Andrés Velásquez, director y fundador de la compañía de cómputo forense mexicana Máttica.

"Hace unos años las personas no sabían que podían denunciar cuando les clonaban las tarjetas bancarias, les robaban dinero por Internet o cuando los calumniaban en redes sociales; hoy la gente está denunciando todo eso", comenta Germán Realpe, consultor en derecho informático y nuevas tecnologías.

Además este tipo de delitos actualmente son castigados severamente. En efecto, la Ley 1273 contempla penas de prisión que van de los 48 a los 120 meses y multas de hasta 1.000 salarios mínimos legales mensuales vigentes.

Sin embargo, los expertos en el tema coinciden en que la tecnología va mucho más rápido que aprovechan la legislación. En ese sentido, mientras se crean normas para atacar este tipo de delitos, surgen nuevas tecnologías para burlarlas y los criminales se de esta situación.

2.3.3 Venezuela

Todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho, y que hacen uso indebido de cualquier medio informático.

La Ley Especial Contra Delitos Informáticos forma parte de un conjunto de instrumentos jurídicos que vienen a establecer el marco de regulación del área tecnológica en Venezuela, aspecto en el cual (como ya se ha dicho en múltiples ocasiones) se avanza a pasos agigantados. Sin embargo, el dinamismo en materia tecnológica crea ciertos inconvenientes debido a que al no estar regulada jurídicamente ésta área, da cobijo a actividades que sin ser "ilícitas" representan una plaga para la sociedad. Como por ejemplo:

Acceso indebido.

Sabotaje o daño a sistemas.

Espionaje informático.

Falsificación de documentos.

Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.

Difusión o exhibición de material pornográfico.

Apropiación de propiedad intelectual, Etc.

Antes de la promulgación de ésta ley las actividades mencionadas anteriormente no estaban tipificadas como delitos**.**

2.3.4 Panamá

En países como España la creación de perfiles falsos en redes sociales como Twitter puede ser penalizada bajo el delito de usurpación de identidad o lesión de privacidad. Precisamente en Panamá la Policía Nacional se ha preocupado por reforzar este tema y ha ayudado a que las personas puedan denunciar el uso incorrecto de las redes sociales, específicamente Twitter y Facebook.

El abogado consultor, Jorge Torregrosa, indicó que en Panamá los delitos informáticos se encuentran tipificados en el Código Penal. “En este caso encontramos una legislación muy completa en el tema de la regulación de los delitos informáticos, imponiendo como sanción penas de prisión de uno a seis años, regula las conductas que van desde la manipulación, alteración, sustracción de la información, hasta sanciones para aquellas personas que enseñen a construir bombas o reclutar personal por medio de la internet para fines terroristas, norma que no vemos en ninguna otra legislación”, reveló.

Destacó que la legislación panameña en esta materia es novedosa por lo que los agentes de instrucción y demás investigadores deben ser altamente capacitados en este tipo de delitos, para que de esta manera se puedan perseguir y determinar la responsabilidad o no de los imputados,

así como también identificar aquellos usurpadores de identidad en cuentas falsas y acosadores cibernéticos que utilizan la internet para hacer daño a las personas.

Dichas normas están claramente establecidas y adoptadas por la Ley 14 de 2007, con las modificaciones y adiciones introducidas por la Ley 26 de 2008, la Ley 5 de 2009, la Ley 68 de 2009 y la Ley 14 de 2010 Título VIII Delitos contra la Seguridad Jurídica de los Medios Electrónicos Capítulo 1 Delitos contra la Seguridad Informática que va desde el Artículo 289 hasta el Artículo 291.

De acuerdo con una publicación del sitio Infobae, el 8.5% de las 271 millones de cuentas activas de Twitter son operadas en la red de forma automatizada, sin la intervención humana, en tiempos en que redes sociales, comunidades virtuales, y bases de datos, se han incorporado a la vida cotidiana. 42 de 100 personas en Panamá tienen hoy día acceso a internet en el país, según la Autoridad de Servicios Públicos de Panamá.

2.3.5 Ecuador

Como antecedente los primeros tipos penales informáticos que se incluyeron en la legislación ecuatoriana fueron en el año 2002 en el proyecto para la creación de la ley de comercio electrónico, firmas

electrónicas y mensajes de datos (17-abr-2002), que posteriormente fueron incluidos en el Código Penal. Cabe destacar que se pensó en esto luego de que uno de los primeros ataques a websites en el país a través de la técnica del Defacing fuera a la página del Municipio de Quito en el año 2001, vale recordar que el primer delito informático que se cometió en el Ecuador fue en el año 1996 en un caso conocido, que fue denunciado pero que nunca obtuvo sentencia y es sobre el redondeo que se realizaba en las planillas realizadas por el antiguo EMETEL, y que no se sabía a dónde se dirigían estas cantidades que muchas veces eran demasiado pequeñas para que cause discusión, pero ya en grandes cantidades era una cantidad de dinero muy apreciable, en esto se puede decir que se utilizó la técnica del salami o rounding Down.

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, publicada en el R.O. / Sup.557 del 17 de Abril del 2002, tiene un avance muy importante en el sentido de incluir figuras penales que castiguen los ilícitos informáticos, con lo cual junto al Código Penal integran normas creadas para la Sociedad de la Información.

Dentro de estas normas promulgadas en la Ley 67 para posteriormente ser transcritas al Código Penal, constan los siguientes ilícitos informáticos:

Art.57 LCEFEMD: Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Art.58 LCEFEMD, Conc. Art.202.1 CP: Contra la Información Protegida.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

2.3.6 México

El estado mexicano en su Código Penal Federal, dedica un capítulo del noveno título de su segundo libro" ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA", donde de manera extremadamente sintética, establece la protección de las comunicaciones. Es en principio escasa la legislación penal al respecto, pero aclaramos, que hay estados mexicanos que tienen sus propias tipificaciones al respecto, a lo que no remitiremos en orden a la extensión que implicaría contemplar cada uno de ellos.

2.4 Entorno Nacional

Desde una perspectiva histórica, el Perú ha sido profundamente afectado por una corrupción administrativa y estatal, que puede medirse desde las postrimerías del periodo colonial hasta nuestros días, lo que ha limitado el desarrollo y el progreso del país.

Dado lo anterior, “ha sido imposible conocer entonces la verdadera magnitud de los “delitos informáticos”, ya que la mayor parte de estos delitos no son descubiertos o no son denunciados a las autoridades responsables” y si a esto se suma la falta de leyes o la mala aplicación de las ya existentes con el fin de proteger 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 mantenga bajo la llamada “cifra oculta” o “cifra negra”.

Los resultados de diversas investigaciones han demostrado que, en varios países de la región, la corrupción y la impunidad han permitido a organizaciones criminales desarrollar y establecer verdaderas estructuras

de poder paralelas. 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 nuestro país se dio una ley Nº 30096, la cual fue muy cuestionada por sus diversos vacíos legales por lo que el pueblo expresando su rechazo, pidió que se observará la autógrafa, ahora ley 30096, la cual dicen debió volver a Comisión en el mejor de los casos, o pasar al archivo y volverse a plantear una propuesta de la adhesión del Perú al Convenio de Cibercrimen, en un marco de respeto irrestricto a las libertades y derechos constitucionalmente protegidos, y en dicho marco plantear una legislación en materia de delitos informáticos, analizar qué hacer con los delitos por medios informáticos y brindar herramientas de informática forense a la Policía.

2.5 Experiencias exitosas

Respecto a otros trabajos realizados de manera oportuna y eficaz, existe el elaborado por **Ricardo Elías Puelles** el cual titula, Luces y sombras en

la lucha contra la delincuencia informática en el Perú, en donde se analiza con mayor profundidad los avatares que nuestro país ha afrontado en el combate contra la ciberdelincuencia.

Cabe mencionar el trabajo realizado por **Jorge Rafael Lujan Sánchez** de título El Contenido Material de los Delitos Informáticos en el Código Penal Peruano, donde Identifica la realidad que evidencia la existencia de los Delitos Informáticos, precisando las posturas que adoptan la Doctrina y la Legislación tanto extranjera como nacional respecto a los Delitos Informáticos.

Así mismo el trabajo realizado por **Albert Gallego Yuste**, titulado Delitos Informáticos: Malware, Fraudes y Estafas a Través de la Red y cómo Prevenirlos, donde nos resalta cada uno de los procesos y mecanismos que utilizan los infractores con el fin de perpetrar los fraudes y delitos informáticos, prestando especial atención al software que se utiliza para estos casos, para una mejor comprensión de los puntos a vigilar por parte de los usuarios.

CAPÍTULO III

PROPUESTA LEGISLATIVA

LEY ESPECIAL DE LOS DELITOS INFORMÁTICOS

3.1 Exposición de motivos

Teniendo en cuenta que la Constitución Política de Perú reconoce que la persona es el fin supremo de la sociedad y el eje principal de toda actividad económica; y considerando también que la informática juega un papel importante dentro de las actividades diarias de los seres humanos, tanto así que es empleada en todas las actividades laborales que el hombre realiza, ya sea en la educación, en la salud, y principalmente en el comercio; pero así como la informática ha evolucionado para ser utilizada en el bien de la comuna, permitiéndonos optimizar y sistematizar las tareas ahorrándonos espacio y sobre todo tiempo, de la misma manera esta evolución se ha convertido en la perfecta plataforma delictiva en la que se basan los ahora llamados delincuentes de cuello blanco.

Este nuevo fenómeno delictivo ha preocupado a nuestros legisladores en el afán de establecer lo correctos patrones de comportamiento en los diferentes campos del Derecho, sin embargo, con la denominación de delitos informáticos se han encontrado muchas críticas a las que inclusive tiene que enfrentar el propio legislador para una adecuada tipificación, ya que bajo ante diversas situaciones podemos encontrar delitos cometidos

por medios informáticos, o bien, los ilícitos que se cometieran de una manera directa en contra de lo que implica todo el mundo del sistema cibernético como sería los hardware, los software, etc. y que posiblemente estaríamos en presencia de una regulación que se encuentra ya establecida como es la del Derecho de Autor, así como la violación a la confidencialidad de la información contenida en medios informáticos, o bien atentar contra éstos últimos, al evolucionar la informática evolucionan los método y las formas de las que se valen los delincuentes para cometer ilícitos El objetivo principal de este documento es la prevención de los delitos informáticos, poniendo en alerta a la comunidad de usuarios acerca de las amenazas que se ciernen sobre ellos al utilizar cualquier tipo de sistema informático. Sobre este objetivo principal, se proponen los siguientes sub-objetivos:

3.2 Texto Normativo

TÍTULO I: Disposiciones Generales

Artículo 1º.- Objeto de Ley

La presente Ley tiene por objeto la prevención y la sanción de los actos ilícitos que afectan de manera directa a los sistemas de información y bienes jurídicos debidamente tutelados, mediante la utilización de las

tecnologías de la información y comunicación, para combatir de manera eficaz a los cibert delincuentes.

Artículo 2º.- Ámbito y Aplicación de la Ley

La presente Ley rige es de aplicación general y rige en todo el territorio nacional de la república del Perú, a toda persona natural o jurídica, nacional o extranjera

TÍTULO II: Disposiciones Específicas

Artículo 3º.- Glosario de Términos

Tecnología; Conjunto de instrumentos, recursos técnicos o procedimientos empleados en un determinado campo o sector.

Sistemas; Conjunto de elementos que se encuentran relacionados entre sí y que buscan un objetivo en común.

Informática; Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.

Datos; los datos son expresiones generales que describen características de las entidades sobre las que operan los algoritmos.

Información; La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje.

Base de datos; Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Acceso indebido a Datos informáticos

Artículo 4º.- El que intencionalmente y sin autorización o excediendo lo permitido acceda, intercepte, utilice parcial o total un sistema informático y utilizando las tecnologías de la información, será sancionado con prisión de uno a cuatro años.

Acceso Indebido a Sistemas Informáticos

Artículo 5º.- El que con la intención de utilizar un dispositivo de la tecnología de la información y accede parcial o en forma total a cualquier programa o a los datos para apropiarse de ellos o cometer cualquier ilícito, será sancionado con prisión de dos a cuatro años.

Interferencia del Sistema Informático

Artículo 6º.- Quien sin justificar altere el funcionamiento de un sistema de información de manera temporal o total, será sancionado con prisión de dos a cinco años.

Daño a sistemas de Información

Artículo 7º.- El que modifique, dañe, destruya o ejecute un programa para inhabilitarlo o realice cualquier acto que altere su funcionamiento será sancionado con prisión de tres a cinco años.

Artículo 8º.- La persona que haga uso de tecnología de información o comunicación, tenga posesión, venda, preste, alquile dispositivos, contraseñas, códigos con la intención de vulnerar un sistema informático, será sancionado con prisión de dos a cinco años.

Delitos Informáticos

Estafa Informática

Artículo 9º.- La persona que influya en el ingreso en el procesamiento, de datos mediante el uso de las tecnologías informáticas, usando datos falsos para obtener un beneficio patrimonial para sí o para otro, será sancionado con prisión de dos a cinco años.

Fraude Informático

Artículo 10º.- El que utilizando indebidamente las tecnologías de la información manipulando sistemas o cualquiera de sus integrados consiguiendo insertar instrucciones falsas, resultando con ello el perjuicio ajeno, será sancionado con prisión de tres a seis años.

Espionaje Informático

Artículo 11º.- El que obtenga información, datos reservados o confidenciales, valiéndose de las tecnologías de la información o comunicaciones, será sancionado con prisión de tres a cinco años.

Hurto Utilizando los Medios Informáticos

Artículo 12º.- El que se apodere de bienes y valores, tangibles o intangibles, personales o patrimoniales sustrayéndoles de su propietario o poseedor utilizando las tecnologías de la información o comunicaciones, para obtener un beneficio económico para sí o para otro, será sancionado con prisión de dos a cinco años.

Ataque DOS (Denegación de Servicios) y Manipulación de Dispositivos para duplicidad de tarjetas y otros

Artículo 13º.- El que valiéndose de las tecnologías de la información o comunicación y con intenciones de impedir a los usuarios el ingreso a los

sistemas informáticos, servicios de redes públicas o privadas, será sancionado con prisión de dos a cinco años.

Artículo 14º.- Los administradores de las redes informáticas públicas o privadas que deshabilitasen los datos de acceso a la misma, será sancionado con prisión de dos a cinco años.

Artículo 15º.- El que sin autorización y con intenciones de duplicar, alterar, grabar, clonar, crear o eliminar datos informáticos que están contenidos en una tarjeta inteligente será sancionado con prisión de dos a cinco años.

Artículo 16º.- El que sin justificación y autorización y a través de las tecnologías de la información haga uso de tarjetas inteligentes que ya hayan caducado, o haya sido revocada por la Institución que la emitió, con el propósito de obtener beneficio para sí o para otro, será sancionado con prisión de tres a cinco años.

Artículo 17º.- El que haciendo uso de las tecnologías de la información y comunicación, y con intención de destruir, alterar o dañar los datos de forma total o parcial de libre disponibilidad o confidenciales, en cualquier estado en que se encuentre será sancionado con prisión de tres a seis años.

Artículo 18º.- El que interfiera, obstruya o interrumpa el uso legítimo de sistemas de información, será sancionado con prisión de dos a cuatro años.

Artículo 19º.- La persona que sin autorización alguna, y valiéndose de las tecnologías de la información, intercepte transmisiones, dirigidos al exterior o interior del sistema de una red, será sancionado con prisión de cuatro a diez años.

Artículo 20º.- El que sin autorización y justificación divulga o propaga contraseñas para el acceso a sistemas, programas o datos almacenados en un dispositivo público o privado, con el objeto de lucrarse para sí o para otro, será sancionado con prisión de tres a seis años.

Artículo 21º.- EL que haciendo uso de las tecnologías de la información y sin autorización propague o divulgue imágenes, audios o videos que en su contenido agreda la dignidad, el honor, la reputación de una persona, será sancionado con prisión de tres a siete años.

Artículo 22º.- EL que sin autorización utilice o divulgue los datos personales, imágenes, videos, audios o textos obtenidos mediante las tecnologías de la información, será sancionado con prisión de cuatro a seis años.

Artículo 23º.- EL que utilizando las tecnologías de la información realice conductas sexuales no deseadas o enviar textos, imágenes, audios, videos de contenido sexual a través de las redes sociales, será sancionado con prisión de dos a cinco años.

Artículo 24º.- El que utilizando las tecnologías de la información difunda, venda, exhiba, intercambie, alquile, ofrezca, produzca, material de contenido violento, sexual o pornográfico de niños, niñas, adolescentes o personas con discapacidad, será sancionado con prisión de cuatro a ocho años.

Artículo 25º.- El que haciendo uso de las tecnologías de la información realice, muestre, venda, alquile, reproduzca, ofrezca, intercambie, venda exhiba, material que exponga la realización de actividades sexuales explícitas o no explícitas, reales o en simulación o que utilice voz de niños, niñas, adolescentes o personas discapacitadas, será sancionado con prisión de tres a doce años.

Artículo 26º.- El que a través de las tecnologías de la información adquiera par sí mismo o para otro material pornográfico en donde se haya utilizado niños, niñas, adolescentes o personas con discapacidad, será sancionado con prisión de dos a seis años.

Artículo 27º.- Los proveedores del servicio de internet deberán prestar la seguridad necesaria estableciendo normas de acceso y el bloqueo a páginas de contenido pornográfico infantil, caso contrario se les considerara coautores de los delitos que le correspondan sobre pornografía infantil en la presente norma.

Artículo 28º.- El que sin autorización y haciendo uso de las tecnologías de la información altere, modifique, guarde, coleccione, imágenes, videos, audios de otra persona alterando su estado original será, sancionado con prisión de dos a cuatro años.

Artículo 29º.- El que utilizando las tecnologías de la información realice actos que atenten directamente contra los intereses y la seguridad nacional será sancionado con prisión de cinco a quince años.

Artículo 30º.- Todo aquel que realice actos terroristas o incita al mismo haciendo uso de las tecnologías de la información y comunicación atentando contra la estabilidad nacional, será sancionado con prisión de diez a veinte años.

TÍTULO III: Disposiciones Finales

La promulgación de la Ley N° 30171 “Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos”. Cuya finalidad es adecuar la Ley N° 30096 a

los estándares legales del 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.

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

30096 Ley de Delitos Informáticos.

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

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

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

Art. 5°.- Incorporación de los artículos 154°-A y 183°-B del Código Penal.

Única Disposición Complementaria Derogatoria.- deroga el **artículo 6°** de la Ley N° 30096 Ley de Delitos Informáticos”

CAPÍTULO IV

CONCLUSIONES

1. La historia de la computación se remonta a los años 60s existiendo previamente a ello diversos aparatos rudimentarios que facilitaban las labores del ser humano como las calculadoras, instrumentos para realizar operaciones a través de tarjetas perforadas, inclusive hasta llegar al rudimentario ábaco, llegando hasta las computadoras que han sufrido diversas modificaciones a través de las denominadas “Generaciones”, en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada.
2. Las nuevas tecnologías en un mundo globalizado, siempre presentarán nuevos y constantes beneficios en cada momento de la vida humana pero también implica que nuevas formas delictivas surjan en días, que sin una legislación que prevea estos aspectos, causarán que los nuevos problemas con nuevas tecnologías sean más difíciles de combatir.
3. La Internet ha venido a evolucionar la historia del hombre como lo han hecho diversos inventos, dándose su aplicación en diversas actividades no solo laborales si también en la comunicación, información, entre otras más, convirtiéndose en una herramienta en

beneficio del hombre y todo los aspectos que lo rodean, existiendo siempre el lado negativo que es resultado del crecimiento global, la facilidad que lleva su uso, y las malas intenciones de la personas.

4. La influencia de los sistemas informáticos en el Derecho da lugar a la existencia del denominado Derecho Informático enfocado a la protección de datos informáticos o la información concentrada en medios magnéticos o digitales.
5. Con la protección de diversos bienes jurídicos en las Leyes reguladoras de los delitos informáticos se han encontrado otras leyes con las que pudieran existir algunas contradicciones para su inadecuada aplicabilidad; tal es el caso del delito de hurto y sus agravantes, que también es protegido por el Código Penal.
6. Hoy en día la delincuencia ha crecido de manera considerada en todo el globo terráqueo y con el uso de medios más modernos para realizar sus fines delictivos como el uso de computadoras, siendo el arma más adecuada para combatir este delito es el establecimiento de legislaciones acordes con esa problemática, tanto a nivel nacional, local, así como internacional, toda vez que se está hablando de una delincuencia que se lleva a cabo en todos los rincones del mundo.

7. La problemática de la Delincuencia Informática ha sido tan complicado ya que como se ha mencionado el avance de la tecnología informática ha sido tan impresionante y rápida que ese avance se ha reflejado en los medios computacionales utilizados por la delincuencia; avances que han aparecido en los sistemas para guardar información dentro de esos sistemas informáticos con una mayor seguridad utilizando el sistema conocido de "encriptación", sin embargo la delincuencia se ha asistido de expertos en informática para violar esas seguridad, encontrando así a los denominados Hacker, Lamer, Cracker
8. La delincuencia informática que ha generado en el mundo desde los años 70s grandes daños a personas en lo particular, a empresas, a entidades financieras y a los propios Países. Por ser una problemática de nivel mundial, esta delincuencia ha sido regulada internacionalmente tal es el caso del Convenio de Budapest, al cual no estamos inscritos, La Convención Internacional sobre la Delincuencia Cibernética, uno de los grandes problemas de toda clase de delincuencia es el de detectar el modus vivendi y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad encontramos a la Criminalística que enfocada a

Los Delitos Informáticos, pues con la ayuda de La Policía Nacional se logrará la aprehensión de los delincuentes que utilizan los grandes avances tecnológicos para sus fines delictivos y que se oculta y huye a través de las líneas alámbricas e inalámbricas de esos sistemas computacionales.

CAPÍTULO V

RECOMENDACIONES

1.- Necesariamente brindar una adecuada educación respecto a las tecnologías de la información, en todos los niveles esto nos ayudaría a prevenirla y combatirla.

El legislador siendo la persona idónea, debe contar con todos los conocimientos que le pueda ofrecer el Derecho Informático, para que luego realice una correcta legislación respecto a la problemática que existe en el país.

2.- Dentro de la legislación por definir debe hacerse una clara distinción de los ilícitos informáticos conforme a los bienes jurídicos que se pretende tutelar.

3.- Establecer políticas especializadas para combatir las diferentes conductas antisociales que se realizan haciendo uso de las tecnologías de la Información, cuyo resultado sea la de la comisión de algún ilícito, por lo que su atención debe de ser cuidadosa.

4.- El gobierno debe de interactuar con el pueblo, tener una alta participación para erradicar este flagelo, donde coordine con las instituciones competentes, y no solo adopten un papel de observadores.

5.- La Policía debe de contar entre sus miembros elemento calificados y capacitados, asistiéndose tanto del Derecho Informático,

como también de otras ciencias auxiliares y disciplinas, que ayuden a localizar y detener al delincuente informático.

6.- Nuestro país es necesario que forme parte de organismos y convenios internacionales para llevar a cabo el combate de todo tipo de delincuencia que se da a nivel globalizado,

7.- Para una adecuada legislación de los Delitos Informáticos no sólo se deben de contemplar posibles reformas o adecuaciones al Código Penal, en sus correspondientes apartados, sino modificar otros textos legales; y delimitar así los bienes jurídicos que deben ser protegidos por los ilícitos informáticos.

CAPÍTULO VI

REFERENCIAS

Y

ANEXOS

BIBLIOGRAFÍA

Armando, Á. M. (2008). *La Problemática Jurídica en la Regulación de los Delitos Informáticos.* México.

Consentino, G. (1998). *Tras los Pasos de la Seguridad Perdida: Delitos Informáticos.* Mérida, España: UNED editores.

Davara, M. A. (1993). *Derecho Informático.* España: Editorial Aranzandi.

Flores Salgado, L. (2014). *Derecho Informático.* México: Gripo Editorial Patria .

García de la Cruz, J. M. (2009). *Delitos Informáticos.* España: El Cid Editores.

Huerta Miranda, M. (1990). *Los Delitos Informáticos.* Editorial Jurídica Cono Sur.

Jijena Leiva, R. (1993). *Los Delitos Informáticos y la Protección Penal a la intimidad.* Chile: Editorial Jurídica de Chile.

Muñoz M. J. (2009). *Historia de la Computación y los Documentos Informáticos.* España: El Cid Editor.

Nuñez Ponce, J. C. (1998). *Software: Licencia de Uso, Derecho y Empresa.* Lima: Editorial de la Universidad de Lima.

Perez Luño, A. E. (1996). *Manual de Informática y Derecho.* Barcelona: Ariel S.A.

Resa Nestares, C. (2005). *Crimen Organizado Transnacional: Definición, Causas y Consecuencias.* Editorial Astrea.

Ricardo, E. P. (2014). *Luces y Sombras en la Lucha contra la Delincuencia informática en el Perú.* Lima.

Rodriguez, D. M. (2003). *Un nuevo desafío jurídico: Los Delitos Informáticos.* Uruguay.

Romeo Casabona, C. M. (1987). *Poder Informático y Seguridad Jurídica.* España: FUNDESCO.

LEYES Y DECRETOS

Congreso de la República. (1991). *Código Penal.* Lima.

Congreso de la República. (1993). *Constitución Política del Perú.* Lima.

Congreso de la República. (1996). *Decreto Legislativo Nº 822 Ley de Derechos de Autor.* Lima.

Congreso de la República. (1994). *Ley Nº 26301 Accion Constitucional de Hábeas Data.* Lima.

Congreso de la República. (1994). *Ley Nº 26301 Accion Constitucional de Hábeas Data.* Lima.

Congreso de la República. (2014). *Ley Nº 30096 Accion Constitucional de Hábeas Data.* Lima.

Congreso de la República. (2000). *Ley Nº 27309, que incorpora los Delitos Informáticos al Código Penal Peruano.*

Congreso de la República. (2014). *Ley Nº 30096, Ley de los Delitos Informáticos.* Lima.

Congreso de la República. (2014). *Ley Nº 30171, Ley que Modifica la Ley Nº 30096 .* Lima.

Congreso de la República. (1996). *Resolución Ministerial Nº 622-96-MTC/ Secreto de las Telecomunicaciones y Protección de Datos.* Lima.

Selección de la Problemática

PROBLEMÁTICA:	CRITERIOS DE SELECCIÓN					TOTAL DE CRITERIOS CON SI	PRIORIDAD
	Se tiene acceso a los datos a)	Su solución Contribuiría a solución de otros problemas b)	Es uno de los que más tiene incidencia social. c)	Afecta Negativamente a la seguridad jurídica d)	En su solución están interesados los responsables de dos o más sector e)		
"LA INSEGURIDAD AL UTILIZAR LOS SERVICIOS DE REDES SOCIALES Y LA PROBLEMATICA JUDICIAL PARA REGULAR LOS DELITOS INFORMATICOS EN EL PRU-2015"	SI	SI	SI	SI	SI	5	1
"VIOLACION DEL DERECHO A LA INTIMIDAD EN EL PERU A TRAVES DE LOS MEDIOS INFORMATICOS PERIODO - 2015	SI	NO	SI	NO	SI	3	3
REGULACION DE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD EN EL HOSPITAL REGIONAL DE LAMBAYEQUE	NO	SI	SI	NO	NO	2	4
NECESIDAD DE IMPONER SANCIONES PENALES EN EL ORDENAMIENTO JURÌDICO PERUANO PARA LOS INFRACTORES MAYORES DE 15 AÑOS POR EL DELITO DE SICARIATO	NO	SI	SI	SI	SI	4	2
PROBLEMAS Y EFECTOS DE LAS DEFICIENCIAS DE LAS CITACIONES JUDICIALES	SI	NO	NO	NO	NO	1	5

Figura 2: Problemáticas presentadas para Selección del problema a Investigar y dar posible solución.

Identificación del Número de las Partes de un Problema

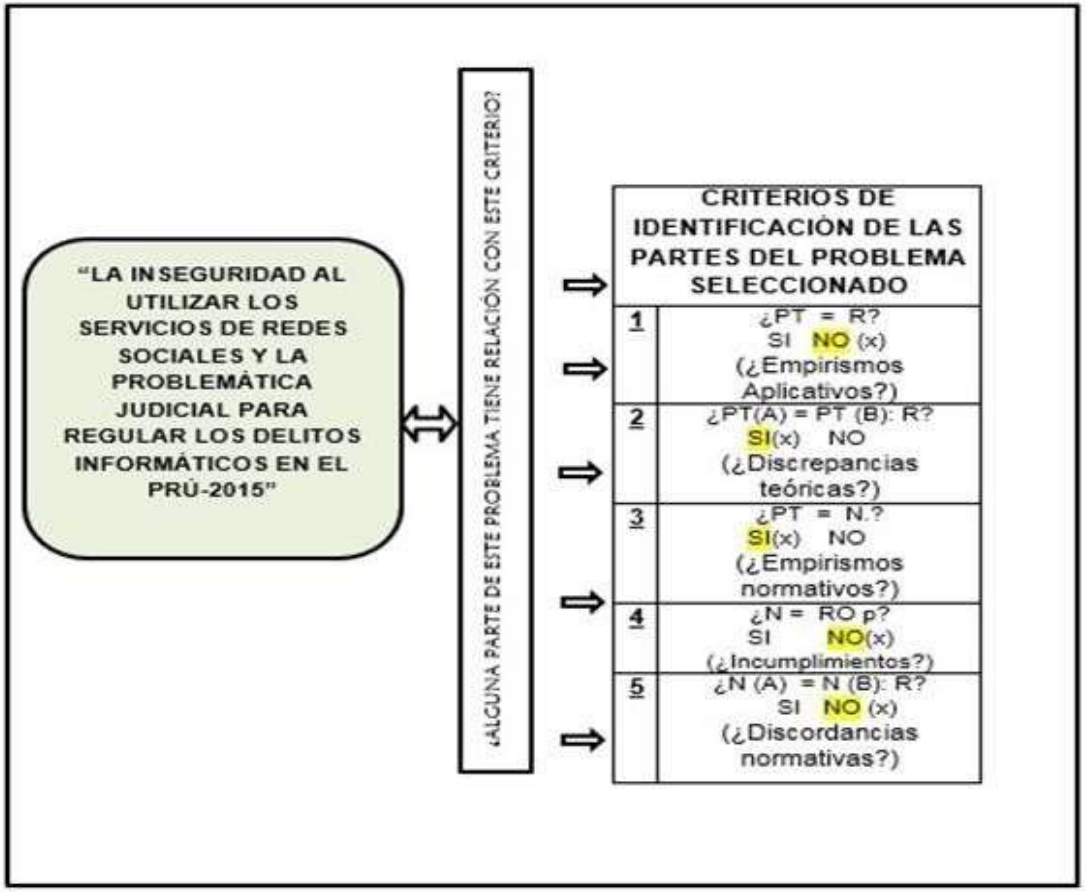

Figura 3: Criterio de las partes de un problema seleccionado.

Identificación del Número de las Partes de un Problema

	CRITERIOS DE SELECCIÓN USADOS COMO CRITERIOS DE PRIORIZACIÓN					SUMA PARCIAL	PRIORIDAD DE LAS PARTES DEL PROBLEMA
	Se tiene acceso a los datos a)	Su solución Contribuiría a solución de otros problemas b)	Es uno de los que más tiene incidencia social. c)	Afecta Negativamente a la seguridad jurídica d)	En su solución están interesados los responsables de dos o más sector e)		
¿PT(A) = PT (B): R? SI(x) NO (¿Discrepancias teóricas?)	1	1	2	2	1	7	1
¿PT = N.? SI(x) NO (¿Empirismos normativos?)	2	2	1	1	2	8	2

Figura 4: Criterios utilizados como priorización en la selección del problema

Matriz Para Plantear la Sub-Hipótesis y la Hipótesis Global

Problema Factor X **Empirismos aplicativos e incumplimientos**	**Realidad Factor A** **"LA INSEGURIDAD AL UTILIZAR LOS SERVICIOS DE REDES SOCIALES Y LA PROBLEMÁTICA JUDICIAL PARA REGULAR LOS DELITOS INFORMÁTICOS EN EL PRÚ-2015"**	**Marco Referencial Facto B**			**Fórmulas de Sub-hipótesis**
		Planteamientos Teóricos	**Normas**	**Legislación Comparada**	
		-B1	**-B2**	**-B3**	
-X1 = Discrepancias Teóricas	**A1 = Operadores del Derecho**	**X**	**X**		**a) A1; -X1; -B1; -B2**
-X1 = Discrepancias Teóricas	**A2 = Comunidad Jurídica**	**X**	**X**	**X**	**b)A2; -X1; -B1; -B2; B3**
-X2 = Empirismos Normativos	**A1 = Operadores del Derecho**	**X**	**X**		**c)-X2; A1; -B1; B2**
-X2 = Empirismos Normativos	**A2 = Comunidad Jurídica**		**X**	**x**	**d)-X2; A2; -B2; -B3**
	Total Cruces Sub-Factores	3	4	2	
	Prioridad por Sub-Factores	2	1	3	

Variables del Marco Referencial

Leyenda:

Planteamientos Teóricos:

-B1 = Conceptos Básicos

Normas:

-B2

Constitución Política del Perú.

La Ley de Delitos Informáticos (Ley N°30096)

Legislación Comparada:

Colombia: Ley 1273 de la Protección de la Información y de los Datos.

República Dominicana: Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.

Argentina: LEY 26.388 de Ley de Delitos Informáticos

Figura 5: Selección de la hipótesis a estudiar

Matriz para Seleccionar Técnicas, Instrumentos e Informantes

O Fuentes para Recolectar Datos

FÓRMULAS DE SUB-HIPÓTESIS	NOMBRE DE LAS VARIABLES CONSIDERADAS EN CADA FÓRMULA (SIN REPETICIÓN Y SÓLO LAS DE A Y B)	TÉCNICAS DE RECOLECCIÓN CON MÁS VENTAJAS Y MENOS DESVENTAJAS PARA CADA VARIABLE	INSTRUMENTO DE RECOLECCIÓN CON MÁS VENTAJAS Y MENOS VENTAJAS PARA CADA VARIABLE.	INFORMANTE O FUENTE QUE CORRESPONDE AL INSTRUMENTO DE CADA TÉCNICA
a) A1; -X1; -B1, B2	A1= Operadores del Derecho	Encuesta	Cuestionario	Informantes: Jueces, Fiscales, INDECOPI
	B2= Normas	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos
b) A2; ; -X1; -B1, -B2; -B3	A2= Comunidad Jurídica	Encuesta	Cuestionario	Informante: Abogados, docentes universitarios, transeúntes.
	B1= Planteamientos teóricos	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos Código Penal; Leyes de Regulación
	B2= Normas	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos
	B3= Legislación Comparada	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos
c) –X2; A1; -B1; -B2	A1= Operadores del Derecho	Encuesta	Cuestionario	Informantes: Jueces, Fiscales, INDECOPI
	B1= Planteamientos Teóricos	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos Código Penal; Leyes de Regulación
	B2= Normas	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos
d) -X2; A2; -B2; - B3	A2= Comunidad Jurídica	Encuesta	Cuestionario	Informante: Abogados, docentes universitarios, transeúntes.
	B1= Planteamientos Teóricos	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos Código Penal; Leyes de Regulación
	B2= Normas	Análisis Documental	Fichas Textuales Fichas resumen	Fuente: Libros y textos
	B3= Legislación Comparada	Análisis Documental	Fuente: Libros y textos	Fuente: Libros y textos

Figura 6: Técnicas, instrumentos e informantes para recolectar datos.

CUESTIONARIO N° 01

DIRIGIDO A PÚBLICO EN GENERAL

Le agradecemos responder este breve y sencillo cuestionario que tiene como propósito obtener datos que nos permitan identificar la necesidad de establecer una reforma a nuestra actual normativa respecto a los Delitos Informáticos según la Ley 30096 – "LEY DE LOS DELITOS INFORMÁTICOS". A su vez es preciso aclarar que el presente instrumento es totalmente anónimo

TIC = **Tecnologías de la Información y Comunicación**

I. DATOS GENERALES: INFORMANTES

Género:

Femenino ( ) Masculino ( )

Edad:

15-20 ( ) 20-30 ( ) 30-39 ( ) 40-49 ( ) 50-59 ( ) 60-69 ( )

70 en adelante ( )

II. PREGUNTAS

1. ¿Tiene conocimiento de la Ley 30069 "Ley de los Delitos Informáticos"?

a) Si

b) No

c) No precisa

d) No sabe

2. **¿Sientes tu derecho a la intimidad violado en las comunicaciones utilizando Internet y las Redes Sociales?**
    a) Si
    b) No
    c) No precisa
    d) No sabe
3. **¿Contratarías y recibirías servicios jurídicos a través de la Red?**
    a) Si
    b) Quizá
    c) Nunca
4. **¿Consideras las compras a través de Internet seguras?**
    a) Si
    b) A veces
    c) Nunca
5. **¿Crees necesaria una regulación para Internet?**
    a) Si
    b) No
6. **¿Crees que necesario preservar la información personal?**
    a) Si
    b) No
7. **¿Sabe usted cuáles son los Delitos más frecuentes asociados a los Delitos Informáticos?**
    a) No
    a) Si

8. **¿Sabe usted Cuáles Son Las Entidades Encargas en el Perú De Velar Por La Protección De Los Niños Y Adolescentes si son violentados en sus derechos a través del uso de Las TIC?**

    a) No

    b) Si

9. **Sabe que daño puede causar un delito informático**

    a) Si

    b) No

10. **¿crees que debe sancionarse el acoso sexual a través del uso de las TIC?**

    a) Si

    b) No

AGRADECEMOS SU AMABLE COLABORACION