UNIVERSIDAD DE HUANUCO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

“VACÍOS LEGALES QUE IMPOSIBILITAN LA SANCIÓN DE LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL PERUANO-2015”

TESIS PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

TESISTA:

IVETT CLARITZA SEQUEIROS CALDERON

ASESORA:

MIRTHA JANET BORJAS GUERRA DE ALARCON

LIMA - PERU

2016

DEDICATORIA:

Este trabajo de investigación lo dedico a toda mi familia, que siempre me apoya incondicionalmente, por su comprensión y el tiempo, que con esfuerzos y sacrificios han sabido compartir mis momentos más difíciles y mis momentos mas alegres.

AGRADECIMIENTO:

A DIOS Por la vida, sabiduría y fortaleza
A la Universidad de Huánuco, por las facilidades en el camino de nuestros estudios.
A los Maestros que impartieron sus enseñanzas, conocimientos con mucha paciencia y abnegación para la culminación de esta maestría.
Así mismo a todas las personas que han colaborado de una u otra manera humilde y desinteresada que me han llevado a obtener un gran éxito.

INDICE

RESUMEN

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

A pesar de ello, 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. Sin embargo, estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos “pishing”, la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

PALABRAS CLAVE: Delitos informáticos, Ley 30096, Ley 30171, vacíos legales

ABSTRACT

In recentyears, a product of evolution of computertechnology has developed a new form of criminalitycalledcybercrime. In relationtothis new criminal way, in Perutheyhaveissuedlaws, whichaimtoprevent and punishillegalactivitiesaffectingcomputersystems and datas as well as secretcommunications, and other legal goodsbeingaffectedwiththistype of crime are as equity, publicfaith and sexual freedom. Law No. 30096 "informationcrimesAct" wasenactedon 21 and publishedonOctober 22, 2013 in theofficialnewspaper "El Peruano". ThenitwaspartiallyamendedbyLaw No. 30171 "LawamendingtheLaw 30096, Lawoninformationcrimes", promulgatedon 9 and publishedonMarch 10, 2014.

However, somebehaviorsdeployed in thecomputerworld, doesnotimplyignoringtheadvantages and facilitiesofferedbythesesystems. There are obviousbenefits of technologicaladvancesthatbringtosocietythe use of informationtechnology and communication. However, thesetechnologicaladvancesmakepossible a new mode of committingtraditionalcrimessuch as fraud and in turnfacilitatesthecommission of new crimessuch as penetrationintocomputernetworks, sendingspam, fishingforinformation "phishing", the digital piracy, themaliciousspreading of viruses and otherattacksoncriticalinformationinfrastructures.

KEYWORDS: CybercrimeLaw 30096, Law 30171, loopholes

INTRODUCCIÓN

Actualmente, en todos los ámbitos y actividades de las personas está inmerso la tecnología, especialmente la influencia de la informática, que se encuentran presente en toda actividad laboral, empresarial, educativa, de recreación, etc, aspectos que dependen día a día más de un adecuado desarrollo de la tecnología informática. Como toda tecnología, brinda beneficios, también se le encuentra deficiencias, ya sea en su desarrollo de software como hardware.

Como consecuencia de este avance informático y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, «delitos informáticos».

Para la realización de la presente investigación, se enfocará desde la conceptualización respectiva del tema, generalidades asociadas a este delito,estadísticas, efecto de éstos en diferentes áreas, como poder afrontar la amenaza de los delitos a través de la seguridad,aspectos de legislación informática, buscando encontrar en el Código Penal algunos vacíos, que nos impidan realizar estas actividades sin miedo a ser vulnerados, y que estos delitos queden impunes.

Al final del trabajo de investigación se establecen las conclusiones pertinentes al estudio, comentarios, resultados y la bibliografía consultada.

CAPÍTULOI
PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

El desarrollo vertiginoso de la ciencia en los últimos 50 años ha sido sorprendente, la cibernética, ciencia que estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos; ha posibilitado que el ser humano pueda alcanzar niveles de conocimiento nunca antes imaginado, crear espacios virtuales de ensueño, y usos que solo en la fantasía del ser humano del pasado se creían concebibles, que sin embargo hoy son realidad.

Pero como en todo desarrollo científico y que hacer de la vida, junto a ese desarrollo útil y fantástico para el ser humano, la cibernética ha posibilitado la aparición de un nuevo tipo de delito, los que hoy son llamados delitos informáticos, un aspecto difícil y complicado para la jurisprudencia, que no se puede desarrollar al ritmo del avance del desarrollo científico y tecnológico y no sabe cómo enfrentar la ciberdelincuencia, porque simple y llanamente el sistema jurídico de los países, no había previsto la aparición de tanto y distintos tipos de delitos, que por su aparición, vertiginosa como el desarrollo de la ciencia misma, no están contempladas dentro de las legislaciones.

El punto básico de este problema, es que, desde el estudio de la ciencia jurídica, se sabe y se puede probar, que los llamados delitos informáticos son reales, pueden y deben ser sancionados por la ley; pero, la mayoría de los códigos penales de los países del mundo, tienen el principio jurídico, como protección de los derechos humanos, que lo que no está prohibido por la ley, es legal, es decir, es permitido, y además, que mientras que la ley no lo determine, el delito conocido por los juristas e incluso tipificado, no puede ser aplicado a nadie, porque

ello sería abuso de autoridad, con el complemento, que la ley no puede ser retroactiva.

En nuestro país, el año 1991 se puso en vigencia el Nuevo Código Penal, según ROXIN (2004) con el objetivo de incluir dentro de ellos los delitos nuevos que no habían sido considerados en loa anteriores, pero el nuevo enfoque no ha sido suficiente para tener en cuenta que en el poco tiempo de haberlo implementado, ya existían nuevos delitos, dentro de ellos los delitos informáticos, que no habían sido considerados, y que imposibilitan que los juristas puedan imponer una sanción penal a los infractores, por el principio fundamental, de que la ley no prohíbe no puede ser considerado ilegal, a pesar de tener la certeza real de que en realidad es un delito el que se comete.

Ante esta realidad evidente, y tratando de reparar los vacíos legales, en relación a los delitos informáticos, en el Nuevo Código Penal Peruano, el Congreso de la República emitió la Ley Nº 30096, denominada Ley de los Delitos Informáticos (2013); y a su vez, tratando de enmendar esos nuevos vacíos legales que aparecían ahora, no solo en el Nuevo Código Procesal Peruano, sino en la ley 30096, se aprobó la Ley Nº 30171, denominada Ley Modificatoria de la Ley de Delitos Informáticos (2014), que es la que actualmente determina las sanciones para la ciberdelincuencia.

Recientemente se ha analizado mucho sobre el tema de la falta de exploración y legislación referente a los delitos informáticos en nuestro país, entre los más comunes destacamos a los fraudes electrónicos e informáticos, mediante los cuales los denominados “hackers” extraen de cuentas bancarias y de registros electrónicos, grandes cantidades de dinero dejando en total estado de indefensión a las instituciones financieras, casas de bolsa, sociedades e incluso a personas físicas para defenderse.

La dación de esta ley, en lugar de generar un mejor enfoque para la jurisprudencia en relación a los delitos informáticos, ha creado grandes polémicas y controversias, pues se considera por una parte que está dirigida a mermar la libertad de opinión, y por otra parte, que no está orientada específicamente a lo que debería estar, es decir, hacia los delitos informáticos o ciberdelincuencia, teniendo no solo grandes vacíos legales, sino también contradicciones en relación a la Constitución Peruana y al Nuevo Código Penal Peruano, pues implementa figuras jurídicas de aplicación para los juristas, que las leyes magnas del país, de acuerdo al Ordenamiento Jurídico, no contemplan, y se contraponen al principio jurídico máximo contenido en todos los códigos penales del mundo, que lo que no está prohibido por la ley es permitido, y en consecuencia no puede ser considerado como delito, a pesar que la realidad diga que es un delito, como es el caso de los delitos informáticos hoy en día, porque aparecen tantos, y de tan diferente índole, que el lento caminar de la justicia peruana no puede emanar leyes en relación de ellos, en tiempo real, sino en el pasado, cuando miles de los delincuentes cibernéticos ya se han aprovechado de esos vacíos legales para que sus delitos queden impunes.

La realidad supera a la teoría, y muchos juristas renombrados de nuestro país hablan de los vacíos legales que tienen el Nuevo Código Procesal Penal Peruano, y sus leyes complementarias como son las leyes Nº 30096 y 30171, sobre los delitos informáticos, pero no se precisa cuáles son esos vacíos legales, y lo que es más complicado, no se fundamente ni sustenta, como debe ser en la jurisprudencia, por ser una ciencia, y nadie se pone de acuerdo cuales son esos vacios legales de los que se habla y que incluso algunos mas avezados los sindican como causa principal inconstitucionalidad de las leyes mencionadas

Es muy sencillo hablar de vacíos legales, de anteponer puntos de vista sobre una ley sobre esos aspectos, pero no es fácil el sustentarlos y fundamentarlos, en base a las mismas leyes que los rigen, y eso es necesario y fundamental para poder retroalimentar una ley, o en su

defecto, cambiar algunos artículos de ella, como es menester de la jurisprudencia, para de esa manera eliminar esos supuestos vacíos legales, y que se pueda aplicar la ley sancionadora para los delitos informáticos no considerados dentro de la ley, sin recurrir a estrategias, que en los tribunales internacional contrastan con los sagrados Derechos Humanos, y con el principio universal de lo que no está prohibido por la ley, es permitido, así sea delito.

Ante el desrrollo de la ciencia cibernética, y el crecimiento de la tecnología de la información y la comunicación, que es la que domina en la actualidad en el mundo, y sobre todo, ante el creciente aumento de los delitos informáticos en nuestro país, es necesario que se reconozcan, que se identifiquen, los vacíos legales que existen en el Nuevo Código Penal y en las leyes complementarias mencionadas, para proponer alternativas viables que permitan reducir y/o eliminar el delito informático en el país, aplicando las sanciones necesarias y contempladas dentro de la ley, para que de esa manera los juristas tengan las herramientas necesarias y suficientes para luchar contra la ciberdelincuencia en el país.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 PROBLEMA GENERAL

¿Qué vacíos legales en el Nuevo Código Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015?

1.2.2 PROBLEMAS ESPECÍFICOS

¿Qué acciones ilegales hechas a través de la tecnología de la información son considerados como delitos informáticos en el Perú?

¿Cuáles son los alcances del Nuevo Código Penal Peruano y sus leyes complementarias para sancionar los delitos informáticos en el Perú?

¿Qué vacíos legales en el Nuevo Código Penal Peruano imposibilitan la sanción de los delitos informáticos en el Perú el 2015?

1.3 OBJETIVO GENERAL

Determinar qué vacíos legales en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015

1.4 OBJETIVOS ESPECÍFICOS

- Identificar qué acciones ilegales hechas a través de la tecnología de la información son considerados como delitos informáticos en el Perú.

- Deslindar cuáles son los alcances del Nuevo Código Penal Peruano y sus leyes complementarias para legitimar los delitos informáticos en el Perú

- Identificar qué vacíos legales en el Nuevo Código Penal Peruano imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

1.5 JUSTIFICACIÓN DE LA INVESTIGACIÓN

El delito y la inseguridad ciudadana en todos sus aspectos, crece a ritmo vertiginoso en el país, cada día se crean nuevas fuentes y

formas delictivas, y la sociedad, a través de sus organismos jurisprudenciales, se ven imposibilitados de defenderse ante los delincuentes, en algunos casos, por leyes protectoras y permisivas de la delincuencia, y en otros por la existencia de vacíos legales, que hacen imposible la sanción de delitos, que se saben en experiencia y en realidad que lo son, pero que por disposiciones de las leyes emanadas del Estado, en la cual se considera que lo que la ley no prohíbe es legal, así sea delito, quedan no solo impunes, sino con licencia de ser nuevamente cometidos por los delincuentes, dejando sin protección de ninguna clase a la sociedad.

En el caso de los llamados delitos informáticos, que afectan no solo a quienes se hallan inmersos dentro del campo de la información en el país, sino que a todos y cada uno de los ciudadanos, ya se han dado leyes específicas, como lo han hecho otros países del hemisferio, en base a Convención Internacional de las Naciones Unidas de lo que se debe considerar como delitos informáticos, pero estas, de acuerdo a especialistas de la jurisprudencia nacional, han sido consideradas contradictorias, polémicas, insuficientes y hasta insustanciales para afrontar a la ciberdelincuencia, que se renueva cada día, generando vacíos legales, que en vez de favorecer la lucha contra la ciberdelincuencia, la entorpece, y en casos, extremo, anula las leyes sancionadoras.

La sociedad se protege de la delincuencia solo a mediante de las leyes sancionadoras, posibilitando que los delincuentes pasen a pagar sus delitos en los penales, y de esa manera se reduce la inseguridad ciudadana, pero en los casos que no es posible hacerlo, como es el caso de los delitos informáticos, en lugar de que una ley disuada del delito, al no sancionarlo, alimenta la posibilidad de que sean más personas quienes cometan esos delitos, con la seguridad de la impunidad al comprobar que las

leyes no tienen manera de cómo sancionarlo, a pesar de que todos saben que es un delito.

Es necesario, en el caso de los delitos informáticos, que los vacíos legales existentes, de acuerdo a la opinión experta de juristas nacionales, sean subsanados lo más `pronto posible, debido en forma especial a que el avance de la ciencia y la tecnología de la información y la comunicación en nuestros días, es vertiginoso, y es la que domina el quehacer de nuestra sociedad, y si no se pone alto a la ciberdelincuencia con las herramientas legales necesarias, se corre el peligro de dejar expuesta a la sociedad entera en manos de los ciberdelincuentes, sin poder hacer nada, y sin tener posibilidad de recuperar lo robado a través de los medios informáticos.

La investigación que se realizará, pretende identificar algunos de los vacíos legales existentes en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias, debidamente fundamentados y sustentados, en relación a los delitos informáticos, para de esa manera proponer alternativas de solución al problema legal presentado, y de esta manera dotar de las herramientas necesarias a los juristas, para que puedan combatir a la ciberdelincuencia que crece cada día, al mismo ritmo vertiginoso del crecimiento de la tecnología de la información y la comunicación.

1.6 LIMITACIONES DE LA INVESTIGACIÓN

En las limitaciones que encontré al realizar la presente investigación, observé que la bibliografía jurídica existente es limitada, hay pocos trabajos de indagación sobre este tema.

1.7 VIABILIDAD O FACTIBILIDAD

Este trabajo de investigación es factible porque dará a conocer a la sociedad y público en general las formas actuales de ataques a la información y violación a la privacidad a través de los delitos informáticos. Brindará información de la legislación dedicada a esta materia, saber de qué manera las leyes protegen al usuario, para evitar ser vulnerados y quede impune el abuso de sus derechos.

Creemos que la mayoria de la sociedad desconoce esta clase de alcances y limitaciones, algunos ni siquiera le dan la importancia necesaria. Aparentemente los ciberdelitos, no lastiman físicamente a las personas tampoco causan daños importantes, razón por la cual, esta investigación se ha basado en antecedentes que actualmente se pueden proyectar para generar posibles escenarios como resultado de un ataque. Para evitar que esta forma de delitos queden sin pena o castigo, es dable la revisión de la legislación peruana, para así tener un mayor conocimiento de la aplicación de las normas respecto a esta clase de delitos.

CAPÍTULO II
MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

ROXIN, C. (2004), sostiene que en el pasado, la religión, la moral, las costumbres y las convenciones sociales tuvieron un importante poder regulador de las conductas humanas en la comunidad y en cierto modo, podían por si solas mantenerlas unidas o vinculadas.

El mismo autor dice que la diversidad y fragmentación de las concepciones modernas en cuanto a los valores que llegó a concebir el individuo, facilitaron que lo costumbrista, lo religioso y lo moral perdieran poder organizador en la sociedad.

.

Afirma además, que, ante este hecho, fue necesaria la aparición del Derecho para asumir esas funciones, y que en principios fue, para determinar a través de obligaciones y derechos, lo que la sociedad consideraba que se podía realizar en forma libre sin afectar lo justo, y lo que se debe sancionar en caso se afecte los derechos de las otras personas, que en suma, son los derechos de la ciudadanía.

Para el autor, esta forma tradicional de regulación del derecho se mantiene vigente, con las limitaciones propias de que la creación del Derecho, no puede estar jamás de acuerdo a los cambios y transformaciones de las sociedades, y siempre han existido de una u otra forma vacíos legales, que la jurisprudencia a través del ejercicio de implementar justicia ha solucionado generalmente en forma satisfactoria.

Sin embargo, los agentes en los últimos años, específicamente desde el desarrollo de la ciencia de la tecnología de la comunicación y la información, la sociedad tiene cambios tan rápidos y profundos, y han

aparecido una cantidad insospechada de ilícitos penales ligados a tecnología y a la ciencia de la comunicación y la información, que la ciencia del Derecho no alcanza a cubrir y se generan vacíos legales que impiden la lucha contra la delincuencia, llamado en estos tiempos como delitos informáticos.

Además indica que los tipos penales de delitos considerados en las legislaciones peruanas, resultan anacrónicos para la situación actual, ya que cuando se redactó el actual Código Penal de 1991, el legislador nacional no tomo en cuenta los delitos informáticos.

En la Ley 27309 (2000), se incorporaron los llamados delitos informáticos en los artículos: 207-A: Acceso indebido a una base de datos; 207-B: Sabotaje Informático y artículo 207-C: Agravantes, dándole solo una temática con respecto a los bienes corpóreos dejando lagunas legales que hoy lamentamos.

Los delitos informáticos tienen su radio de acción principalmente en los atentados contra los derechos de autor, violación de la intimidad personal, falsificación de documentos informáticos, entre otros. Si se inspecciona el sistema penal peruano, se puede apreciar que el texto punitivo tipifica ciertas conductas posibles de ser cometidas mediante medios informáticos, el turismo sexual infantil **(**artículo 181-A**)**; la pornografía infantil **(**artículo 183-A**)** ;el hurto agravado utilizado sistema de transferencia electrónica de fondos de la telemática en general, (numeral 3 del segundo párrafo del artículo 186); el delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos **(**Inciso 8 del artículo 198**)**, e incluso el delito de daños (artículo 205), desde la perspectiva del atentado contra el hardware (en su condición de bien material),el acceso indebido a una base de datos,(artículo 207-A), el sabotaje informático (artículo 207-B) y sus agravantes (artículo 207-C).

Al respecto TIEDERMANN, K (2000), refiere que la tarea del Derecho no es quedarse atado a viejas categorías teóricas que nada sirven sino, al contrario, es adaptarse y proveerse de nuevas modos de prevención y protección de la sociedad. Es por este motivo que el Derecho Penal debe inspeccionarse a sí mismo, y encuadrase en estos hechos que protejan a las personas, mas no esconderse en acequias legales que no ayudan a nada.

HUME, J. (2003), indica que el Derecho sustantivo debe también prevenir la comisión de éste tipo de hechos que de ninguna manera pueden ser entendidos como errores involuntarios.

Para PEÑA, D. (2005), el Derecho material debe amparar los intereses de la sociedad, logrando evitar manipulaciones computarizadas habituales o no, apoyadas en el conocimiento de los objetos, programas, así como de algunas informaciones que incrementen y hagan imposible la revelación de estos ilícitos.

El mismo PEÑA, D. (2007), manifiesta que la nebulosa del ciberdelito, requiere un estudio especial y conocimientos de causa, para poder cumplir con la labor de tipificar suficientemente estos delitos con miras hacia una adecuada protección social, ya que la expansión del mundo informático es progresivo en nuestro medio, ya sea en el sector público o sea en el privado (el comercio, la actividad bancaria, la actividad industrial, el negocio de los particulares y empresas, etc.)

HUGO, S. (2004), dice que ha llegado el momento que el Derecho Penal responda a las múltiples exigencias sociales que el mundo moderno demanda, y de este modo, rompa su sólida moldura anquilosada y evolucione conjuntamente con el desarrollo de la investigación científica, para así permitir el real resguardo de la seguridad y de la sociedad, ya que al parecer, se está quedando anquilosado en esta materia de los novísimos delitos informáticos.

2.2 BASES TEÓRICAS

2.2.1 DELITO INFORMÁTICO.

Con el crecimiento de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Encontramos diferentes maneras de delinquir lo hacen por medio de configuraciones electrónicas que van que son ligadas a diferentes tipos de herramientas delictivas que buscan infiltrase y dañar todo lo que a su paso encuentren en el dominio informático.

Al respecto BRIZZIO, C. (2000), dice que el crimen informático puede incluir delitos habituales como el fraude, el robo, chantaje, falsificación y el desfalco de patrimonios públicos en los que los ordenadores y redes han sido empleados como medios.

STANDLER,R (2002),señala que un delito informático es toda aquel acto, habitual y no jurídico, que se ejecuta por medios informáticos o que tiene como objeto arruinar computadoras, aparatos eléctricos y redes cibernéticas.

JENSON, B. (1996), indica que, de acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

De igual manera, HUGO, S, (2004), dice que la definición genérica para delito informático de la Organización para la

Cooperativa Económica y el desarrollo, es cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.

2.2.2 CARACTERÍSTICAS DEL DELITO INFORMÁTICO.

Según TELLEZ, J. (1995), los delitos informáticos presentan las siguientes características principales

a) **CONDUCTAS CRIMINALES DE CUELLO BLANCO**

b) **ACCIONES OCUPACIONALES**

c) **ACCIONES DE OPORTUNIDAD**

d) **PROVOCAN SERIAS PÉRDIDAS ECONÓMICAS**

e) **OFRECEN POSIBILIDADES DE TIEMPO Y ESPACIO**

f) **MUCHOS CASOS Y POCAS DENUNCIAS**

g) **PROLIFERACIÓN CONTINÚA**

h) **ILÍCITOS DE IMPUNIDAD ANTE LA LEY.**

i) **DELITOS INFORMÁTICOS QUE GENERA FRAUDE O ROBO POR MEDIOS DE TARJETAS DE CRÉDITO.**

j) **REGISTROS MAGNÉTICOS TRANSITORIOS**

k) **SISTEMAS IMPERSONALES**

l) **EN EL DISEÑO DE UN SISTEMA IMPORTANTE ES DIFÍCIL ASEGURAR QUE SE HAN PREVISTO TODAS LAS SITUACIONES POSIBLES Y ES PROBABLE QUE EN LAS PREVISIONES QUE SE HAYAN HECHO QUEDEN HUECOS SIN CUBRIR.**

m) **EN EL CENTRO DE CÁLCULO HAY UN PERSONAL MUY INTELIGENTE**

n) **EL ERROR Y EL FRAUDE SON DIFÍCILES DE EQUIPARAR.**

2.2.3 TIPOS DE DELITOS INFORMÁTICOS.

Según Hüme, J. (2005) la criminalidad informática incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

a) CRÍMENES QUE TIENEN COMO OBJETIVO REDES SOCIALES

b) CRIMENES DESARROLLADOS POR MEDIO DE LOS ORDENADORES DEL INTERNET

c) TIPIFICACIÓN SEGÚN LA ACTIVIDAD INFORMÁTICA.

- Sabotaje informático.
- Fraude a través de computadoras.
- Estafas electrónicas.
- Pesca u olfateo de claves secretas.

- Estratagemas.
- Juegos de azar.
- Fraude a los consumidores por Internet.
- Blanqueo de dinero.
- Copia ilegal de software y espionaje informático.
- Infracción de los derechos de autor.
- Infracción del Copyright de bases de datos.
- Uso ilegítimo de sistemas informáticos ajenos.
- Acceso no autorizado.
- Delitos informáticos contra la privacidad.
- Interceptación de e-mail.
- Pornografía infantil.
- Espionaje.

a) TIPIFICACIÓN SEGÚN EL METODO O INSTRUMENTO.

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

- Modificación de datos tanto en la entrada como en la salida.

- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

- Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas.

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

- Acceso a áreas informatizadas en forma no autorizada.

b) TIPIFICACIÓN SEGÚN EL OBJETIVO O FIN.

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

- Destrucción de programas por cualquier método.

- Daño a la memoria.

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

c) TIPIFICACIÓN SEGÚN ACTIVIDADES DELICTIVAS GRAVES.

- Terrorismo.

- Narcotráfico.

- Espionaje
- Espionaje industria.
- Otros delitos:

2.2.4 EL PROBLEMA DE LA JURISPRUDENCIA SOBRE DELITOS INFORMÁTICOSA NIVEL INTERNACIONAL.

A medida que se ha ido incrementando la incidencia delictiva electrónica, numerosos países han promulgado leyes que declaran ilegales nuevas prácticas como el caso de la piratería informática; además, han actualizado leyes obsoletas para que delitos virtuales habituales; en los cuales se incluye el fraude, el vandalismo o el sabotaje; se consideren ilegales. A Pesar de estos y otros esfuerzos, las autoridades de turno todavía afrontan graves problemas en el ámbito de informático.

En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada por la doble tipificación penal: la carencia de leyes similares en los dos países que prohibían ese comportamiento; y, esto impidió la cooperación oficial, según informa el Departamento de Justicia de los Estados Unidos.

Los oficiales del país sudamericano requisaron el apartamento del pirata e incautaron su equipo de computadora, aduciendo posibles violaciones de las leyes nacionales.

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas.

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

c) Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

2.2.5. EL CONVENIO INTERNACIONAL SOBRE CIBERCRIMINALIDAD

El Convenio sobre cibercriminalidad, también conocido como el Convenio de Budapest (2004), es el primer tratado internacional que busca hacer frente al incremento de los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. El Convenio incluye una lista de los crímenes que cada estado firmante debe transponer a su legislación propia.

Requiere la criminalización de actividades tales como la piratería (que incluye la producción, venta o distribución de herramientas de hacking) y los delitos relacionados con la pornografía infantil, y se expande responsabilidad penal por la violación de la propiedad intelectual.

Asimismo, exige a cada estado participante la implementación de ciertos mecanismos procesales dentro de sus leyes.

Finalmente, el Convenio obliga a los estados firmantes a prestar cooperación internacional en la mayor medida posible para las investigaciones y procedimientos relativos a infracciones penales vinculadas a sistemas y datos informáticos o para la recogida de pruebas electrónicas de una infracción penal

La transposición de las disposiciones del Convenio en la legislación nacional es difícil, especialmente si se requiere la incorporación de las expansiones sustanciales que van en contra de los principios constitucionales.

2.2.6 DELITO INFORMÁTICO DE ACUERDO AL NUEVO CÓDIGO PENAL PERUANO.

El Código Penal Peruano , regulado por el Decreto Legislativo N° 635, con diversos artículos protege la información contenida en los software, o lo que se le asemeje, considerándose a ello dentro de delitos tipificados como por ejemplo la apropiación ilícita o violación a la intimidad, pero no se tipifica el Delito Informático propiamente dicho, sancionándose a éste, sin nombrarlo, dentro de la comisión de una comunidad de delitos cometidos por los sujetos delictivos utilizando software o hardware.

a) DELITO DE VIOLACIÓN A LA INTIMIDAD

En el Código Penal está tipificado en el artículo 154 el Delito de violación a la intimidad.

b) DELITO DE HURTO POR TRANSFERENCIA ELECTRONICA DE FONDOS, TELEMATICA EN GENERAL Y EMPLEO DE CLAVES SECRETAS

Esta referido en el articulo 185 del Código Penal.

c) DELITO DE FALSIFICACIÓN DE DOCUMENTOS INFORMÁTICOS.

Decreto Legislativo 681 modificado por la Ley 26612.

2.2.7 VACÍO LEGAL O LAGUNA JURÍDICA.

BASTERAS (2003), dice que se denomina laguna jurídica o del Derecho a la ausencia de reglamentación legislativa en una materia concreta. Es una situación de vacío en la ley que ha sufrido la patología jurídica de omitir en su texto la regulación concreta de una determinada situación, parte o negocio, que no encuentra respuesta legal específica; con ello se obliga a quienes aplican dicha ley (jueces, abogados, fiscales, secretarios judiciales, etc.) al empleo de técnicas sustitutivas del vacío, con las cuales obtener respuesta eficaz a la expresada tara legal.

2.2.8 HERRAMIENTAS UTILIZADAS PARA SU SOLUCIÓN.

ATRIA, F. y otros (2005). Dicen que ante esta situación, si a un juez se le solicita una resolución, no puede negarse y debe suplir la laguna jurídica a través de distintas herramientas. Las más habituales son:

a) DERECHO SUPLETORIO

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

b) **INTERPRETACIÓN EXTENSIVA**

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

c) **ANALOGÍA**

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

d) **ACUDIR A OTRAS FUENTES DEL DERECHO**

Como la costumbre o los principios generales del Derecho.

e) **NORMA CRUZADA**

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

2.2.9. CASOS EN QUE LA JURISPRUDENCIA PERUANA CONSIDERA QUE EXISTEN VACÍOS LEGALES.

Por más esfuerzos que haga el legislador a fin de contener en el supuesto de hecho general y abstracto que constituye la ley las más variadas e imprevisibles circunstancias, inevitablemente su creación será superada por la realidad.

El paso del tiempo, el cambio de las circunstancias, el avance de la tecnología, hacen que la ley revele tarde o temprano sus imperfecciones.

Pero el problema de los vacíos de la ley no es el reconocer que existen, pues la imperfección del ordenamiento legal es más o menos obvia, y además admitida por la propia ley, sino cuándo estamos frente a un verdadero vacío legal.

a) **CUANDO LA LEY SOLO DA AL JUEZ UNA ORIENTACIÓN GENERAL**

Señalándole expresa o tácitamente hechos, conceptos o criterios no determinados en sus notas particulares, entonces la ley remite al juez de buena fe o a los usos del tráfico o deja a su apreciación si existe un mal uso.

b) **CUANDO LA LEY CALLA EN ABSOLUTO**

Intencionalmente, ya porque no se previó el caso.

c) **CUANDO LA LEY ES INCOMPLETA**

Se refiere al caso en que la ley regula una materia pero sin tener en cuenta alguna de sus posibilidades

2.3 DEFINICIONES CONCEPTUALES

INFORMÁTICA

Tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

DELITO

Acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

DELITO INFORMÁTICO

Acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet

VACÍO LEGAL O LAGUNA JURÍDICA

Carencia de reglamentación legislativa en una materia concreta.

2.4 HIPÓTESIS

2.4.1 HIPÓTESIS GENERAL.

Existen vacíos legales en el Nuevo Código Penal Peruano y en sus leyes complementarias que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

2.4.2 HIPÓTESIS ESPECÍFICAS.

H_1 Existen acciones realizadas a través de la tecnología de la información que son considerados como delitos informáticos en el Perú

H_2 Existen vacíos legales en el Nuevo Código Penal Peruano que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

H3 Existen leyes complementarias en el Nuevo Código Penal Peruano que sancionan los delitos informáticos en el Perú

2.5 VARIABLES

2.5.1 VARIABLE INDEPENDIENTE:

VACÍO LEGAL

Ausencia de reglamentación legislativa en una materia concreta.

DIMENSIONES

Alcances del Nuevo Código Penal Peruano y sus leyes complementarias para sancionar los delitos informáticos

Vacíos legales en la ley Nº 30096 imposibilitan la sanción de los delitos informáticos

Vacíos legales en el Nuevo Código Penal Peruano imposibilitan la sanción de los delitos informáticos

2.5.2 VARIABLE DEPENDIENTE:

DELITO INFORMÁTICO

Acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

DIMENSIONES

Acciones ilegales realizadas a través de la tecnología de la información que son considerados como delitos informáticos.

Acciones ilegales realizadas a través de la tecnología de la información que no son considerados como delitos informáticos

2.6 OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLE DEPENDIENTE	INDICADORES	SUB-DIMENSIONES	INDICADORES	ÍTEMS
Vacío legal	Alcances del Nuevo Código Penal Peruano y sus leyes complementarias para sancionar los delitos informáticos	La ley solo da al juez una orientación general La ley calla en absoluto	Mala redacción Artículos estipulados en las leyes con definiciones ambiguas.	¿Existen los suficientes alcances en el Nuevo Código Penal para sancionar los delitos informáticos? ¿Existen en las leyes complementarias del Nuevo Código Penal los alcances suficientes para sancionar los delitos informáticos?
	Vacios legales en la ley Nº 30096 imposibilitan la sanción de los delitos informáticos	La ley es incompleta	Incompetencia del legislador	¿Están tipificados adecuadamente los delitos informáticos en el Nuevo Código Penal?
	Vacios legales en el Nuevo Código Penal Peruano imposibilitan la sanción de los delitos informáticos	La ley solo da al juez una orientación general La ley calla en absoluto La ley es incompleta	No corresponde a la realidad que se pretende regular	¿Pueden los fiscales y los jueces aplicar de acuerdo al Nuevo Código Penal y a las leyes complementarias adecuadamente las acusaciones y sanciones sobre los delitos informáticos? ¿Cuáles son las dificultades que se encuentra en las leyes?

VARIABLE DEPENDIENTE	DIMENSIONES	SUB-DIMENSIONES	INDICADORES	ÍTEMS
Delito informático	Acciones ilegales realizadas a través de la tecnología de la información que son considerados como delitos informáticos	Ingreso ilegal a sistemas interceptado ilegal de redes interferencias daños en la información (borrado, dañado, alteración o supresión de data crédito) Violación de información confidencial Usos comerciales no éticos	Mal uso de artefactos Chantajes Fraude electrónico Robo de bancos Ataques realizados por crackers Violación de los derechos de autor Pornografía infantil	¿Se tiene clara la especificación y las sanciones de los ingresos ilegales a los sistemas? ¿Se tiene clara la especificación y las sanciones de los daños ocasionados en la información? ¿Se tiene clara la especificación y las sanciones de los chantajes realizados a través de medios informáticos? ¿Es delito los comerciales no éticos en los medios informáticos? ¿Es delito el correo electrónico no solicitado a través de los medios informáticos? ¿Es delito la información con contenido obsceno u ofensivo en los medios informáticos? ¿Es delito el hostigamiento/acoso a través de los medios informáticos?

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. TIPO DE INVESTIGACIÓN

Básica o no experimental. Porque se recogerán los datos directamente de la realidad, y el investigador no manipulará las variables, solo se las describirá tal como se presentan. Además de acuerdo a Barriga Hernández (2004), las investigaciones de este tipo sirven para engrandecer el conocimiento científico.

3.1.1 ENFOQUE

Cualitativa. Porque se relacionan las variables a partir de sus características específicas, y se determina los resultados a través del análisis y la interpretación de los datos fundamentando y sustentando los resultados a través de los antecedentes de la investigación y las bases teóricas.

3.1.2DISEÑO

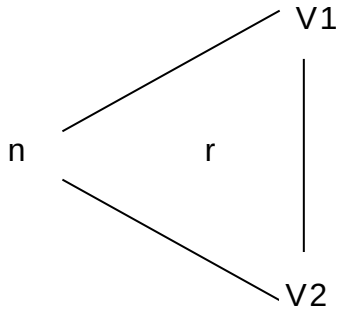
El diseño del presente trabajo de investigación fue no experimental, ya que se realizó sin manipular deliberadamente las variables. Es decir se trata de estudios donde no se alteran intencionalmente las variables.

La investigación es correlacional transeccional.

Según Moreno (2000) una investigación es correlacional porque mediante este tipo de estudio se trata de determinar el grado de relación existente entre dos o más variables en forma cuantitativa mediante el coeficiente de correlación (p. 10,11).

Además es transeccional porque la unidad de análisis es observada en un solo punto en el tiempo.

El trabajo de investigación se representa mediante el siguiente esquema o diagrama:



Donde:

N : Tamaño de la muestra

V1 : Vacío Legal

V2 : Delito Informático

O : Observación y medición de ambas variables

R : Notación estadística de interrelación (Coeficiente de correlación)

3.2 POBLACIÓN Y MUESTRA

POBLACIÓN

La población estará conformada por los fiscales del distrito judicial de Huaura que laboran en el distrito de Huacho.

MUESTRA

Por ser una población relativamente pequeña se considerará a 30 fiscales como muestra**.**

De las 60 personas unidades de análisis se llegó la conclusión de 30 unidades de análisis, como muestra en la presente investigación, aplicando la fórmula del muestreo aleatorio simple, que corresponde Arkín - Kolton:

$$n = \frac{N}{(N-1)\,K^2 + 1}$$

Dónde:

n:tamaño de muestra

N: tamaño de la población

K^2: error muestra

Empleando la fórmula anterior de muestreo y considerando un margen de error de 5% resulta un tamaño de muestra de 24 unidades de análisis:

$$n = \frac{60}{(60-1)\,0.05^2 + 1}$$

n =30 unidades de análisis, serán seleccionados aleatoriamente para que de esta manera nuestra muestra sea lo más representativa posible.

3.3. TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

LA ENCUESTA

Se utilizará para de esa manera poder recoger los datos en forma anónima y facilitar la interacción con los sujetos de la muestra.

La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente por escrito. Ese listado se denomina cuestionario.

Es impersonal porque el cuestionario no lleva el nombre ni otra identificación de la persona que lo responde, ya que no interesan esos datos. Es una técnica que se puede aplicar a sectores más amplios del universo, de manera mucho más económica que mediante entrevistas.

3.3.1. PARA LA RECOLECCIÓN DE DATOS

ENTREVISTA

Se entrevistará a los sujetos de la muestra para de esa manera poder tener los datos específicos en forma directa de los sujetos de la muestra y de esa manera poder analizarlos de acuerdo a los objetivos.

Es la comunicación mediante el contacto directo con el entrevistado y el entrevistador, a través de un dialogo. En el caso de este trabajo, se trató de la recepción de opiniones sin influir en ellas.

Se utiliza la entrevista guiada para focalizar la opinión del entrevistado en los temas de interés para la investigación, lo cual permitirá libertad de opinión, mientras el entrevistador toma notas sobre la información proporcionada.

3.3.2. PARA LA PRESENTACIÓN DE LA INFORMACIÓN

Se procederá al vaciado de los datos en tablas estadísticas no probabilísticas, puesto que al ser una investigación cualitativa se trabaja con los porcentajes de los datos obtenidos. Se utilizará el programa Excel.

3.3.3. PARA EL ANÁLISIS E INTERPRETACIÓN DE DATOS

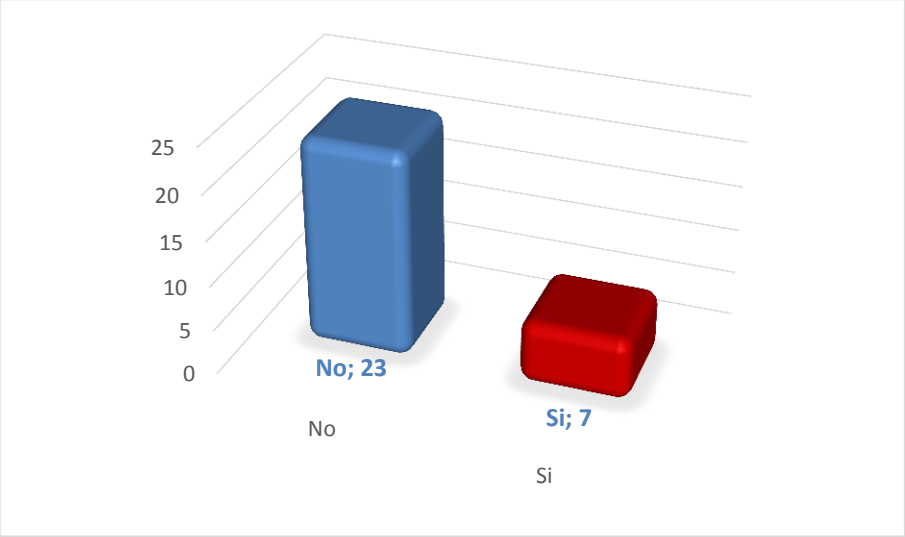
Los datos obtenidos serán interpretados y analizados en relación al marco teórico de la investigación, el cual servirá como sustento y fundamentación de los análisis e interpretación de los datos recolectados.

CAPÍTULO IV
RESULTADOS

4.1. PROCESAMIENTO DE DATOS

1. ¿Existen los suficientes alcances en el Nuevo Código Procesal Penal para sancionar los delitos informáticos?

Ítem	Frecuencia	Porcentaje
Si	7	25%
No	23	75%
Total	**30**	**100%**

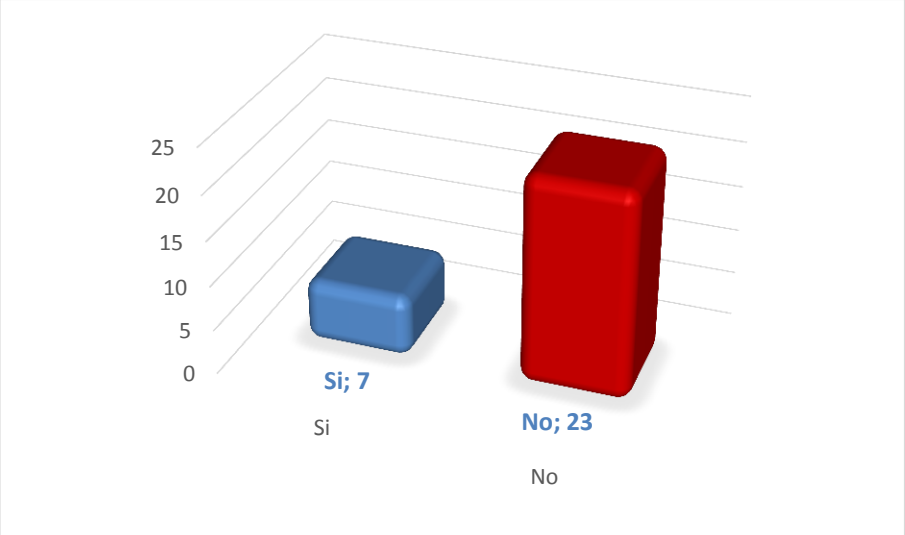


Interpretación

Del total de encuestados, 23 (75%), no creen que el Nuevo Código Procesal Penal cuenta con los suficientes alcances para poder sancionar los delitos informáticos, en cambio con un 25%, creen que si los hay.

2. ¿Existen en las leyes complementarias del Nuevo Código Procesal Penal los alcances suficientes para sancionar los delitos informáticos?

Ítem	Frecuencia	Porcentaje
Si	7	25%
No	23	75%
Total	30	100%

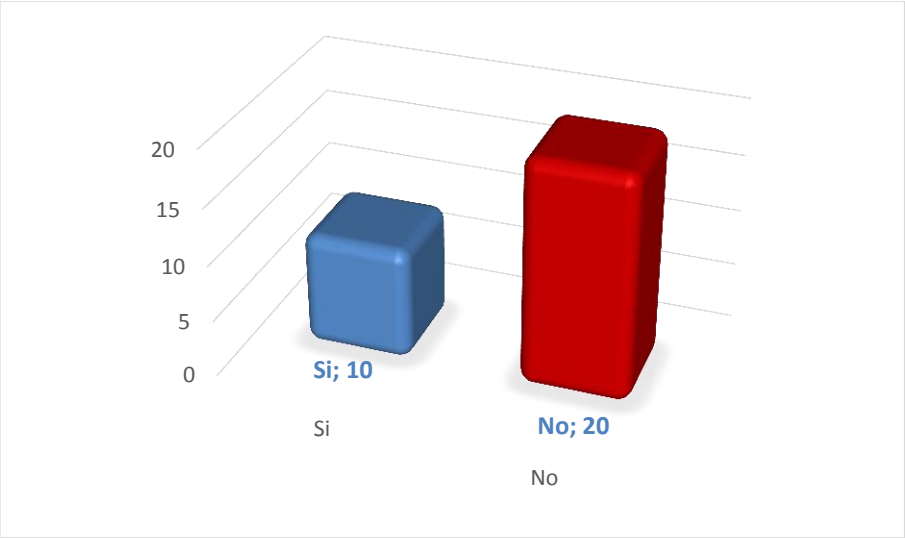


Interpretación

Respecto a si creen que las leyes complementarias del Nuevo Código Procesal Penal cuenta con los suficientes alcances poder sancionar los delitos informáticos, 23 personas (75%) creen que no existen tales alcances, en cambio 7 personas (25%), creen que si los hay.

3. ¿Están tipificados adecuadamente los delitos informáticos en el Nuevo Código Procesal Penal?

Ítem	Frecuencia	Porcentaje
Si	10	33%
No	20	67%
Total	30	100%

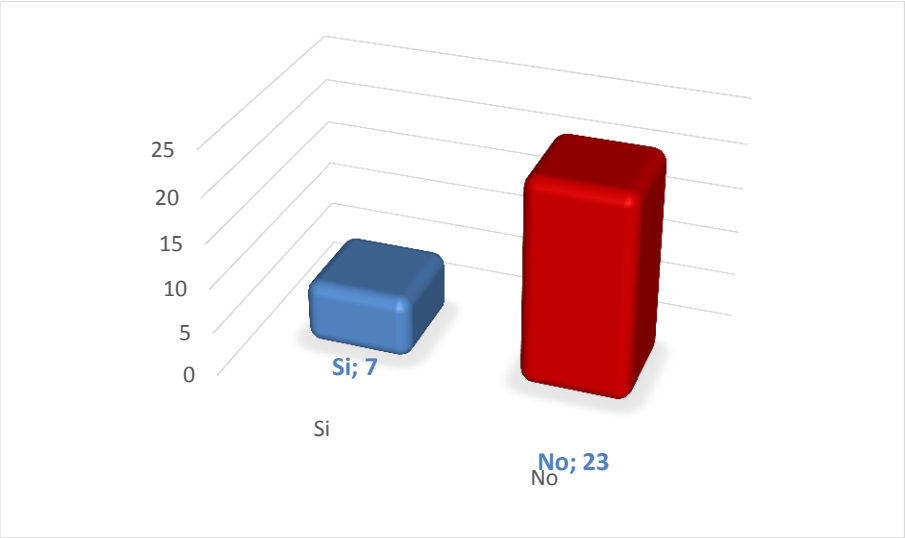


Interpretación

Las opiniones o el alcance que tienen los encuestados, se encuentra dividido, con un ligera mayoría de 20 encuestados con un 67% cree que no están debidamente tipificados los delitos informáticos en el Código Procesal Penal, en cambio 10 personas con un 33% sí creen que si lo están.

4. ¿Se pueden incluir los nuevos delitos informáticos dentro de la tipificación que se realiza en el Nuevo Código Procesal Penal?

Ítem	Frecuencia	Porcentaje
Si	7	17%
No	23	83%
Total	30	100%

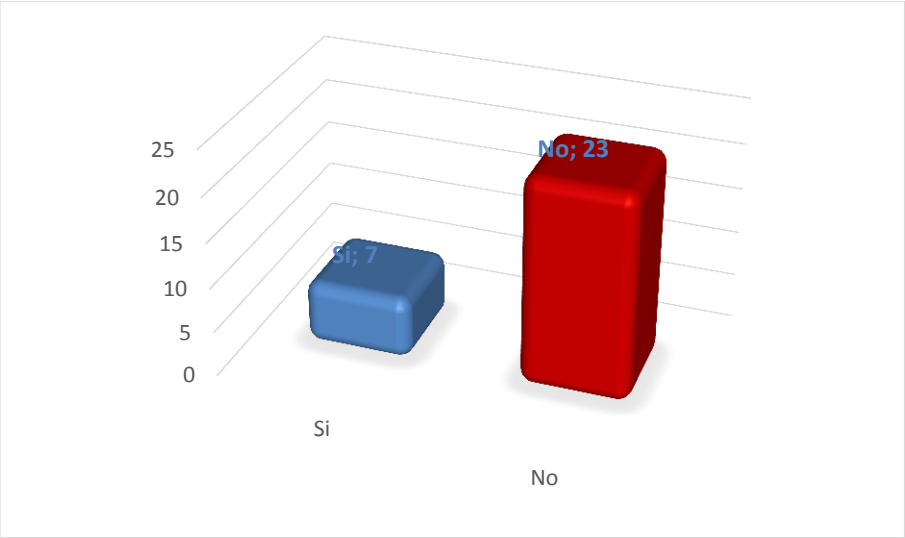


Interpretación

Según lo interpretado por los encuestados, con una mayoría considerada de 23 personas con un 83% no creen que se puedan incluir nuevos delitos informáticos dentro de la tipificación que se realiza en el Nuevo Código Procesal Penal, en cambio 7 personas con un 17% sí creen que se puede hacer.

5. ¿Pueden los fiscales y los jueces aplicar de acuerdo al Nuevo Código Procesal Penal y a las leyes complementarias adecuadamente las acusaciones y sanciones sobre los delitos informáticos?

Ítem	Frecuencia	Porcentaje
Si	7	75%
No	23	25%
Total	30	100%

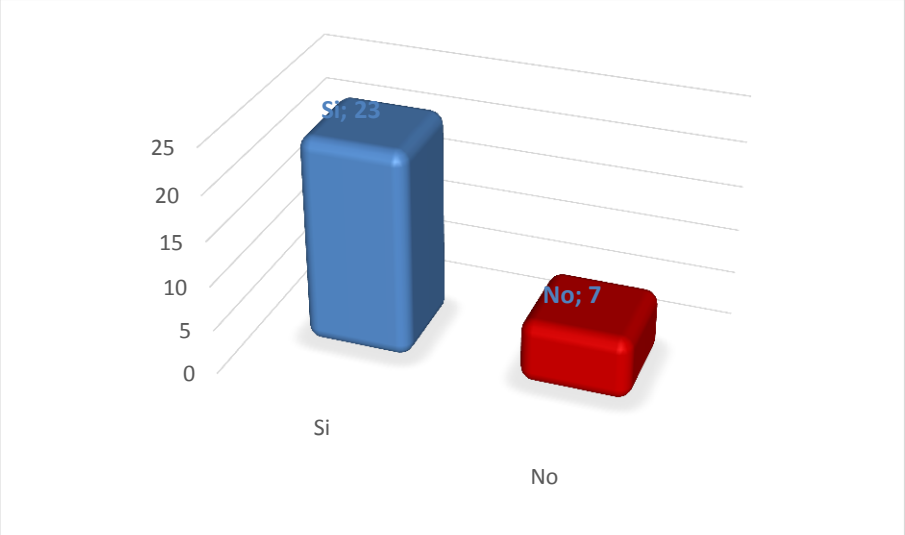


Interpretación

Del total de encuestados, con 23 personas en su mayoría y con un 75% Si creen que los fiscales y los jueces pueden aplicar de acuerdo al Nuevo Código Procesal Penal y las leyes complementarias las acusaciones y sanciones sobre los delitos informáticos, en cambio 7 personas con un 25% creen que no pueden hacerlo del todo.

6. ¿Se tiene clara la especificación y las sanciones del interceptado ilegal a las redes?

Ítem	Frecuencia	Porcentaje
Si	23	75%
No	7	25%
Total	30	100%

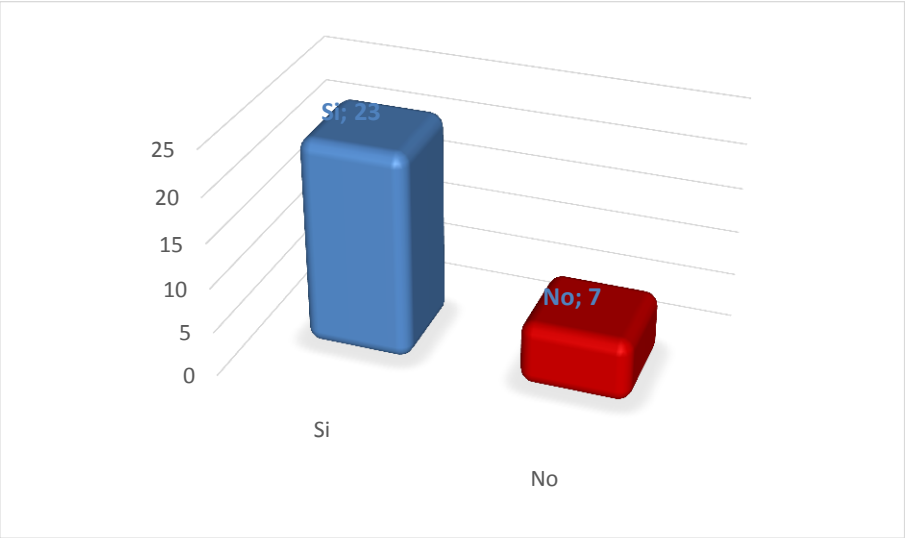


Interpretación

Del total de encuestados, en su mayoría con un 75% Si creen tener claro la especificación y las sanciones del interceptado ilegal a las redes, en cambio con un 25% manifestaron no tenerlo del todo claro.

7. ¿Se tiene clara la especificación y las sanciones de los daños ocasionados en la información?

Ítem	Frecuencia	Porcentaje
Si	23	75%
No	7	25%
Total	30	100%



Interpretación

Del total de encuestados, 23 personas en su mayoría con un 75% Si creen tener claro la especificación y las sanciones de los daños ocasionados en la información, en cambio 7 personas con un 25% manifestaron no tenerlo del todo claro.

4.2. CONTRASTACIÓN DE HIPÓTESIS

H_1 Existen acciones realizadas a través de la tecnología de la información que son considerados como delitos informáticos en el Perú

Los datos que se han expresado en la encuesta nos indica que los delitos informáticos se realizan a través de las tecnologías de la información, ya que la información a través de este medio permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.

Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el uso de la tecnología informática y comunicación. Sin embargo, estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos “pishing”, la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales, son entre otros los delitos que se presentan a menudo y que parten de acciones realizadas a través de las llamadas “tecnologías de la información”

H_2 Existen vacíos legales en el Nuevo Código Penal Peruano que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

En base a los resultados obtenidos, se concluye de que la mayoría de los encuestados indican que existen vacíos legales en el Código

Penal, por lo tanto imposibilita el trabajo adecuado que deben desempeñar tanto fiscales como jueces.

Estos vacíos se dieron en temas como: la pornografía infantil y el turismo sexual, terminales de telefonía de celulares, apología al terrorismo, elusión de medidas tecnológicas, ingreso de equipos tecnológicos a centros de reclusión, entre otros.

Todos estos delitos informáticos considerados de suma importancia, debido al reciente aumento de actividad criminal en ese rubro, que muchos especialistas consideraban habían muchas lagunas legislativas que podían incluso determinar la impunidad cuando se utilizaba instrumentos informáticos, lagunas y vacíos que se pretendieron eliminar con la promulgación de la nueva ley.

H_3 Existen vacíos legales que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

De acuerdo a la encuesta realizada, la mayoría de fiscales coincidió en la existencia de vacíos legales en la Ley 30096, ya que no se podían precisar el agravante del delito, la forma como afecta, cosa que no estaban precisadas en la referida ley, casos como la violación a la intimidad, intercepción telefónica, tráfico ilegal de datos personales, pornografía infantil, entre otras.

Por lo tanto esta ley no cumplía del todo con prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fé pública y la libertad sexual.

H_4 Existen vacíos legales en la ley Nº 30171 que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.

A pesar de los esfuerzos por creer que esta ley corregiría los vacíos encontrados en la ley 30096, del total de encuestados, coincidieron que, también existen vacíos en esta ley, ya que como se mencionó anteriormente, dado los avances tecnológicos constantes, aparecerán modalidades nuevas conforme evoluciona las tecnologías de información, por ende tipificar estos nuevos delitos, siempre será motivo de hacer las respectivas modificaciones a la ley vigente.

CAPÍTULO V
DISCUSIÓN DE RESULTADOS

5.1 ANÁLISIS DE LOS RESULTADOS

De acuerdo con la contrastación de los resultados se establece que existe vacíos legales en las leyes 30096 y 30171, donde se evidencia sus deficiencias, y por más que se plantearon diversas modificaciones a la ley, adecuándolo al documento internacional que se creó antes del Convenio de Budapest. Se buscó adaptar nuestra norma contra los delitos informáticos a los estándares que la comunidad europea exige para poder ser parte del Convenio.

Todo esto en respuesta a la preocupación por los vacíos encontrados en las leyes, dada las claras imprecisiones que contenía, que eventualmente podrían vulnerar derechos incluso de los mismos usuarios a los que se pretende proteger. Por ello, se puede decir que las modificaciones establecidas por la ley 30171 generaron un después a la norma sobre delitos informáticos; debido a que los mismos en esencia recogen la estructura o los llamados puntos mínimos regulatorios que el Convenio de Budapest advierte.

No existía una delimitación precisa de la responsabilidad penal para algunos casos, como por ejemplo: la autorevisión de los sistemas informativos, la copia de base de datos por la misma persona a la que le pertenece dicha información, el ingreso al sistema informático con autorización del dueño; hechos que debieron exceptuados como delitos, pero que la ley primigenia de delitos informáticos al ser ambigua no lo permitía.

El conocimiento por parte de los fiscales de la provincia de Huara, nos da indicios de lo compleja de la situación, de la preparación y la información que manejan para aplicar las leyes, del criterio y los

fundamentos que se considera a la hora de dictaminar que pena corresponde o no para un delito informático.

En la mayoría de sus afirmaciones, aún creen que la los términos de “tecnologías de la información y comunicación” es el punto de partida para la tipificación de los delitos informáticos. Esta serie de ambigüedades en las leyes solo generan confusión e incertidumbre al no saber qué medidas aplicar, dado que los casos que se presentan en cuestión de delitos informáticos, van evolucionando según las nuevas tecnologías, por ende insta a que siempre se tengan que realizar modificaciones en las leyes.

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

CONCLUSIONES

- Dada la naturaleza virtual de los delitos informáticos, estos se pueden volver confusos en su tipificación, ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área

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

- Nuevas modalidades de negocios por internet, como el comercio electrónico es un claro ejemplo de cómo los delitos pueden aparecer de diversas formas, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

- Los delitos informáticos no deben impedir que el usuario se prive de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

RECOMENDACIONES

- Si bien las leyes se han promulgado con la finalidad de combatir los delitos informáticos, se debe entender que los sistemas y datos informáticos siempre serán vulnerables ante cualquier tipo de tecnología, por lo mismo, por lo tanto se deben crear nuevos métodos para protegerse utilizando la propia tecnología para ello. En el campo del derecho, el hecho de autoinfringir nuestro sistema o datos informáticos (como se entendía con la ley de delitos informáticos antes de ser modificada) ya sea realizando pruebas a los sistemas y datos informáticos o solo porque así se deseara implicaba incurrir en delito. Pues este era un grave problema de la norma primigenia, es por ello que era evidente que la modificación a ley 30096 debía permitir eliminar esa incertidumbre que existía para establecer una exención a la responsabilidad penal para los casos que donde uno mismo desee traspasar la medida de seguridad que contengan los datos o sistemas informáticos sin incurrir en delito por ello.

- A pesar de las observaciones que se han hecho a las leyes, no se dan cuenta de que ya existen casos, informes o jurisprudencia de los problemas que ha tenido para aplicarse o se sustente la necesidad de más modificaciones. La lucha contra la delincuencia informática está condenada a fracasar si es que las leyes se siguen escribiendo de espaldas a la evidencia empírica y a las necesidades de los jueces y fiscales que están llamados a aplicarla.

- Se deben impulsar los canales de comunicación y diálogo con nuestras autoridades políticas pues esto permitirá enriquecer la lucha contra este nuevo fenómeno delictivo mundial y evitar que los cambios normativos se realicen a puerta cerrada y sin la participación u opinión ciudadana. Es necesario emprenderla ya, para ejercer libremente nuestros derechos y exhortar que se respeten nuestras garantías.

REFERENCIAS BIBLIOGRÁFICAS

CALDERON, L. (2010). "*Delitos informáticos y Derecho penal*", Ubijus, México.

BRAMONT, L. (2000). "*Delitos informáticos*", enRevista Peruanade Derecho de la Empresa, Derecho InformaticoyTeleinformaticaJuridica, Nº 51, Asesorandina. Lima.

CAMACHO, L (1997). "*El delito informático*" Graficas Condor, Madrid.

DÍAZ, A., (2010). «*El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*, Redur8,Rioja.

DURAND(2002) "*Los delitos informáticos en el Código Penal Peruano*" enRevista Peruana de Ciencias Penales. N° 11, Lima.

MORANT(2003), J; "*protección penal de la intimidad frente a las nuevastecnologías*", Ed. Practica de Derecho, Valencia, 2003.

MORON, E. (2002). "*Internet y Derecho Penal: hacking y otras conductas ilícitas en la red"*, Ed. Aranzadi, 2° ed., Navarra, 2002,

ORTS (2001). "*Delitos informáticos ydelitos comunes cometidos a través de la informática"*, Tirant Lo Blanch, Valencia.

VILLAVICENCIO, F. (2013), "*Derecho Penal- Parte general*", 4 reemp.,Grijley, Lima,

CUESTIONARIO DE INVESTIGACIÓN

Sr. Juez/Fiscal del Distrito Judicial de Huaura.

El presente cuestionario responde a la investigación **VACÍOS LEGALES QUE IMPOSIBILITAN LA SANCIÓN DE LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL PERUANO-2015.**, forma parte de nuestra Tesis de Licenciatura, le agradecemos su participación en la encuesta, y le rogamos que sus respuestas sean las más adecuadas al problema de investigación. Le aseguramos el total anonimato de su persona en la investigación, por ser uno de los principios éticos que rigen la investigación científica.

1.1 DATOS GENERALES

1.1 Cargo que ocupa en el Poder Judicial y/o ministerio Público

a) Juez. b) Fiscal

1.2 Tiempo de ejercicio del cargo

a) 0-2 años b) 2-4 años c) 4-6 años d) Más de 6 años

1.2 PREGUNTAS

1. ¿Existen los suficientes alcances en el Nuevo Código Procesal Penal para sancionar los delitos informáticos?

2. ¿Existen en las leyes complementarias del Nuevo Código Procesal Penal los alcances suficientes para sancionar los delitos informáticos?

3. ¿Están tipificados adecuadamente los delitos informáticos en el Nuevo Código Procesal Penal?

4. ¿Se pueden incluir los nuevos delitos informáticos dentro de la tipificación que se realiza en el Nuevo Código Procesal Penal?

5. ¿Pueden los fiscales y los jueces aplicar de acuerdo al Nuevo Código Procesal Penal y a las leyes complementarias adecuadamente las acusaciones y sanciones sobre los delitos informáticos?

6. ¿Se tiene clara la especificación y las sanciones del interceptado ilegal a las redes?

7. ¿Se tiene clara la especificación y las sanciones de los daños ocasionados en la información?

ANEXO

MATRIZ DE CONSISTENCIA

VACÍOS LEGALES QUE IMPOSIBILITAN LA SANCIÓN DE LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL PERUANO-2015

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES
¿Qué vacíos legales en el Nuevo Código Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015?	**Objetivo general.** Determinar qué vacíos legales en el Nuevo Código Penal Peruano y en sus leyes complementarias imposibilitan la sanción de los delitos informáticos en el Perú el 2015. **Objetivos específicos.** Identificar qué acciones ilegales realizadas a través de la tecnología de la información	**Hipótesis general.** Existen vacíos legales en el Nuevo Código Penal Peruano y en sus leyes complementarias que imposibilitan la sanción de los delitos informáticos en el Perú el 2015. **Hipótesis específicas.** Existen acciones ilegales realizadas a través de la tecnología de la información que son considerados como delitos	Delito informático	Falsificación de documentos Falsedad ideológica Omisión de declaración que debe constar en el documento Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos Delito contra los derechos de autor de software Delitos contra los derechos de autor en general

	son considerados como delitos informáticos en el Perú. Identificar qué acciones ilegales realizadas a través de la tecnología de la información no son considerados como delitos informáticos en el Perú Determinar cuáles son los alcances del Nuevo Código Procesal Penal Peruano y sus leyes complementarias para sancionar los delitos informáticos en el Perú Identificar qué vacios legales en el Nuevo Código Procesal Penal Peruano imposibilitan la sanción de los delitos informáticos en el Perú el 2015.	informáticos en el Perú. Existen acciones ilegales realizadas a través de la tecnología de la información que no son considerados como delitos informáticos en el Perú Existen alcances en el Nuevo Código Procesal Penal Peruano y en sus leyes complementarias para sancionar los delitos informáticos en el Perú Existen vacios legales en el Nuevo Código Procesal Penal Peruano que imposibilitan la sanción de los delitos informáticos en el Perú el 2015. Existen vacíos legales en la ley Nº 30096 que imposibilitan la sanción de los delitos	Vacío legal	Mala redacción Artículos estipulados en las leyes con definiciones ambiguas. Incompetencia del legislador No corresponde a la realidad que se pretende regular

	Identificar qué vacios legales en la ley Nº 30096 imposibilitan la sanción de los delitos informáticos en el Perú el 2015. Identificar qué vacios legales en la ley Nº 30171 imposibilitan la sanción de los delitos informáticos en el Perú el 2015	informáticos en el Perú el 2015. Existen vacíos legales en la ley Nº 30171 que imposibilitan la sanción de los delitos informáticos en el Perú el 2015.		