022

UAP UNIVERSIDAD ALAS PERUANAS

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

Escuela Académico Profesional de Derecho

TESIS

"IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ.2017"

PRESENTADA POR:

Br. HUARMI ALBERCA VELASCO

ASESORES:

Dr. LUIS WIGBERTO FERNANDEZ TORRES (ASESOR TEMÁTICO)

Dr. EDWIN BARRIOS VALER (ASESOR METODOLÓGICO)

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

LIMA, PERÚ

2017

UNIVERSIDAD ALAS PERUANAS

FACULTAD DE DERECHO Y CIENCIA POLITICA

ESCUELA PROFESIONAL DE DERECHO

DICTAMEN DE EXPEDITO DE TESIS N° 022 -T-2018-OIYPS-FDYCP-UAP

Visto, el Oficio N° 048-2018-OGYT-FDYCP-UAP, de fecha 22.02.2018 de la Oficina de Grados y Títulos, en el que se solicita la revisión final de trabajo de Investigación presentado por el/la bachiller **HUARMI ALBERCA VELASCO** a fin que se declare expedito para sustentar la tesis titulada "**IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS, PERU 2017**"

CONSIDERANDO

Que, el Reglamento de Grados y Títulos aprobado por Resolución Rectoral N° 15949-2015.R-UAP de fecha 28.12.2015, contempla las disposiciones normativas correspondientes a las funciones de las Oficinas de Investigación, el mismo que concuerda con lo dispuesto por el Reglamento de Investigación e Innovación Tecnológica aprobado por Resolución Rectoral N° 17483-2017-R-UAP de fecha 15.12.2016.

Que, de la revisión de la tesis, se aprecia que esta cuenta con el informe de el/la asesor/a metodólogo Dr. Edwin Barrios Valer de fecha 19 de febrero de 2018 y el informe de el/la asesor/a temático Dr. Luis Wigberto Fernández Torres de fecha 20 de febrero de 2018, informes que señalan que la tesis ha sido desarrollada conforme a las exigencias requeridas para el trabajo de investigación correspondiente al aspecto temático y procedimiento metodológico.

DICTAMEN

Atendiendo a estas consideraciones y al pedido de el/la bachiller **HUARMI ALBERCA VELASCO** esta Jefatura **DECLARA EXPEDITA LA TESIS**; titulada "**IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART.9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MJOR CONDUCTA DELITIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS, PERU 2017**"Debiendo el/la interesado/a continuar y cumplir con el proceso y procedimiento para que se le programe el examen oral de sustentación de Tesis.

La Victoria, 02 de Marzo de 2018

UAP UNIVERSIDAD ALAS PERUANAS
FACULTAD DE DERECHO Y CIENCIA POLITICA
ESCUELA PROFESIONAL DE DERECHO

Dra. FELIPA ELVIRA MUÑOZ ECURO
Jefa de Investigación y Proyección Social

FEMC/hsm

INFORME N° 003-EBV-T-2018

AL : **Dr. Ricardo Alfredo Díaz Bazán PhD**
Decano de la Facultad de Derecho y Ciencia Política

DE : **Dr. Edwin Barrios Valer**
Docente Asesor
Código N° 022715

REFERENCIA: Memorándum N° 0137– 2017 – OGYT- FDYCP - UAP

ASUNTO : Asesoría metodológica: Tesis

BACHILLER : HUARMI ALBERCA VELASCO
Título: "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ - 2017"

FECHA : 19 de febrero de 2018.

Tengo el agrado de dirigirme a Usted, con relación a la referencia, a fin de hacer de vuestro conocimiento el presente informe, la evaluación de los aspectos de forma y fondo, a la tesis del Br. HUARMI ALBERCA VELASCO:

1. DE LOS ASPECTOS DE FORMA

Se ha considerado la **Resolución Vicerrectoral N° 2342-2013-VIPG-UAP**, que regula la estructura del proyecto de Tesis, la estructura de la Tesis, y que hace referencia a las **normas APA.**

2. DE LOS ASPECTOS DE FONDO

TÍTULO DEL TRABAJO DE INVESTIGACIÓN

Con relación al título del tema de investigación: "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ - 2017" consideramos, que cumple con los requisitos para un trabajo de investigación a nivel de pregrado de la Facultad de Derecho de la Universidad Alas Peruanas.

DEL CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

Con referencia a este punto, metodológicamente consideramos trascendental, ya que de éste se deriva todo el desarrollo del trabajo de investigación, en consecuencia describimos los puntos más resaltantes:

- Descripción de la realidad problemática, este acápite del trabajo de investigación cuenta con los requisitos y naturaleza de un estudio coherente, el mismo que obedece a los métodos deductivo e inductivo.
- Delimitación de la Investigación, se hizo de acuerdo a los parámetros de la Universidad Alas Peruanas, tomando en cuenta la delimitación espacial, temporal, social y conceptual.
- Problemas de la Investigación, respecto a este punto neurálgico, el Bachiller: HUARMI ALBERCA VELASCO, ha desarrollado tanto el problema general como los problemas específicos, de acuerdo a una adecuada operacionalización de las variables: tipificación de conducta delictiva y suplantación de identidad en los delitos informáticos.
- Objetivos de la investigación, se observa un planteamiento adecuado de los mismos, tanto del objetivo general, como de los específicos, además fueron redactados con verbos en infinitivo, tal como advierte la teoría.
- Hipótesis y variables de la investigación, existe un planteamiento adecuado de las mismas, obedeciendo a la formulación del problema.
- Metodología de la investigación, expresa un planteamiento metodológico adecuado de acuerdo a los parámetros de la Universidad Alas Peruanas.
- Justificación e importancia de la investigación, referente a este punto, el tesista considera su justificación de acuerdo a los criterios establecidos por la teoría de la investigación científica.

EL CAPÍTULO II: MARCO TEÓRICO

- Todo el contenido del Marco Teórico se ha desarrollado, tomando en cuenta el sistema de referencias bibliográficas APA, en sexta edición y los contenidos se adecúan a los requisitos de un trabajo de investigación en el campo del derecho, de ahí su importancia al estar constituido por las teorías que dilucidan los aspectos fundamentales del estudio jurídico social.

DEL CAPÍTULO III: PRESENTACÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Este capítulo representa un punto neurálgico en la realización de un trabajo de investigación, en tal sentido está constituido por los siguientes puntos:

- Análisis de Tablas y Gráficos, cumple con los requisitos de la universidad.
- Discusión de Resultados, desarrolló de acuerdo a las exigencias de un trabajo de investigación de nivel universitario.
- Conclusiones: guardan relación directa con los objetivos de investigación.
- Recomendaciones, guardan relación directa con las conclusiones.
- Fuentes de información, fueron desarrolladas, tomando en cuenta el sistema de referencias bibliográficas APA, en sexta edición

ANEXOS

Matriz de Consistencia, se observa en los anexos.

Instrumento(s), se observan en los anexos

Validación de instrumento por expertos (Ficha de validación del instrumento. Juicio de expertos), se observan en los anexos.

Anteproyecto de Ley.

CONCLUSIÓN:

Por lo expuesto, habiéndose cumplido con las sesiones de asesoramiento correspondiente al **Aspecto Metodológico de la tesis titulada:** "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ - 2017" considero que el Bachiller **HUARMI ALBERCA VELASCO** ha realizado **la tesis** conforme a las exigencias establecidas por la Facultad, para su preparación y elaboración; el mismo que está concluido y listo para ser sustentada.

Atentamente,

Dr. EDWIN BARRIOS VALER
Asesor Metodológico
Código N° 022715

INFORME N° 01-2018[1]-T[2]-2017

AL : **Dr. Ricardo Alfredo Díaz Bazán Ph. d**
Decano de la Facultad de Derecho y Ciencia Política

DE : **Dr. Luis Wigberto Fernández Torres**
Docente Asesor
Código N° 051666

REFERENCIA: Memorándum No. 0137-2017-OGYT-FDYCP-UAP

ASUNTO : **Asesoría temática:** Tesis

BACHILLER : HUARMI ALBERCA VELASCO

TÍTULO: "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS, PERU. 2017"

FECHA : 20 de febrero de 2018

Tengo el agrado de dirigirme a Usted, con relación a la referencia, a fin de hacer de vuestro conocimiento el presente informe, la evaluación de los aspectos de forma y fondo:

1. **DE LOS ASPECTOS DE FORMA**

   Se ha considerado la **Resolución Vicerrectoral N° 2342-2013-VIPG-UAP**, que regula la estructura del proyecto de Tesis, la estructura de la Tesis, y que hace referencia a las **normas del APA.**

2. **DE LOS ASPECTOS DE FONDO**

   TÍTULO DEL TRABAJO DE INVESTIGACIÓN

   Con relación al título del tema de investigación consideramos "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS, PERU. 2017".

   DEL CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

   – **Descripción de la realidad problemática[3]**

   El desarrollo desmedido de las nuevas tecnologías en el área informática han aparecido diversas conducta ilícitas virtuales y que se han generado en un problema de inseguridad jurídica en cuanto a la

---

[1] Sigla de los nombres y apellidos del docente asesor.
[2] Tesis.
[3] Es necesario argumentar cada aspecto del trabajo de investigación desarrollado por el bachiller, toda vez que es publicado en el Repositorio Institucional, incluyendo los informes de los asesores.

informática a nivel mundial, así como en el Perú, los cuales no son ajenos a este tipo de problemática, es necesario señalar que la falta de regulación jurídica en los delitos informáticos acarrean la criminalidad informática, debiéndose entender a ésta como los actos que vulneran la ley vigente, es decir que nuestra legislación hace referencia solo algunos tipos de delitos establecidos en el Código Penal vigente y se describe de una manera muy general, ocasionando así diversos vacíos legales, es así que debe señalarse las sanciones imponibles de acuerdo a la gravedad de la comisión del delito.

–Justificación e importancia de la investigación

La presente investigación se justifica desde el punto de vista teórico, porque a través de ésta, se determinó la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, en consecuencia servirá como antecedente teórico para trabajos académicos, beneficiando a la sociedad piurana en principio y posteriormente a la sociedad peruana, ya que el problema de investigación afecta a todos y está vigente hoy más que nunca, asimismo, se ha desarrollado considerando las pautas metodológicas, desde la identificación del tema, la búsqueda de fuentes de información, la matriz de consistencia, el plan de tesis, considerando el diseño metodológico de enfoque cuantitativo.

EL CAPÍTULO II: MARCO TEÓRICO

–Antecedente de la Investigación

La investigación ha buscado antecedentes internacionales:

- Investigación denominado "Delitos Informáticos en Latinoamérica – 2012, del litoral, Santa Fe – Argentina, Temperini, 2012.
- Investigación titulado: "Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador", de la Escuela Superior Politécnica del litoral en la Ciudad de Guayaquil, 2009.
- Tesis titulada: "Delitos emergentes en internet y el desafío de carabineros de Chile en la prevención y control en la era informática", de Toledo Dumenes, José Alfonso, en el 2006.

–Bases Teóricas

Las bases teóricas han descansado en la descripción de dos términos fundamentales: Tecnología de la Información y Sociedad de la Información, explicando los antecedentes necesarios e identificadores del Derecho Informático, ya que ambos conceptos son los que le otorgan un objeto de estudio propio, el cual requiere una metodología especifica con categorías conceptuales propias y cuyan fuentes tienen particularidades originadas en el vertiginoso cambio inherente al ámbito tecnológico.

–Bases Legales

- Constitución Política del Perú,
- Ley No. 27309 sobre delitos informáticos,

- Código Penal,
- Ley No. 28493 sobre la regulación del uso del correo electrónico comercial no solicitado,
- Ley No. 27291 sobre la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- Ley No. 30096 sobre los delitos informáticos.

–Definición de Términos Básicos

Se ha realizado de manera apropiada y acorde con el fondo de la investigación.

DEL CAPÍTULO III: PRESENTACÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

–Discusión de Resultados

La investigación ha realizado el análisis estadístico de carácter No experimental Correlacional entre mediante un tipo de investigación básica, en donde se corroboran las afirmaciones del autor en el sentido que se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017, tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,868,lo que indica que existe una correlación positiva alta entre las variables.

–Conclusiones

La tesis materia de informe, luego de haber realizado la contrastación necesaria de las fuentes en que se basa, así como en el trabajo de campo realizado, concluye que existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

–Recomendaciones

La tesis materia de informe, recomienda:

- La modificatoria de la Ley No.30096 (Ley de delitos informáticos), en lo referente a suplantación de identidad (Anteproyecto de Ley que propone la modificatoria del artículo 9 de la Ley No.30096.
- Al poder Judicial implementar talleres de aprendizaje sobre la tipificación y desarrollo de delitos informáticos.
- Al Ministerio Público implementar talleres de aprendizaje sobre la tipificación y desarrollo de delitos informáticos.

- A la Policía Nacional organizar eventos que busquen la utilización de las tecnologías adecuadas para una mejor tipificación de los delitos virtuales.

–Fuentes de información

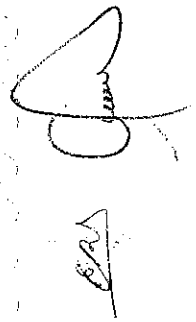
El tesista ha recurrido a 18 fuentes de información tanto nacional como extranjera, la cual se considera está relacionada directamente con el tema materia de su investigación.

CONCLUSIÓN

Por lo expuesto, habiéndose cumplido con las sesiones de asesoramiento correspondiente al **aspecto temático,** considero que el bachiller **HUARMI ALBERCA VELASCO** ha realizado **la tesis** conforme exigencias establecidas por la Facultad, para su preparación y elaboración; el mismo que está concluido y listo para ser sustentado.

Atentamente,

Dr. Luis Wigberto Fernández Torres
Docente de la FDyCP
Universidad "Alas Peruanas"



Dedicatoria

A mis padres por su apoyo incondicional para lograr mi desarrollo profesional, y cada uno de sus concejos y motivación para ser cada día mejor persona.

Huarmi.

Agradecimientos

Mis sinceros agradecimientos:

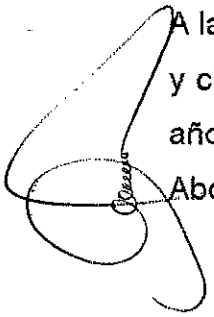
A mis padres por su apoyo incondicional para el logro de mis objetivos profesionales.

A mi alma mater la "Universidad Alas Peruanas", Facultad de Derecho y Ciencia Politica, por la valiosa experiencia que tuve en sus aulas.

A mis maestros, en especial a mis asesores, por ayudarme a completar el proceso de análisis, revisión y corrección del tema de investigación, interés, preocupación, profesionalismo y apoyo para la culminación del presente trabajo y por el tiempo que dedicaron a esta investigación.

El autor.

Reconocimiento



A la Universidad Alas Peruanas, a los docentes de la facultad de derecho y ciencia política, por todo el apoyo académico que se me brindó en los años de formación profesional, hacia el logro de alcanzar el título de Abogado.

El autor.

Índice

CAPÍTULO II: MARCO TEÓRICO

CAPÍTULO III:

PRESENTACIÓN, ANÁLISIS E INTERPRETACIÓN DE ESULTADOS

ANEXOS:

Resumen

La presente investigación denominada "Importancia de proponer modificaciones normativas a fin de tipificar una mejor conducta delictiva en materia de suplantación de identidad en los delitos informáticos, Perú 2017", busca: Determinar la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

El estudio de investigación se realizó bajo el enfoque cuantitativo, referente al tipo de investigación pertenece a la investigación básica, respecto al nivel corresponde al nivel correlacional, en cuanto al diseño de investigación corresponde al diseño no experimental, transversal, correlacional, con referencia a la técnica de investigación, se eligió la encuesta y como instrumentos, dos cuestionarios (sobre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos), respecto a la población estuvo constituida por 424 estudiantes de la Universidad Alas Peruanas de Piura, matriculados en el año 2017 y la muestra es no probabilística intencionada, a criterio del investigador, 72 estudiantes de la Universidad Alas Peruanas de Piura.

Al culminar la presente investigación se arribó a la siguiente conclusión: Se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017, tal como se corrobora, a través del estadígrafo de la Rho de Spearman igual a 0,868, lo que significa que existe una correlación positiva alta entre las variables en estudio.

Palabras claves: tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, facilidad de acceso a las redes sociales, falta de control en las redes sociales, elementos de prueba digital.

Abstract

The present investigation called "Importance of proposing normative modifications in order to typify a better criminal behavior in the matter of identity theft in computer crimes, Peru 2017", seeks to: Determine the relationship that exists between the typification of criminal behavior and the impersonation of identity in computer crimes, Piura 2017.

The research study was conducted under the quantitative approach, referring to the type of research belongs to basic research, with respect to the level corresponds to the correlational level, in terms of research design corresponds to the non-experimental, cross-sectional, correlational design, with reference to the research technique, the survey was chosen and as instruments, two questionnaires (on the typification of criminal behavior and identity theft in cybercrime), with respect to the population consisted of 424 students from Alas Peruanas University of Piura, enrolled in 2017 and the sample is intentionally non-probabilistic, at the researcher's discretion, 72 students from the Alas Peruanas University of Piura.

At the end of the present investigation, the following conclusion was reached: It was determined that there is a significant relationship between the typification of criminal behavior and identity theft in computer crimes, Piura 2017, as corroborated, through the statistic of the Rho of Spearman equal to 0.868, which means that there is a high positive correlation between the variables under study.

Keywords: typification of criminal behavior and identity theft in computer crimes, ease of access to social networks, lack of control in social networks, digital evidence.

Introducción

La evolución tecnológica de nuestro mundo moderno está transformándose de una manera ilimitada en el ciberespacio con una enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones las cuales conllevan a la importancia que tiene su progreso para el desarrollo de un país; Las transacciones comerciales y financieras, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

La presente investigación que tiene como título "Importancia de proponer modificaciones normativas a fin de tipificar una mejor conducta delictiva en materia de suplantación de identidad en los delitos informáticos, Perú 2017", trata sobre la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017, al ser un problema latente en nuestra sociedad y sobre todo con el incremento notorio de los delitos de este tipo, todo ello se puede evidenciar a nivel nacional y también se refleja en la ciudad de Piura, que se constituye en el escenario de desarrollo de la presente tesis.

La presente tesis está constituida por tres capítulos, los que se describen a continuación:

En el Primer capítulo se presenta la descripción de la realidad problemática relacionada con la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, además de la delimitación de la Investigación con aspectos relacionados a las delimitaciones de la investigación, empezando por la delimitación espacial, delimitación social, delimitación temporal y delimitación conceptual, seguidamente se realiza el planteamiento del problema, describiendo también el problema de investigación principales y secundarios y estableciendo los objetivos de investigación; el objetivo general y los objetivos específicos, planteando la hipótesis general y secundarias y variables de la investigación, abordando la hipótesis y variables, donde se expone la formulación de la hipótesis general y secundarias, identificándose las variables de estudios, estableciendo la operacionalización de las variables del tema de

investigación, describiremos el tipo y nivel de la investigación, se presenta la metodología de la investigación, desarrollaremos el diseño, el tipo y nivel de la investigación el método y diseño de la investigación, la población y muestra estudiada, señalamos también las técnicas e instrumentos de recolección de datos y finalmente, indicamos los criterios de validez y el criterio de confiabilidad de los instrumentos a través de la prueba de confiabilidad, posteriormente señalaremos la justificación, importancia y las limitaciones de la investigación.

El Segundo capítulo contiene el marco teórico, en el que se desarrollan los antecedentes de la investigación vinculados a los problemas sociales y jurídicos relacionados a la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, las bases teóricas sustentan cada una de las variables, desarrollando también las bases legales que regulan el problema de investigación y finalmente la definición de términos básicos.

En el Tercer capítulo se desarrolla la presentación, análisis e interpretación de resultados, se esboza la presentación del estudio de campo realizado a los sujetos informantes (estudiantes de la Universidad Alas Peruanas de Piura) con sus respectivos análisis de datos, realizando también el análisis de tablas y gráficos, posteriormente se ubican las conclusiones y recomendaciones a las que arriba la investigación, además las fuentes de información, referencias bibliográficas y los respectivos anexos considerados.

El autor.

CAPÍTULO I:

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

Desde el desarrollo desmedido de las nuevas tecnologías en el área informática han aparecido diversas conductas ilícitas virtuales y que se han generado en un problema de inseguridad jurídica en cuanto a la informática a nivel mundial así como en nuestro país Perú, no somos ajenos a este tipo de problemática, es necesario señalar que la falta de regulación jurídica en los delitos informáticos acarrean la criminalidad informática, debiéndose entender a ésta como los actos que vulneran la ley vigente, es decir que nuestra legislación hace referencia solo algunos tipos de delitos establecidos en el código penal vigente y se describen de una manera muy general ocasionando así diversos vacíos legales es así que debe señalarse las sanciones imponibles de acuerdo a la gravedad de la comisión del delito, por lo que es necesario tener el marco conceptual claro para poder tipificarlo, lo que resulta cuestionable es que tenemos que asumir y estar preparados para enfrentarnos en algún momento la posibilidad de ser víctimas de un delito informático dado el creciente aumento en nuestros días de este tipo de ilícitos penales en donde inclusive el autor lo realiza incluso sin ánimo de lucro sino por el contrario por mera inquietud de juego.

Las actividades criminales que se configuran en las distintas modalidades de delitos informáticos existentes, ha llevado a que la legislación en el Perú estén encuadrarlas solo en figuras típicas tradicionales, tales como el robo, el hurto, los fraudes, las falsificaciones, las estafas, los sabotajes, los cuales en la actualidad la institución encargada de ver este tipo de ilícitos es la División de Investigación de Delitos de Alta Tecnología, Sin embargo, dado el uso de las técnicas informáticas y la peculiaridad del delito informático ahí la necesidad de crear una ley especial que regule este tipo de delitos de manera específica, sin embargo nuestra carrera profesional nos empuja a que podamos estar con todas las herramientas jurídicas para poder contrarrestar este flagelo que se viene dando en nuestro país.

El aumento del nivel de los delitos informáticos es alarmante, no solo a nivel local sino a nivel mundial con la diferencia que diversos países ya han optado diversas medidas legales para sancionar estos actos ilícitos como la creación de leyes especiales y que nuestro país aún solo se encuentra de manera general tal es así la criminalidad informática representa una amenaza para el desarrollo económico del país y también para la sociedad en su conjunto, situación que cada día toma mayor importancia con la especialidad que han adoptado algunas empresas para proteger y vigilar la competencia, es así que se dan las copias ilegales de software y espionajes informáticos, pornografía infantil, infracción a los derechos de autor entre otros, tal es así que el bien jurídico protegido viene a ser la Información ya que está en las persona puede presentar un valor económico o intrínseco por su fluidez y trafico jurídico.

La situación jurídica peruana en la descripción de este problema no garantiza la seguridad legal en la informática jurídica es por eso que existe la gran necesidad de poder alcanzar una propuesta para la creación de una ley especial que regule los delitos informáticos de manera específica.

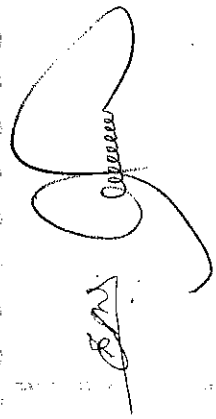
1.2 Delimitación de la Investigación

1.2.1 Delimitación Espacial

La Investigación se ha realizado en las instalaciones de la Universidad Alas Peruanas de Piura.

1.2.2 Delimitación Social

El estudio de investigación abarcó en primera instancia a los estudiantes de la Universidad Alas Peruanas de Piura, de la facultad de derecho y Ciencia Política.



1.2.3 Delimitación Temporal

El periodo que comprende la presente investigación es el año 2017.

1.2.4 Delimitación Conceptual:

Para el desarrollo del trabajo se ha considerado pertinente desarrollar aspectos tales como: "Derecho Informático, Los delitos Informáticos, Sabotaje Informático, Espionaje Informático, Fraude mediante computadoras, Phishing o pesca de claves secretas, Infracción a los derechos de autor, Uso ilegitimo de sistemas informáticos ajenos, Delitos informáticos contra la privacidad, Pornografía infantil".

1.3 Problema de Investigación

1.3.1 Problema General

¿Qué relación existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017?

1.3.2 Problemas Específicos

a) ¿Qué relación existe entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017?

b) ¿Qué relación existe entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017?

c) ¿Qué relación existe entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017?

1.4 Objetivo de la Investigación

1.4.1 Objetivo General

Determinar la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

1.4.2 Objetivos Específicos

a) Determinar la relación que existe entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017.

b) Determinar la relación que existe entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017.

c) Determinar la relación que existe entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017..

1.5 Hipótesis y Variables de la Investigación

1.5.1 Hipótesis General

Existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

1.5.2 Hipótesis Específicos

a) Existe una relación significativa entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017.

b) Existe una relación significativa entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017.

c) Existe una relación significativa entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017.

1.5.3 Variables:

Variable "1": Tipificación de conducta delictiva

La tipicidad es la adecuación, o encaje del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley como delito. Si la adecuación no es completa no hay delito. La tipicidad es la adecuación, el encaje, la subsunción del acto humano voluntario al tipo penal. La tipicidad lo aplica el juez, la tipificación lo realiza el legislador, la calificación de un comportamiento como delito lo hace el

fiscal. La tipificación es la criminalización de una norma de cultura realizada por el legislador y establecida en una ley penal. (Goldstein, 2001).

Variable "2": Suplantación de identidad en los delitos informáticos

La suplantación de identidad en los delitos informáticos consiste en: El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (Congreso de la República, 2013).

1.5.3.1 Operacionalización de las Variables

Variable	Definición conceptual	Definición operacional	Dimensiones	Escala
Variable 1: Tipificación de conducta delictiva	La tipicidad es la adecuación, o encaje del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley como delito. Si la adecuación no es completa no hay delito. La tipicidad es la adecuación, el encaje, la subsunción del acto humano voluntario al tipo penal. La tipicidad lo aplica el juez, la tipificación lo realiza el legislador, la calificación de un comportamiento como delito lo hace el fiscal. La tipificación es la criminalización de una norma de cultura realizada por el legislador y establecida en una ley penal. (Goldstein, 2001).	La tipificación de conducta delictiva, consiste en los procedimientos diversos para establecer los criterios objetivos para poder delimitar una conducta antijurídica y punible desde todo punto de vista.	✓ Antijuridicidad ✓ Gravedad de los hechos. ✓ Valoración de la prueba	Nominal Nominal Nominal
Variable 2: Suplantación de identidad en los delitos informáticos	La suplantación de identidad en los delitos informáticos consiste en: El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (Congreso de la República, 2013).	La suplantación de identidad en los delitos informáticos, consiste en las actividades mediante las cuales una persona se hace pasar por otra y en el campo cibernético o virtual resulta común.	✓ Facilidad de acceso a las redes sociales. ✓ Falta de control en las redes sociales. ✓ Elementos de prueba digital	Nominal Nominal Nominal

1.6 Metodología de la Investigación

1.6.1 Tipo y Nivel de la investigación

a) Tipo de Investigación

El tipo de investigación que corresponde al presente trabajo de investigación por sus características es la investigación básica porque la intención del estudio es el aporte teórico y la caracterización jurídica conceptual de las variables: tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos.

b) Nivel de Investigación

El nivel de investigación asumido es el correlacional, porque el objetivo de la investigación es el de determinar la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos en la ciudad de Piura durante el periodo 2017.

1.6.2 Método y Diseño de la Investigación

a) Método de la investigación

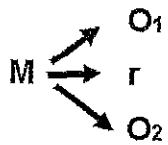
La presente tesis, respecto al método de investigación, por sus características, corresponde a los métodos lógicos (Deductivo – Inductivo) como los métodos empíricos (Observación) cabe mencionar que para el tratamiento y procesamiento de la información se recurrió a los métodos analítico y sintético, a través de la estadística, tanto descriptiva como inferencial.

b) Diseño de la Investigación

El diseño de investigación es No experimental porque se acopió datos sin tratar de introducir tratamientos nuevos ni cambios; se hacen observaciones o mediciones acerca de estados, circunstancias, conductas características existentes, se observa los fenómenos en su ambiente natural para después analizarlos.

Y es de diseño transversal porque se recolectan datos en un solo momento, en un tiempo único, aplicando el cuestionario.

De acuerdo a las características de la presente investigación, el diseño corresponde al no experimental, transversal, correlacional, ya que mide el grado de relación entre las variables: tipificación de conducta delictiva y suplantación de identidad en los delitos informáticos, el mismo que obedece al siguiente esquema:



M = muestra
O = observación
1, 2, = variables correlacionales: tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos.
r = grado de correlación entre las variables.

1.6.3 Población y muestra de la Investigación

a) Población

Según Hernández, Fernández y Bautista (2013: 235), "la población es el conjunto de todos los casos que concuerdan con una serie de especificaciones (....) Las poblaciones deben situarse claramente en torno a sus características de contenido, de lugar y en el tiempo".

La población objeto de estudio estaba conformada por 423 estudiantes de la Facultad de Derecho y Ciencia Política, de la Universidad Alas Peruanas de Piura en la ciudad y Región de Piura, en el año 2017.

b) Muestra

Según Hernández, Fernández y Baptista (2013:235), "la muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población (...) Básicamente categorizamos las muestras en dos grandes ramas, las muestras no probabilísticas y las muestras probabilísticas.

En estas últimas todos los elementos de la población tienen la misma posibilidad de ser escogidos y se obtienen definiendo las características de la población y el tamaño de la muestra (...) en las

muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra. Aquí el procedimiento no es mecánico, ni con base en fórmulas de probabilidad, sino depende del proceso de toma de decisiones de una persona o de un grupo de personas, y desde luego las muestras seleccionadas obedecen a otros criterios de investigación".

En el caso de la investigación la muestra estuvo conformada por 72 estudiantes de la Facultad de Derecho y Ciencia Política, de la Universidad Alas Peruanas de Piura en la ciudad y Región de Piura, en el año 2017.

1.6.4 Técnicas e Instrumentos de recolección de datos

a) Técnicas

Para realizar el acopio de información relevante y objetiva, que contribuyó al tema de investigación se empleó las siguientes técnicas: Técnica de la encuesta para indagar la opinión acerca de las variables: tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, a través de dos cuestionarios, la Técnica de procesamiento de datos para procesar los resultados de las encuestas a los estudiantes de la Facultad de Derecho y Ciencia Política, de la Universidad Alas Peruanas de Piura en la ciudad y Región de Piura, en el año 2017. La Técnica del Fichaje para registrar la indagación de bases teóricas del estudio. La Técnica de Opinión de expertos para validar la encuesta-cuestionario. Y la Técnica de la estadística descriptiva e inferencial para el procesamiento e interpretación de los resultados.

b) Instrumentos

Para realizar la recolección de datos, que contribuya al tema de investigación se empleará el siguiente instrumento:

El Cuestionario: Hernández Sampieri (2016) manifiesta que "El cuestionario es un instrumento de investigación. Este instrumento se

utiliza, de un modo preferente, en el desarrollo de una investigación en el campo de las ciencias sociales, para la obtención y registro de datos. Es una técnica ampliamente aplicada en la investigación de carácter cualitativa". (P.5).

Los cuestionarios sobre tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos que fueron aplicados a los estudiantes de la Facultad de Derecho y Ciencia Política, de la Universidad Alas Peruanas de Piura en la ciudad y Región de Piura, en el año 2017.

Confiabilidad de los instrumentos:

Alfa de Cronbach del Cuestionario sobre tipificación de conducta delictiva

Análisis de Fiabilidad

Cronbach's Alpha	N de Ítems
0,904	15

Fuente: Cuestionario sobre tipificación de conducta delictiva.

Programa Estadístico SPSS 24

Alfa de Cronbach del Cuestionario sobre suplantación de identidad en *los delitos informáticos*

Análisis de Fiabilidad

Cronbach's Alpha	N de Ítems
0,902	15

Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos.

Programa Estadístico SPSS 24

Los valores obtenidos, nos indican que los instrumentos: Cuestionario sobre tipificación de conducta delictiva y Cuestionario sobre suplantación de identidad en los delitos informáticos, son altamente confiables y por ende pueden ser aplicados durante el desarrollo de investigación.

1.6.5 Justificación, Importancia y Limitaciones de la Investigación

a) Justificación

El presente estudio de investigación adquirió relevancia en las siguientes justificaciones:

Justificación Teórica: teniendo en cuenta la importancia del tema, la presente investigación se justifica desde el punto de vista teórico porque a través de ésta, se determinó la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, en consecuencia servirá como antecedente teórico para trabajos de investigación posteriores.

Justificación Práctica: la presente investigación beneficiará a la sociedad piurana en principio y posteriormente a toda la sociedad peruana, ya que el problema de investigación afecta a todos y está vigente hoy más que nunca.

Justificación Metodológica: la investigación se ha desarrollado considerando las pautas metodológicas, desde la identificación del tema, la búsqueda de fuentes de información, la matriz de consistencia, el plan de tesis, considerando el diseño metodológico de enfoque cuantitativo. Ello nos ha permitido presentar dos instrumentos: cuestionario sobre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, los mismos que podrán servir de guía o modelo para otros estudios sobre el tema. Respecto a los instrumentos, estos son dos cuestionarios, referentes a tipificación de conducta delictiva y suplantación de identidad en los delitos informáticos, que obedecen a la técnica de la encuesta.

b) Importancia

Es importante investigar este tema debido a que los delitos informáticos, tienen un incremento notable, por el mismo hecho del avance descomunal de la tecnología.

c) Limitaciones

Durante la investigación se presentaron dificultades como son:

En este tipo de trabajos, las limitaciones generalmente son de carácter económico, ya que por la misma naturaleza de estos trabajos no tienen financiamiento, ni del estado, ni mucho menos de la empresa privada, por lo que tuvo que ser solventado en su integridad por el investigador, esta dificultad fue absuelta por el investigador en su totalidad.

CAPÍTULO II:
MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes Internacionales:

Temperini, Marcelo Gabriel Ignacio; Doctorando en Derecho en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral, Santa Fe – Argentina, en su trabajo de investigación denominado: "Delitos Informáticos en Latinoamérica - 2012"; (Temperini, 2012), desarrolla lo siguiente: Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina (Norton, 2012). El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina (Palazzi, 2000). El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. Por otro lado, el crecimiento sostenido del mercado negro de la información (Panda Security, 2011), funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información

personal. De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos (Norton, 2012), en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. Entre los desafíos citados anteriormente, uno de los más importantes es el hecho que este tipo de delitos pueden ser cometidos sin respetar barreras geográficas o jurisdiccionales. En este sentido, cualquier delincuente informático puede operar acciones desde un determinado lugar, conectarse a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. La cadena puede tener indeterminadas variables dependiendo de la complejidad del ataque y de los conocimientos del delincuente. Si bien esta situación no sucede en todos los casos, es relativamente sencillo realizar estos ataques en la actualidad para personas con conocimientos en informática. Esto representa para el Derecho un verdadero desafío a vencer. Manuel Castells (2012), en ocasión de un discurso del 2001, y hablando del "caos" positivo que Internet genera en la comunicación, dijo: "Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España". En seguida citó el ejemplo de cuando en 2000 un sitio Web de EE.UU. organizó la venta de votos de personas ausentes, hecho que representaba un delito electoral en ese país. Pero la Web se mudó a Alemania, donde ese hecho ya no podía ser perseguido por las leyes de ese país. En consecuencia, una importante cantidad de grupos de delincuentes informáticos, organizan sus ataques desde lugares con poca o nula legislación en la materia, o bien, en aquellos países que

aun teniendo legislación al respecto, no poseen un adecuado sistema para la detección y persecución eficaz de este tipo de delitos. Un ejemplo de ello fue el caso de un ataque de tipo viral que costó a empresas norteamericanas miles de millones de dólares, el cuál fue atribuido por el FBI a un estudiante en Filipinas al que no se lo pudo acusar de crimen alguno. Rápidamente el gobierno filipino dispuso legislación para combatir el crimen cibernético con el objetivo de evitar futuros inconvenientes (Williams, 2001). En un contexto de incremento de la ciberdelincuencia organizada a nivel mundial, los llamados "paraísos legales informáticos", son los considerados al momento de ejecución de estas actividades. En palabras del Dr. Marcelo Riquert (2013), habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad. En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica. Elementos del Trabajo y metodología En cuanto a la metodología, se ha trabajado inicialmente en la recolección de la legislación aplicable en cada uno de los países pertenecientes a Latinoamérica, más precisamente de los siguientes países que se detallan a continuación por orden alfabético: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela. Si bien se ha intentado analizar la mayor cantidad de los países de la región señalada, algunos de ellos han debido ser excluidos del estudio. Entre los diferentes límites fijados en los alcances de la investigación, se debe destacar que la misma recoge solamente la normativa vigente en países latinoamericanos en los aspectos de derecho sustantivo, no considerando dentro de los

objetivos aquellos referidos al ámbito del derecho procesal penal. (Temperini, 2012).

En el 2008, Montaño Álvarez, Alejandro Armando, en su trabajo de investigación titulado: "La regulación de los delitos informáticos", en la Universidad Nacional Autónoma de México" hace una descripción de los delitos informáticos más comunes en la red y afirma que su país está avanzando con una regulación jurídica especial sobre el avance de estas nuevas tecnologías; sin embargo existen aún limitaciones serias para el tratamiento de este tipo de delitos, en consecuencia es urgente la adecuación y actualización de la normativa al respecto. (Montaño Álvarez, 2008).

En el 2009, Ureta Arreaga, Laura Alexandra, en su trabajo de investigación titulado: "Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador", Escuela Superior Politécnica del Litoral, en la ciudad de Guayaquil - Ecuador. Sostiene que es indudable el crecimiento del uso de la tecnología informática por lo que algunos países ya tomaron acciones al respecto y que no debemos ser ajenos para ello y que debemos de tomar las medidas necesarias para prevenir ser víctimas de estos delitos. (Ureta Arreaga, 2009).

En el 2006, Toledo Dumenes, José Alfonso, en su tesis titulada: "Delitos emergentes en internet y el desafío de carabineros de chile en la prevención y control en la era informática", en la Universidad de Chile, arriba a la siguiente conclusión: Afirma que la criminología antigua se ha alojado ahora en un ciberespacio por lo que describe las modalidades de delitos informáticos y la regulación estos en algunos países y la premura que acarrea este fenómeno de crecimiento desmedido de los delitos informáticos en lo referente a su regulación y control en los diferentes ámbitos del quehacer humano, en una sociedad tan convulsionada como es la sociedad chilena. (Toledo Dumenes, 2006).

2.1.2. Antecedentes Nacionales

En el 2000 se promulgó la Ley 27309 que modifica los artículos 207-A Y 207-B del código penal y establece de manera general la interferencia, acceso o copia ilícita contenida en base de datos, y alteración, daño o destrucción de base de datos.

En el 2010, Alva Manchego, Fernando Emilio en su tesis titulada: "Sistema de información de detección de plagio en documentos digitales usando el método document Fingerprinting", Pontificia Universidad Católica del Perú". Afirma que actualmente, el plagio de documentos digitales es un problema que afecta, en diferentes dimensiones, a la sociedad en su conjunto y, muy especialmente, al ámbito académico es por esto que en este sentido habría una infracción a los derechos de autor y por lo tanto se debe normativizar en este campo del desarrollo académico.

En el 2007, Purizaca Castro, Walter, realizó un trabajo de investigación en la Universidad Alas Peruanas de Piura, titulado: "Los delitos informáticos" en el que concluye que los países europeos ya están preparados en su ordenamiento jurídico sobre estos delitos y que en nuestro país aún no se da mucha importancia a un tema deliberante se está incrementando cada día por lo que sería necesario una regulación especial en lo referente a la normativa vigente al respecto. (Purizaca Castro, 2007).

En el 2010, Quezada Castro, Guillermo Alexander, de la Universidad Alas Peruanas de Piura establece en su tesis sobre "La responsabilidad civil extracontractual del usuario como proveedor del contenido ilícito en la vulneración de la intimidad en el internet" el cual conceptualiza la necesidad de regulación en cuanto al derecho informático y el desarrollo de los delitos informáticos que contravienen a la intimidad personal. (Quezada Castro, 2010).

2.2. Bases Legales

Bases Legales Nacionales

Entre las bases legales nacionales se citan a las siguientes, las mismas que guardan relación directa con la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos:

La Constitución Política del Perú, articulo 2 numerales 5,6 y 7; y articulo 97.

El Código Penal: artículos 207-A, 207-B y 207-C.

Mediante Ley No. 27309 publicada el 17/07/2000 se han incorporado los artículos 207-A y 207-B sobre delitos informáticos a la Legislación Penal. Efectivamente, se ha vuelto a modificar el Código Penal, esta vez para adicionar cuatro artículos modificatorios y el 207-C sobre la Exención de pena de los artículos anteriores.

Artículos 183-B y 183-C Al Código Penal, en materia de pornografía infantil en internet.

Ley 28493 - Regula el uso del correo electrónico comercial no solicitado (Spam) del 18 de marzo de 2005.

Ley 27291 - Modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica. (Promulgada el 23-6-2000 y Publicada el 24-6-2000).

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 (Bramont Arias Torres, 2011). En la actualidad, los delitos informáticos están previstos en el Capítulo X (Congreso de la República, 2000) 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 cualificantes agravantes), 207°-D (tráfico ilegal de datos), y en las leyes penales especiales.

Entre estas leyes penales especiales, se encuentra la Ley Nº 30096 (Congreso de la República, 2013) "Ley de Delitos Informáticos". Esta Ley de Delitos Informáticos está conformado por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Cap. I), delitos contra datos y sistemas informáticos (Cap. II), delitos informáticos

contra la indemnidad y libertad sexual (Cap. III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Cap. IV), delitos informáticos contra el patrimonio (Cap. V), delitos informáticos contra la fe pública (Cap. VI), disposiciones comunes (Cap. VII).

Posteriormente, se promulgo la Ley N° 30171 (Congreso de la República, 2011) "Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos". La finalidad de esta ley fue adecuar la Ley N° 30096 a los estándares legales del Convenio Sobre la Cibercriminalidad (en adelante convenio de Budapest), al incorporar en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10, de la referida Ley la posibilidad de cometer el delito deliberada e ilegítimamente. Las modificaciones de la Ley N° 30171, con respecto a los delitos informáticos, consisten en las siguientes:

- Art. 1°.- Modificación de los artículos 2°, 3°, 4°, 5°, 7°, 8° y 10° de la Ley N° 30096 Ley de Delitos Informáticos.
- Art. 2°.- Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley N° 30096 Ley de Delitos Informáticos.
- Art. 3°.- Incorporación del artículo 12° a la Ley N° 30096 Ley de Delitos Informáticos.
- Art. 4°.- Modificación de los artículos 158°, 162° y 323° del Código Penal.
- Art. 5°.- Incorporación de los artículos 154°-A y 183°-B del Código Penal.
- Única Disposición Complementaria Derogatoria.- deroga el artículo 6° de la Ley N° 30096 Ley de Delitos Informáticos.

Finalidad y objeto de la ley

El Art. 1° de la Ley de delitos informáticos establece que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticos, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal -patrimonio, la fe pública y la libertad sexual, etc.- que puedan ser afectados mediante la utilización de las TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y desarrollo. Con esta Ley, se intenta garantizar la lucha eficaz contra la ciberdelincuencia.

Esta Ley no responde políticocriminalmente a la necesidad de ejercer la función punitiva del Estado enfocada en la protección de la información, sino, tiene como principal objetivo la estandarización de la ley penal

peruana con el ordenamiento penal internacional, principalmente por la Convenio contra la cibercriminalidad del Consejo Europeo (CETS 185), denominado Convenio de Budapest 30171 (Congreso de la República, 2011 – Octava Disposición Complementaria).

Bien jurídico tutelado

El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la "información" de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etc. Respecto de la información, debe ser entendida como el contenido de las bases y/o banco de datas o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico y es la importancia del "valor económico" de la información lo que ha hecho que se incorpore como bien jurídico tutelado (Gutiérrez Francés, 2002).

Sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco de la persona por la fluidez y el tráfico jurídico, y por los sistemas que lo procesan o automatizan los mismos que 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 (Gonzáles de Chaves Calamita, 2004), 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 (Gutiérrez Francés, 2002) sin perjuicio que uno de tales bienes este independientemente tutelado por otro tipo penal.

2.3 Bases Teóricas

Los delitos informáticos, son un conjunto de omisiones típicas, antijurídicas y dolosas cometidos por personas naturales o jurídicas y producidas desde una ciber-computadora de manera virtual.

Romeo Casabona se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Para Davara Rodríguez no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Ni el Código Penal de 1995 introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. Define el Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

Hoy en día la revolución tecnológica ha crecido infinitamente es así que la mayoría de acciones que realizan las empresas, personas naturales, personas jurídicas, esta virtualidad que se está llevando a través del sistema informático, por este motivo que también ha avanzado la delincuencia de manera virtual, estas conductas se les denomina delitos informáticos que son producidos desde una computadora conectada a una red donde es los hechos son planeados por una o más personas.

Los delitos Informáticos implican actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido

de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho

Es cualquier acto ilegal ejecutado con dolo para el que es esencial el conocimiento y uso, propio o ajeno, de la tecnología informática para su comisión, investigación o persecución con la finalidad de beneficiarse con ello (Institutito Nacional de Estadística e Informática, 2012).

El Código Penal Peruano, al incorporar la figura del delito informático, no establece una definición genérica del mismo, pero, lo conceptualiza en forma típica como: "las conductas típicas, antijurídicas y culpables, en que se tiene a las computadoras como instrumento o fin"; y, atípica, entendiendo que los delitos informáticos son "las actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".

Dada la complejidad del delito informático y que además vulnera varios valores o bienes jurídicos protegidos por la sociedad, el tipo básico debería contener la delimitación precisa de lo que está penado con una pena privativa de la libertad o inhabilitación para acceder al servicio informático por un determinado plazo de tiempo.

Como se ha visto en el capítulo tercero sobre nuevas tipologías, el espectro es amplio y en mucho de los casos no ingresan en el tipo penal vigente por el Código Penal que nos rige (Purizaca Castro, 2012).

Derecho Informático, es un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada "tecnología de la información".

A partir de los conceptos de "Tecnología de la Información" y "Sociedad de la Información", que son antecedentes necesarios e identificadores del Derecho Informático, ya ambos conceptos son los que le otorgan un objeto de estudio propio, el cual requiere una metodología específica con categorías conceptuales propias (además de las que comparte con las otras ramas del Derecho), y cuyas fuentes tienen particularidades originadas en el vertiginoso cambio inherente al ámbito tecnológico

Los delitos Informáticos, implican actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios,

estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Es cualquier acto ilegal ejecutado con dolo para el que es esencial el conocimiento y uso, propio o ajeno, de la tecnología informática para su comisión, investigación o persecución con la finalidad de beneficiarse con ello.

El Código Penal Peruano, al incorporar la figura del delito informático, no establece una definición genérica del mismo, pero, lo conceptualiza en forma típica como: "las conductas típicas, antijurídicas y culpables, en que se tiene a las computadoras como instrumento o fin"; y, atípica, entendiendo que los delitos informáticos son "las actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".

Dada la complejidad del delito informático y que además vulnera varios valores o bienes jurídicos protegidos por la sociedad, el tipo básico debería contener la delimitación precisa de lo que está penado con una pena privativa de la libertad o inhabilitación para acceder al servicio informático por un determinado plazo de tiempo.

Como se ha visto sobre nuevas tipologías, el espectro es amplio y en mucho de los casos no ingresan en el tipo penal vigente por el Código Penal que nos rige.

Sabotaje Informático, debe entenderse como aquellas "alteraciones causadas en datos computarizados o programas informáticos con la intención de obstaculizar el funcionamiento de un sistema informático o de telecomunicaciones", siempre que los datos o programas afectados infieran en la actividad de empresa, pues de no ser así afectarían bienes de distinta naturaleza y por ende ajeno al bien jurídico "información", todo lo que se refiere a la destrucción, modificación o inutilización de archivos y ficheros informatizados, distribución de virus y programas delictivos.

El Espionaje Informático debe entenderse como "la obtención, con ánimo de lucro y sin autorización además, de valor para el tráfico económico de la industria o comercio", todo lo que se refiere a la falsificación en materia informática, reproducción no autorizada de un programa informático protegido.

Phishing o pesca de claves secretas, los sabuesos suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los delincuentes utilizan programas para identificar claves de usuarios, que mes tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

Infracción a los derechos de autor, los medios tecnológicos disponibles en la actualidad y que se emplean en el ciberespacio permiten el intercambio de información y productos en forma incorporal. Para hacer posible este tránsito de información, ha sido preciso traducirla a un código binario que permite transmitir imágenes, sonido y texto. Es lo que se denomina "bienes digitales". En general, las legislaciones protegen, bajo la denominación del derecho de autor, todas las creaciones artísticas y científicas, en cuanto a la posibilidad de ser reproducidas por cualquier medio.

Los delitos informáticos contra la privacidad, se refiere a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la Imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

La pornografía infantil en internet, este gran problema social que está experimentando un impresionante proceso de expansión principalmente por dos motivos. El primero es el uso masivo del internet en una sociedad cada vez más globalizada; mientras que el segundo, es la dificultad de perseguir este delito gracias al uso de tecnología cada vez más avanzada, que impide el rastreo de los criminales y víctimas.

Al respecto, hay que entender también que Para el autor Joaquín Galileo Soto Campos señala que "La distribución de pornografía infantil por todo el

mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material «ofensivo» que se transmita o archive".

Consideraciones sobre el spam y los sujetos intervinientes

Analizar el spam como comúnmente se conoce a la invasión a la privacidad, requiere de algunas aclaraciones señalando a qué tipo de acciones se les considera spam y a cuáles no. Se considera spam al ataque a la privacidad caracterizada por la invasión indiscriminada y no autorizada al correo electrónico de una persona física jurídica por medio del envío de mails publicitarios o de cualquier otro tipo, lo cual indica que el envío de un solo e-mail no autorizado no cumpliría el tipo penal.

Es necesario mencionar que la cantidad de e-mails recibidos por el sujeto pasivo deben ser no autorizados ya que si él los ha permitido, entraremos en la esfera de la libre determinación por lo que tampoco podría constituirse el delito por extracción. Dos de los elementos que caracterizan este acto ilícito son:

a) Que la cantidad de-mails debe ser significativa

b) Que los mismos deben ser no autorizados por receptor

Existen siempre dos posibilidades en cuanto a los sujetos activos: los que actúan con dolo y los que lo hacen con culpa. El concepto de culpa tal y como lo mencioné en Capítulos anteriores implica negligencia, impericia, imprudencias y falta de observación de los deberes o reglamentos a su cargo.

Es necesario destacar quiénes deberían ser considerados responsables en este tipo de delitos, el administrador del Server receptor no tiene la posibilidad de controlar el contenido de los mails recibidos por un usuario por lo tanto se descarta de antemano su responsabilidad en estos casos. En todo proceso de envío y recepción de mails intervienen al menos cuatro sujetos:

a) El emisor: que es aquella persona que redacta y envía el mail a uno o varios destinatarios a fin de hacer de su conocimiento el contenido a él o los receptores.
b) El Server emisor: es la persona o página Web encargada de redireccionar el mail hacia el destino o destinos finales del mismo.
c) El Server receptor: es aquel donde se halla alojada la dirección de correo del receptor y sirve de puente entre el Server emisor y el receptor final es donde se almacena todo el correo del usuario final que puede ser el sujeto pasivo.
d) El receptor final: es la persona física jurídica titular de la dirección de correo electrónico hacia la cual fue enviado el mail que pueden las condiciones correctas constituir un caso de spam.

Resulta imposible el envío de un mail sin la voluntad expresa del sujeto, razón por la cual este tipo de conductas dolosas deben penalizarse en forma directa, y en este caso el bien jurídico protegido resulta la intimidad, lo cual dará en cada legislación el rango de penas aplicables a este tipo de delitos. En los casos del envío de e-mails no depende de la voluntad expresa de quien figura como emisor ya que podríamos hablar aquí de usurpación de correo es decir, en los casos en que alguien por medio de técnicas de hacking (Es la acción en la cual un tercero, no titular de un equipo o un sitio Web determinado, accede al mismo por la utilización de código de programación o software específico) (Cámpoli, 2012) pueda enviar correo desde una dirección ajena o bien en los casos de envío automático nos encontraremos ante un virus de tipo gusano que se auto distribuye, con lo cual no podríamos hablar de responsabilidad directa del titular de la dirección de correo desde la cual el mismo es enviado ya que existe una negligencia por falta de control del ingreso de virus al equipo propio, lo cual no puede constituir delito desde que resulta casi imposible determinar desde qué momento el equipo se encuentra afectada al ser infectado, además, el correo guardado no se encuentra bajo control directo del usuario sino de Server receptor en el cual se almacena. El emisor y el server emisor o proveedor de servicio para el emisor son quienes realmente pueden controlar o actuar con pleno conocimiento de la actitud desplegar. La responsabilidad del emisor es clara ya que con pleno conocimiento de

su acción genera la invasión a la privacidad del receptor enviando en forma manual o automática los correos electrónicos a los receptores a través de listas de correo obtenidas o creadas por el mismo a partir de datos obtenidos en forma legítima o ilegítima. Existen los sujetos posibles, el emisor del spam y el Server emisor. El emisor directo es para quien la responsabilidad resulta expresamente dolosa toda vez que nadie puede enviar por negligencia, imprudencia o impericia cientos o miles de correos electrónicos de publicidad. El emisor resulta responsable a título de dolo.

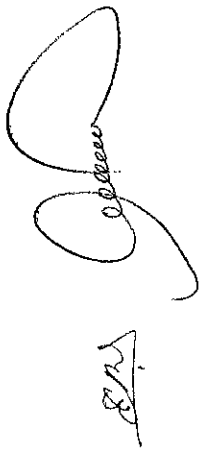
El problema a resolver es del Server emisor de que por razones obvias la máquina no podrá resultar responsable de delito alguno pues no es otra cosa que el medio para la comisión del delito y por definición del derecho penal sólo se ocupa de conductas humanas no de acciones mecánicas. Quien dirige el Server mantiene una obligación de control sobre el tráfico del mismo pero no siempre los filtros creados permiten detener el tráfico de spam en forma efectiva. Se debe considerar el hecho de que existe también una acción directa de los creadores de spam para evadir las defensas predispuestas y permitir la circulación de los mismos, aún a pesar de los esfuerzos de los programadores responsables de los equipos de transmisión de los e-mails. (Trillo Minutti, 2012).

Es evidente que no se puede adjudicar responsabilidad penal a los directores de los Servers salvo en los casos en que actúen en conjunto con los emisores actuando dolosamente pudiéndoseles imputar diferentes grados de coparticipación.

Nos queda la responsabilidad civil en los casos en que el spam produjera daños verificables en el receptor lo cual presentaría nuevos problemas de la imputabilidad. Como se ha argumentado, resulta imputable a título de dolo el envío de spam según las definiciones vertidas, razón por la cual me atrevo a especificar dos tipos penales específicos para este tipo de conductas que podrían incluirse en la legislación mexicana los cuales son:

a) Envío de correo no solicitado: el que enviare correos electrónicos no solicitados en cantidades significativas si estos no contuvieren un mecanismo para retirar al receptor de las listas del emisor sufrirá la pena de...

b) Responsabilidad de los directores de los servers emisores: en todos los casos en que se compruebe responsabilidad penal por spam de los emisores, se deberá analizar la participación de los responsables de los servers emisores la cual sólo podrá imputarse a título de dolo y por acciones directas de los mismos independientemente de la responsabilidad civil que les pudiere corresponder, la cual deberá sustanciarse por separado y según una ley especial. Según el grado de participación que se demuestra en cada caso se les imputará cómo coautores o como partícipes. (Trillo Minutti, 2012).



Como he señalado, resulta imputable a título de dolo el envío de spam según las definiciones vertidas; en resumen se puede establecer que existen dos responsabilidades, la penal por el spam y la civil. Si nos encontráramos frente a una nueva sociedad nos hallaríamos frente un nuevo grupo humano que intentaría proteger sus propios bienes jurídicos y así nacería un nuevo derecho penal como el que ahora necesita este país, el cual podría denominarse Derecho Penal Informático o Ciberderecho y para ello es imprescindible presentar un tema sobre esta nueva norma internacional.

El derecho penal informático como norma internacional:

Es necesaria la internacionalización de las normas penales de derechos informáticos, ya que desde antiguo se sostiene que el derecho penal es el reflejo de las normas morales y éticas que hacen posible la vida en sociedad, por lo cual podemos afirmar que el derecho penal es el reflejo normativo para la protección de aquéllos bienes jurídicos que esta sociedad considera valiosos. Los sujetos pasivos damnificados por estos delitos corresponden a un grupo particular que puede resultar afectado si se encuentra en contacto directo con la tecnología, específicamente con las Redes e Internet. Este es el grupo que presenta un interés concreto por la creación de una legislación penal que proteja sus derechos, la cuestión será demostrar el hecho de que sí se ha creado una nueva sociedad a la cual con todos los cambios que ha sufrido se le podría denominar Cibernacion. Esta no posee un ámbito físico en especial y por su propia constitución no posee un régimen de gobierno ya que más bien se parece a la definición y anarquía.

Toda sociedad se encuentra integrada por individuos, pero la diferencia fundamental radica en el hecho de que no necesariamente en esta Cibernación, los individuos responden a sus características físicas, históricas y aún genéticas como en el campo natural. De hecho en el ciberespacio, es la misma persona física que una moral, de aquí en todos los casos, ambas son incorpóreas a fin de unir los espacios físicos en la Red, así también en la Red no existe el sexo ya que al menos detrás de monitor puede ser un hombre una mujer quien este del otro lado. Tampoco existe la posibilidad de discriminar por sexo u orientación sexual ya que nadie sabe realmente si el que está en el otro extremo de la red es heterosexual u homosexual, hombre, mujer, adulto o niño. (Trillo Minutti, 2012).

Esto hace de la Cibernacion quizás el lugar menos discriminatorio de la historia de la humanidad, aunque a veces nos encontremos con estados como Corea en donde impiden el acceso a la Red a aquéllos que se oponen al régimen del gobierno imperante, sin embargo a lo mucho un estado puede impedir el acceso de sus connacionales a la cibernacion pero no implica que puede ejercer el control sobre sus integrantes.

Esta situación es la primera razón de orden sociológico que aconseja la creación de un Ciberderecho Penal cuyo ámbito de aplicación espacial sea el ciberespacio.

La sociedad de la Cibernacion si bien posee caracteres de todas las sociedades que integran el mundo, se integran ya los idiomas existentes en esta misma donde se hallan muchas características que le son propias y que además han nacido con ella. De hecho existe un lenguaje común integrado por palabras que fuera de su entorno carecen del significado alguno como por ejemplo el hacking, cracking spam, etc.

Estas son en definitiva las características básicas y nos permiten inferir el hecho de que nos encontramos ante una nueva sociedad que requiere de su propia regularización, por otra parte, esta sociedad carece de un elemento, y es el que reclama seguridad jurídica, la cual sólo puede obtenerse por medio de una regulación unificada ya que la multijuricidad en esta sociedad impide que las reglas sean parejas para todos los que la integran.

Se comenzó a observar el nacimiento en distintas partes del mundo de legislación referida a estos tópicos, incorporando las correspondientes figuras típicas introduciéndolas en los respectivos ordenamientos jurídicos a través de la modificación del Código Penal o creando leyes penales especiales. En este sentido, particular trascendencia tendrían en su oportunidad los ordenamientos normativos de Estados Unidos contenidas en la Federal Computer Crime Act (1984) y la Computer Fraud and Abuse Act (1986), y la correspondiente a Gran Bretaña conocida como Computer Misuse Act (1990). Así mismo el FBI mantiene el programa Uniform Crime Reporting(UCR, Informes, Uniformes de Crímenes).

Las agencias policiales locales completan un informe mensual que envían al FBI y que se consolidan y se reúnen en informe que documentan las estadísticas. El Nacional Incident-Based Reporting System (NIBRS; Sistema Nacional de Informes Basados en Incidentes) especifica los datos de los que se debe informar directamente el FBI a través de los sistemas de procesamiento de datos que cumplen con las especificaciones de NIBRS.

La policía de un país no suele tener jurisdicción oficial en otros países, sin embargo, cuando la policía de diferentes países colabora, el impacto sobre el crimen puede ser importante. Este efecto se aprecia en los grandes esfuerzos de colaboración entre la policía y otras agencias del orden en varios países, sin embargo en México no ha habido unión por parte de las policías a fin de lograr combatir el cibercrimen de manera conjunta entre todas las entidades federativas que conforman a la Nación mexicana. (Trillo Minutti, 2012).

De lo planteado con anterioridad, he establecido que existen dos razones suficientes para la creación de un sistema penal único para el Ciberespacio. Por lo demás, podemos considerar que nos encontramos ante una nueva sociedad que será la que quedará regulada por estas leyes especiales, lo cual de ninguna forma alteraría las soberanías nacionales, lo cual es el temor que se tiene en varios Estados, si se crea un organismo internacional dedicado a perseguir y juzgar los delitos cometidos en la Red. Así mismo, creo necesario establecer el tratamiento de la tipificación de los delitos

electrónicos e informáticos en el ámbito Internacional, señalando lo que en algunos países se ha hecho al respecto. (Trillo Minutti, 2012).

En Alemania las formas típicas del derecho alemán son:

a) Espionaje de datos (Arts. 2002)
b) Estafa informática (263)
c) Utilización abusiva de cheques o tarjetas de crédito (266)
d) Falsificación de datos con valor probatorio (269
e) Engaño en el tráfico jurídico mediante elaboración de datos (270)
f) Falsedad ideológica (271)
g) Uso de documentos falsos (273)
h) Destrucción de datos (303)
i) Sabotaje informático 303). (http://www.libardo.50megs.com/Delito Intimidad.htm).

El Código Penal Alemán, incluye secciones sobre el espionaje de datos, la modificación de datos y el sabotaje informático (secciones 202ª, 303aa y 303b del Código Penal). (Littlejohn Zinder, 2011).

En Argentina, no cuentan con leyes especiales para los delitos electrónicos. Sin embargo, el Código Penal del país, incluye otras leyes que pueden aplicarse a determinados delitos, independientemente de si se comenten mediante ordenadores o bien Internet. Por ejemplo los Artículos 128 y 129, que tratan sobre la pornografía infantil, consideran ilegal la publicación, creación, reproducción o distribución de imágenes obscenas. Así mismo, en el Artículo segundo de la Ley de Crimen Organizado se establece, que si tres o más personas participan juntos en un crimen relacionado con pornografía, secuestro o tráfico de niños pueden ser acusados conforme a este Artículo.

La posibilidad de enfrentarse a otros delitos informáticos que no estén relacionados con la pornografía infantil es muy limitada en este país, es decir, la Ley Argentina solo abarca delitos cometidos contra gente, cosas, animales, mas no ataques digitales.

En España, dentro de Código Penal Español, se contiene a los delitos informáticos de manera amplia, así mismo se señalan las sanciones aplicables a cada caso en particular, teniendo así los siguientes delitos informáticos:

a) Ataques que se producen contra el derecho a la intimidad.
b) Infracciones a la propiedad Intelectual a través de la protección de los derechos de autor.
c) Falsedades
d) Sabotajes informáticos
e) Fraudes informáticos
f) Amenazas
g) Calumnias e injurias
h) Pornografía infantil

En Francia, en su Ley número 88-19 del 5 de enero de 1988 se encuentra tipificado el fraude informático, el cual consta de:

a) Acceso fraudulento a un sistema de elaboración de datos
b) Sabotaje informático
c) Destrucción de datos
d) Falsificación de documentos informáticos
e) Uso de documentos informáticos falsos

Así mismo han firmado el Acuerdo contra el cibercrimen de la COE, el cual no es condicionante sino que fue necesario que Francia aprobara su propialegislación para llevar a cabo la implementación del mismo.

El Código Penal francés, incluye disposiciones relacionadas con los delitos informáticos desde 1993. Los artículos del 323-1 al 323-4 tratan sobre la obtención de acceso por medios fraudulentos o manipular o distorsionar el funcionamiento de, o introducir datos fraudulentos en sistemas automatizados de procesamiento de datos. (Littlejohn Zinder, 2011).

Queda claro que la mejor posibilidad de tener una regulación a nivel Internacional con respecto a los delitos electrónicos e informáticos, es la firma de un Tratado Internacional que regule las cuestiones suscitadas en la Red o aquéllas que atañen a los derechos de la Cibernación.

Como podrá suponerse, existen dos maneras de concluir y establecer recomendaciones del presente Capítulo, una de carácter político y la otra de carácter penal, sobre la cual se intentan delinear los posibles tipos penales a fin de que sean incluidos en la legislación Mexicana. Desde el punto de vista político, lo que se requiere y a la brevedad posible, es una Declaración sobre seguridad ante hechos de Ciberterrorismo a fin de poner

sobre aviso a los Estados con sistemas vulnerables o deficientes. Desde el punto de vista penal, de acuerdo a lo expresado en el Capítulo en el que se define al hacking (Capítulo II), existe el agravante para este tipo de conductas cuando ponen en riesgo la salud o la vida de la población, la cual debe imponerse desde mi punto legislativo, la pena máxima dentro de cada sistema penal. Si bien estas previsiones penales quizá no sean todo lo necesario para evitar este tipo de actos, lo que sí creo firmemente es que son casi indispensables a efecto de tener previstos los tipos penales necesarios para el cumplimiento de la acción preventiva que establezco en el Capítulo VI, por parte tanto de la sociedad, legislación penal y autoridades nacionales e intencionales competentes.

2.4. Definición de términos básicos

a) Espionaje informático: robo de información por cualquier medio, la recopilación de la información estratégica de una empresa por la competencia o por un tercero a petición de esta.

b) Ciberdelicuente: es básicamente cualquier tipo de actividad criminal con conocimientos de informática en la que utiliza un ordenador para cometer actos ilícitos de manera virtual y enviando desde los virus y los espías hasta la suplantación de identidad.

c) Delito informático: es el conjunto de acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información.

d) Derecho informático: se denomina derecho informático al conjunto de normas, reglas y principios jurídicos que tiene por objeto evitar que la tecnología pueda conculcar (infringir vulnerar) derechos fundamentales del hombre, que se ocupa de la regulación derivadas de la producción, uso comercialización de los bienes informáticos, así como la transmisión de datos.

e) Hackers: conocido también como "Pirateo Informático", consiste en entrar sin autorización a una computadora y explorar su interior.

f) Informática: es la ciencia que tiene por finalidad almacenar y ordenar, según un tratamiento lógico y con cierto criterio científico, todos los datos necesarios para la solución de un problema que se trata.

g) Informática jurídica: es la aplicación de la computadora a la actividad legal, para maximizar su eficiencia y su eficacia, logrando luego una recuperación muy rápida y agilizando la actividad administrativa o de investigación jurídica.

h) Infracción a los derechos de autor: es el uso indebido o no autorizado de cualquier obra de autor nacional o e como la copia, comercialización, explotación, u otra actividad que viole algún nacional o internacional sobre el particular.

i) Internet: es una red de computadoras o también llamados ordenadores, formada por ciento de miles de computadoras conectadas permanentemente por el mundo, habiendo sido considerada como la Red de redes.

j) Sistema de información: conjunto de partes que funcionan relacionándose entre sí con el objetivo de capturar, almacenar y procesar información.

k) Tecnología de información: comprende los aspectos relacionados al hardware de un sistema de información, el cual comprende computadoras, servidores, equipos de comunicación y equipos de seguridad, así como los sistemas que permiten su operación y que son necesarios para el funcionamiento de los sistemas de información.

l) Sabotaje Informático: es cualquier actividad encaminada a la inhabilitación temporal o permanente, parcial o total de los medios informáticos con la finalidad de vulnerar la capacidad productiva de la empresa propietaria de esos medios u organismo público.

CAPÍTULO III

PRESENTACIÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

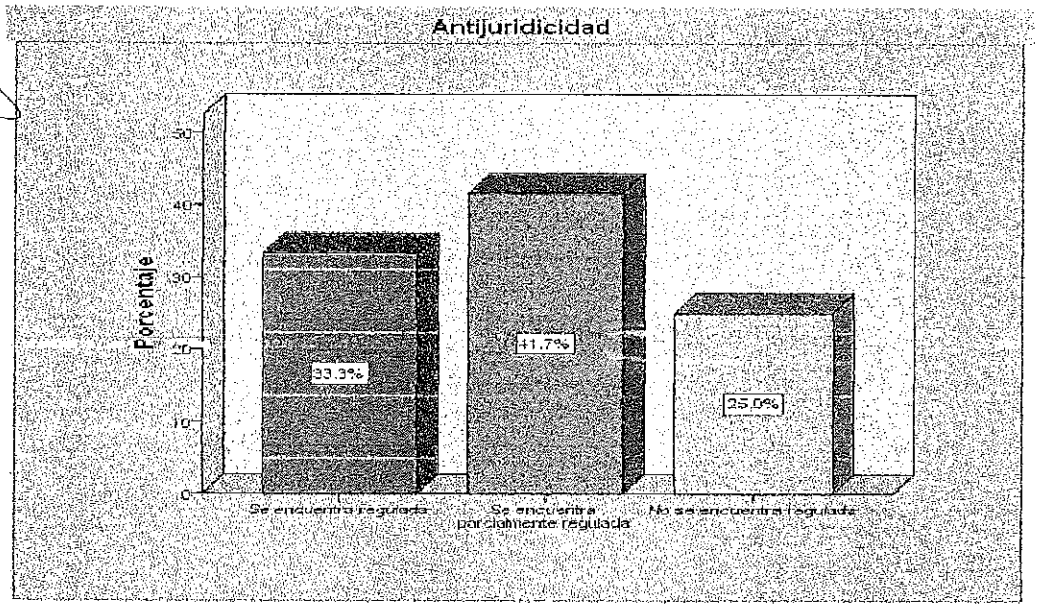
3.1. Análisis de Tablas y Gráficos

TABLA N° 1

RESULTADOS DE LA DIMENSIÓN ANTIJURIDICIDAD					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Se encuentra regulada	24	33,3	33,3	33,3
	Se encuentra parcialmente regulada	30	41,7	41,7	75,0
	No se encuentra regulada	18	25,0	25,0	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre tipificación de conducta delictiva.

GRÁFICO N° 1



Fuente: Cuestionario sobre tipificación de conducta delictiva.

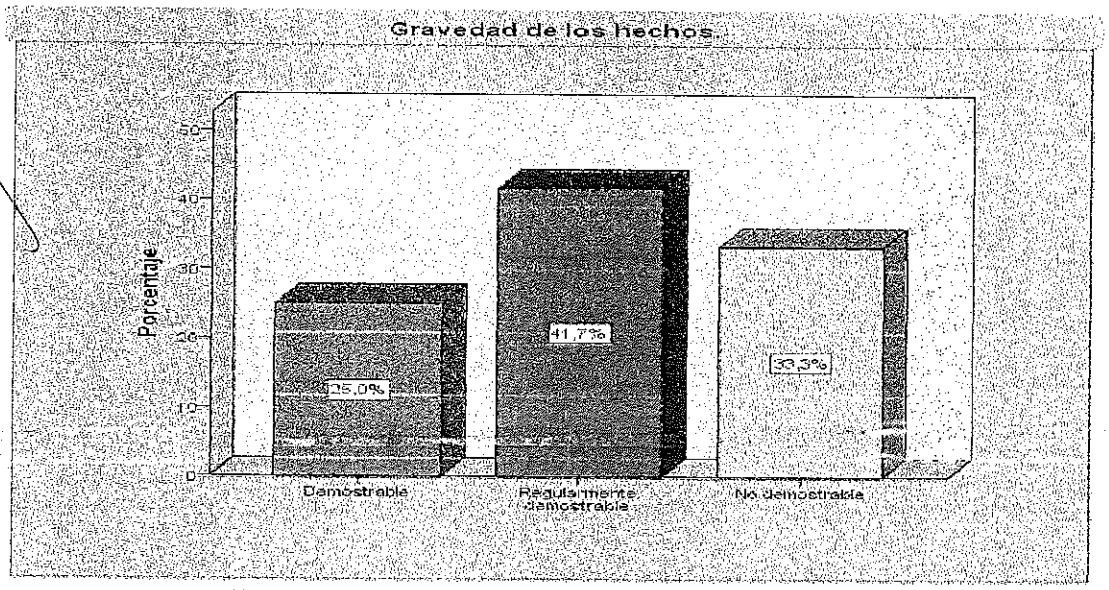
Al observar el contenido de la tabla y gráfico N° 1, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable tipificación de conducta delictiva, en la dimensión antijuridicidad; 24, que representa al 33,3% manifiesta que se encuentra regulada; mientras que 30, que equivale al 41,7%, manifiesta que se encuentra parcialmente regulada y 18, que representa al 25,0% manifiesta que no se encuentra regulada respecto a la dimensión antijuridicidad; ello nos lleva a concluir que la mayoría de la muestra afirma que la antijuridicidad en la tipificación de la conducta delictiva se encuentra parcialmente regulada, tal como se evidencia en la tabla y gráfico precedentes.

TABLA N° 2

RESULTADOS DE LA DIMENSIÓN GRAVEDAD DE LOS HECHOS					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Demostrable	18	25,0	25,0	25,0
	Regularmente demostrable	30	41,7	41,7	66,7
	No demostrable	24	33,3	33,3	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre tipificación de conducta delictiva.

GRÁFICO N° 2



Fuente: Cuestionario sobre tipificación de conducta delictiva.

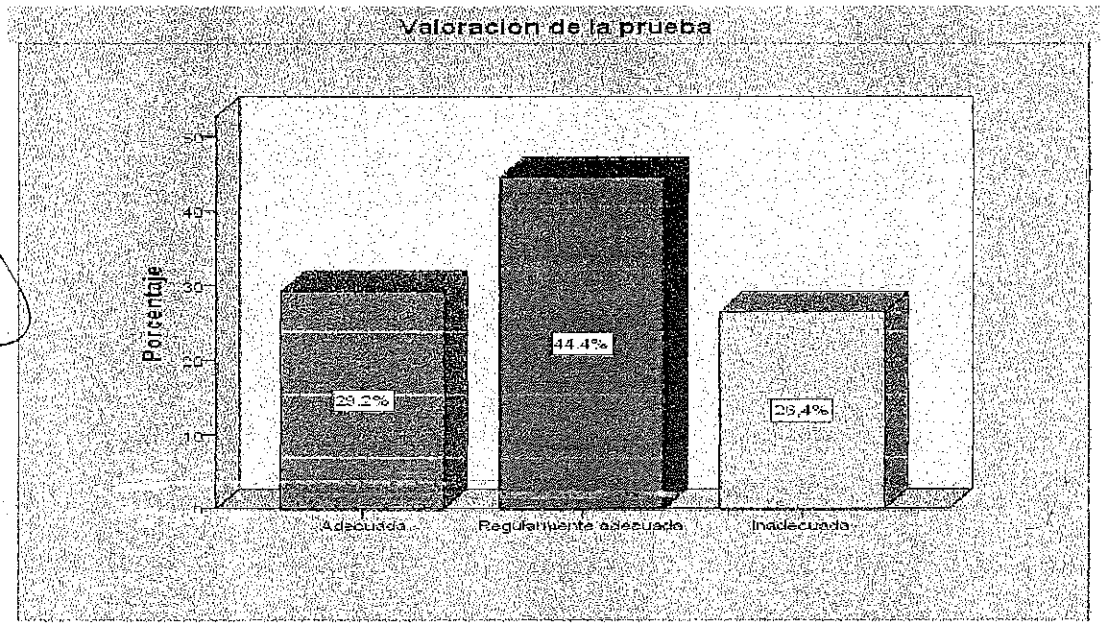
Al observar el contenido de la tabla y gráfico N° 2, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable tipificación de conducta delictiva, en la dimensión gravedad de los hechos; 18, que representa al 25,0% manifiesta que es demostrable; mientras que 30, que equivale al 41,7%, manifiesta que es regularmente demostrable y 24, que representa al 33,3% manifiesta que no es demostrable respecto a la dimensión gravedad de los hechos; ello nos lleva a concluir que la mayoría de la muestra afirma que la gravedad de los hechos en la tipificación de la conducta delictiva es regularmente demostrable, tal como se evidencia en la tabla y gráfico precedentes.

TABLA N° 3

RESULTADOS DE LA DIMENSIÓN VALORACIÓN DE LA PRUEBA					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Adecuada	21	29,2	29,2	29,2
	Regularmente adecuada	32	44,4	44,4	73,6
	Inadecuada	19	26,4	26,4	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre tipificación de conducta delictiva.

GRÁFICO N° 3



Fuente: Cuestionario sobre tipificación de conducta delictiva.

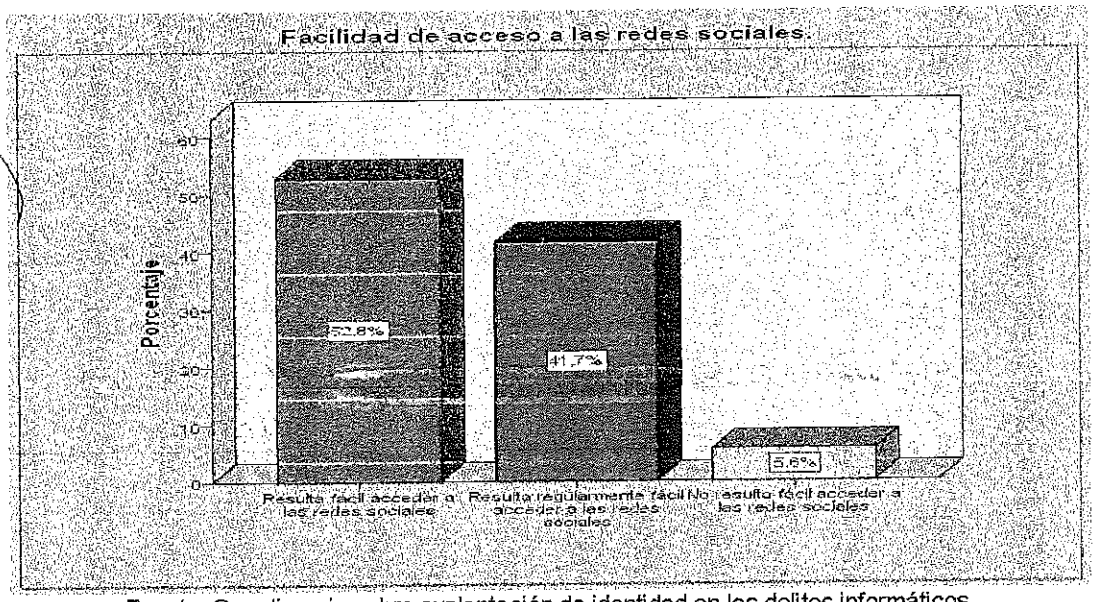
Al observar el contenido de la tabla y gráfico N° 3, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable tipificación de conducta delictiva, en la dimensión valoración de la prueba; 21, que representa al 29,2% manifiesta que es adecuada; mientras que 32, que equivale al 44,4%, manifiesta que es regularmente adecuada y 19, que representa al 26,4% manifiesta que no es adecuada respecto a la dimensión valoración de la prueba; ello nos lleva a concluir que la mayoría de la muestra afirma que la valoración de la prueba en la tipificación de la conducta delictiva es regularmente adecuada, tal como se evidencia en la tabla y gráfico precedentes.

TABLA N° 4

RESULTADOS DE LA DIMENSIÓN FACILIDAD DE ACCESO A LAS REDES SOCIALES					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Resulta fácil acceder a las redes sociales	38	52,8	52,8	52,8
	Resulta regularmente fácil acceder a las redes sociales	30	41,7	41,7	94,4
	No resulta fácil acceder a las redes sociales	4	5,6	5,6	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos.

GRÁFICO N° 4



Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos.

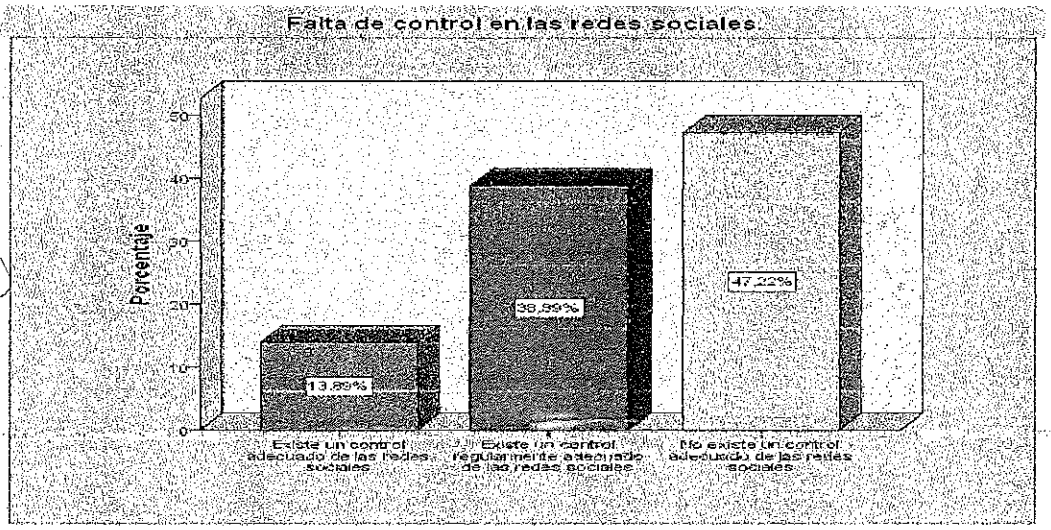
Al observar el contenido de la tabla y gráfico N° 4, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable suplantación de identidad en los delitos informáticos, en la dimensión facilidad de acceso a las redes sociales; 38, que representa al 52,8% manifiesta que resulta fácil acceder a las redes sociales; mientras que 30, que equivale al 41,7%, manifiesta que resulta regularmente fácil acceder a las redes sociales y 4, que representa al 5,6% manifiesta que no resulta fácil acceder a las redes sociales respecto a la dimensión facilidad de acceso; ello nos lleva a concluir que la mayoría de la muestra afirma que resulta fácil acceder a las redes sociales en la suplantación de identidad en los delitos informáticos, tal como se evidencia en la tabla y gráfico precedentes.

TABLA N° 5

RESULTADOS DE LA DIMENSIÓN FALTA DE CONTROL EN LAS REDES SOCIALES					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Existe un control adecuado de las redes sociales	10	13,9	13,9	13,9
	Existe un control regularmente adecuado de las redes sociales	28	38,9	38,9	52,8
	No existe un control adecuado de las redes sociales	34	47,2	47,2	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos

GRÁFICO N° 5



Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos

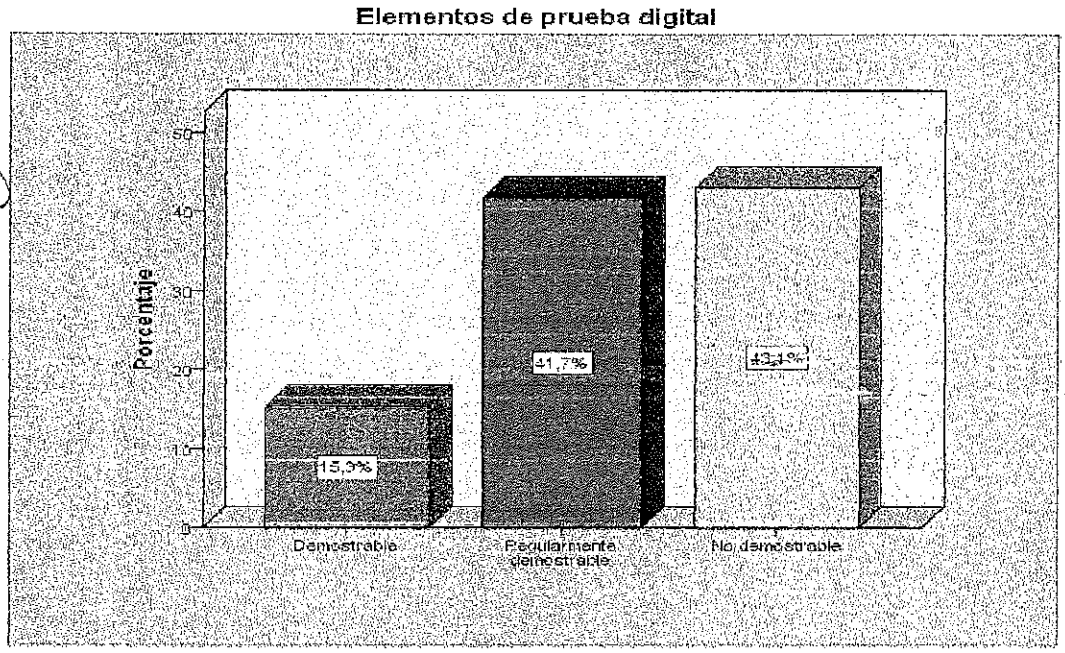
Al observar el contenido de la tabla y gráfico N° 5, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable suplantación de identidad en los delitos informáticos, en la dimensión falta de control en las redes sociales; 10, que representa al 13,9% manifiesta que existe un control adecuado de las redes sociales; mientras que 28, que equivale al 38,9%, manifiesta que existe un control regularmente adecuado de las redes sociales y 34, que representa al 47,2% manifiesta que no existe un control adecuado de las redes sociales respecto a la dimensión falta de control en las redes sociales; ello nos lleva a concluir que la mayoría de la muestra afirma que no existe un control adecuado de las redes sociales en la suplantación de identidad en los delitos informáticos, tal como se evidencia en la tabla y gráfico precedentes.

TABLA N° 6

RESULTADOS DE LA DIMENSIÓN ELEMENTOS DE PRUEBA DIGITAL					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Demostrable	11	15,3	15,3	15,3
	Regularmente demostrable	30	41,7	41,7	56,9
	No demostrable	31	43,1	43,1	100,0
	Total	72	100,0	100,0	

Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos

GRÁFICO N° 6



Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos

Al observar el contenido de la tabla y gráfico N° 6, los resultados del cuestionario aplicado a una muestra representativa de 72 estudiantes de la Universidad Alas Peruanas de Piura, respecto a la variable suplantación de identidad en los delitos informáticos, en la dimensión elementos de prueba digital; 11, que representa al 15,3% manifiesta que es demostrable; mientras que 30, que equivale al 41,7%, manifiesta que es regularmente demostrable y 31, que representa al 43,1% manifiesta que no es demostrable respecto a la dimensión elementos de prueba digital; ello nos lleva a concluir que la mayoría de la muestra afirma que no es demostrable en la suplantación de identidad en los delitos informáticos, tal como se evidencia en la tabla y gráfico precedentes.

Prueba de Hipótesis.

Después de procesar los resultados obtenidos de cada variable y sus dimensiones correspondientes a través del programa SPSS 24, se obtuvo los siguientes valores como coeficientes:

Respecto a la hipótesis general:

H_i Existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

H_0 No existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017.

Toma de decisión

Se puede apreciar en la tabla N° 7 que, al correlacionar los resultados totales de las variables tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, se obtiene un valor de Rho de Spearman =0,868; lo que indica que existe una correlación positiva alta; en consecuencia se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Tal como se evidencia en el siguiente cuadro de correlación, a través del software SPSS 24:

TABLA N° 7

CORRELACIÓN DE LA HIPÓTESIS GENERAL				
			Tipificación de conducta delictiva	Suplantación de identidad en los delitos informáticos
Rho de Spearman	Tipificación de conducta delictiva	Coeficiente de correlación	1,000	,868**
		Sig. (bilateral)	.	,000
		N	72	72
	Suplantación de identidad en los delitos informáticos	Coeficiente de correlación	,868**	1,000
		Sig. (bilateral)	,000	.
		N	72	72
**. La correlación es significativa en el nivel 0,01 (2 colas).				

Respecto a las hipótesis específicas:

Primera hipótesis específica

H_i Existe una relación significativa entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017.

H_0 No existe una relación significativa entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017.

Toma de decisión

Se puede apreciar en la tabla N° 8 que, al correlacionar los resultados totales de la variable tipificación de conducta delictiva y la dimensión facilidad de acceso a las redes sociales, de la variable suplantación de identidad en los delitos informáticos, se obtiene un valor de Rho de Spearman = 0,808; lo que indica que existe una correlación positiva alta; en consecuencia se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Tal como se evidencia en el siguiente cuadro de correlación, a través del software SPSS 24:

TABLA N° 8

CORRELACIÓN DE LA PRIMERA HIPÓTESIS ESPECÍFICA				
			Tipificación de conducta delictiva	Facilidad de acceso a las redes sociales.
Rho de Spearman	Tipificación de conducta delictiva	Coeficiente de correlación	1,000	,808**
		Sig. (bilateral)	.	,000
		N	72	72
	Facilidad de acceso a las redes sociales.	Coeficiente de correlación	,808**	1,000
		Sig. (bilateral)	,000	.
		N	72	72
**. La correlación es significativa en el nivel 0,01 (2 colas).				

Segunda hipótesis específica:

H_i Existe una relación significativa entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017.

H_0 No Existe una relación significativa entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017.

Toma de decisión

Se puede apreciar en la tabla N° 9 que, al correlacionar los resultados totales de la variable tipificación de conducta delictiva y la dimensión falta de control en las redes sociales de la variable suplantación de identidad en los delitos informáticos, se obtiene un valor de Rho de Spearman = 0,839; lo que indica que existe una correlación positiva alta; en consecuencia se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Tal como se evidencia en el siguiente cuadro de correlación, a través del software SPSS 24:

TABLA N° 9

CORRELACIÓN DE LA SEGUNDA HIPÓTESIS ESPECÍFICA				
			Tipificación de conducta delictiva	Falta de control en las redes sociales.
Rho de Spearman	Tipificación de conducta delictiva	Coeficiente de correlación	1,000	,839**
		Sig. (bilateral)	.	,000
		N	72	72
	Falta de control en las redes sociales.	Coeficiente de correlación	,839**	1,000
		Sig. (bilateral)	,000	.
		N	72	72
**. La correlación es significativa en el nivel 0,01 (2 colas).				

Tercera hipótesis específica:

H_i Existe una relación significativa entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017.

H_0 No Existe una relación significativa entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017.

Toma de decisión

Se puede apreciar en la tabla N° 10 que, al correlacionar los resultados totales de la variable tipificación de conducta delictiva y la dimensión elementos de prueba digital de la variable suplantación de identidad en los delitos informáticos, se obtiene un valor de Rho de Spearman =0,858; lo que indica que existe una correlación positiva alta; en consecuencia se rechaza la hipótesis nula y se acepta la hipótesis de investigación. Tal como se evidencia en el siguiente cuadro de correlación, a través del software SPSS 24:

TABLA N° 10

CORRELACIÓN DE LA TERCERA HIPÓTESIS ESPECÍFICA				
			Tipificación de conducta delictiva	Elementos de prueba digital
Rho de Spearman	Tipificación de conducta delictiva	Coeficiente de correlación	1,000	,858**
		Sig. (bilateral)	.	,000
		N	72	72
	Elementos de prueba digital	Coeficiente de correlación	,858**	1,000
		Sig. (bilateral)	,000	.
		N	72	72
**. La correlación es significativa en el nivel 0,01 (2 colas).				

3.2. Discusión de Resultados:

Temperini, Marcelo Gabriel Ignacio; Doctorando en Derecho en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral, Santa Fe – Argentina, en su trabajo de investigación denominado afirma que las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina (Norton, 2012). El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina (Palazzi, 2000). El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. Por otro lado, el crecimiento sostenido del mercado negro de la información (Panda Security, 2011), funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal. De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos (Norton, 2012), en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses (Temperini, 2012). Los resultados de la presente investigación corroboran con las afirmaciones del autor en el sentido que se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017; tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,868, lo que indica que existe una correlación positiva alta entre las variables.

Montaño Álvarez, Alejandro Armando, en su trabajo de investigación titulado: "La regulación de los delitos informáticos", en la Universidad Nacional Autónoma de México" hace una descripción de los delitos informáticos más comunes en la red y afirma que su país está avanzando

con una regulación jurídica especial sobre el avance de estas nuevas tecnologías; sin embargo existen aún limitaciones serias para el tratamiento de este tipo de delitos, en consecuencia es urgente la adecuación y actualización de la normativa al respecto. (Montaño Álvarez, 2008). Al respecto los resultados de la presente investigación concuerdan con el autor, ya que se puede advertir que en nuestro país existen serias dificultades en el control de los delitos informáticos y por ende se plantea una modificación de la normativa vigente, con respecto a los delitos informáticos específicamente en los delitos de suplantación de identidad.

La policía de un país no suele tener jurisdicción oficial en otros países, sin embargo, cuando la policía de diferentes países colabora, el impacto sobre el crimen puede ser importante. Este efecto se aprecia en los grandes esfuerzos de colaboración entre la policía y otras agencias del orden en varios países, sin embargo en México no ha habido unión por parte de las policías a fin de lograr combatir el cibercrimen de manera conjunta entre todas las entidades federativas que conforman a la Nación mexicana. De lo planteado con anterioridad, he establecido que existen dos razones suficientes para la creación de un sistema penal único para el Ciberespacio. Por lo demás, podemos considerar que nos encontramos ante una nueva sociedad que será la que quedará regulada por estas leyes especiales, lo cual de ninguna forma alteraría las soberanías nacionales, lo cual es el temor que se tiene en varios Estados, si se crea un organismo internacional dedicado a perseguir y juzgar los delitos cometidos en la Red. (Trillo Minutti, 2012). Los resultados de la presente tesis, corroboran lo manifestado por el autor, ya que los delitos informáticos, merecen un tratamiento especializado, por la misma magnitud de este problema, en concordancia con ello estos delitos deberían ser abordados de manera conjunta con los países que se vean afectados de una u otra manera.

3.3 CONCLUSIONES:

PRIMERA:

Se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017; tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,868, lo que indica que existe una correlación positiva alta entre las variables.

SEGUNDA:

Se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017; tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,808, lo que indica que existe una correlación positiva alta entre las variables.

TERCERA:

Se determinó que existe una relación significativa entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017; tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,839, lo que indica que existe una correlación positiva alta entre las variables.

CUARTA:

Se determinó que existe una relación significativa entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017; tal como se corrobora con el coeficiente de correlación de Spearman Rho igual a 0,858, lo que indica que existe una correlación positiva alta entre las variables.

3.4. RECOMENDACIONES:

PRIMERA:

Al Congreso de la República del Perú, se recomienda la Modificatoria de la Ley N° 30096 (Ley de delitos informáticos); en lo referente a suplantación de identidad (Anteproyecto de ley que propone la modificatoria del art. 9 de la Ley 30096 a fin de tipificar una mejor conducta delictiva en materia de suplantación de identidad en los delitos informáticos, Perú.2017)

SEGUNDA:

Al Poder Judicial implementar talleres de aprendizaje sobre la tipificación y desarrollo de delitos informáticos, para evidenciar un mejor control en la administración de justicia.

TERCERA:

Al Ministerio Público implementar talleres de aprendizaje sobre la tipificación y desarrollo de delitos informáticos, para evidenciar un mejor control en la administración de justicia y sobre todo garantizar la seguridad de los usuarios de las redes sociales.

CUARTA:

A la Policía Nacional del Perú, específicamente a la División de delitos de Alta Tecnología, organizar eventos que busquen la utilización de las tecnologías adecuadas para una mejor tipificación de los delitos virtuales.

3.5 Fuentes de Información

Ajucum Juárez, D. (2012). *Reinserción Social del Condenado posterior al cumplimiento de la pena de prisión.* Quetzatenando: Universidad Rafael Landívar.

Alva Garcia, K. M. (2014). *Fortalecimiento de la Proteccion al Ambiente y los Recursos Naturales en la Constitucion Peruana de 1993.* Trujillo: Universidad Privada Antenor Orrego.

Alvarez Zapata, O. J. (2013). *Perspectivas de la Mineria Artesanal y de Pequeña Escala Responsable: Un Analisis de Proyecto Piloto en El Choco.* Medellin: Universidad Nacional de Colombia.

Ambiente, M. d. (2011). *Compendio de la Legislacion Ambiental Peruana.* Lima: Ministerio del Ambiente.

Astaburuaga Chales de Beaulieu, F. A. (2010). *La Discrecionalidad Administrativa en el Contexto del Sistema de Evaluacion de Impacto Ambiental.* Santiago de Chile: Universidad de Chile.

Carrillo Hoyos, S. V. (2011). *Comunidades y Mineria: La Comunicacion en el Conflicto.* Lima: Pontificia Universidad Catolica del Peru.

Comercio, E. (15 de Enero de 2017). *http://elcomercio.pe/lima/nuevos-decretos-legislativos-mineria-informal-159109.*

Congreso de la Republica del Peru. (2005). *Ley General del Ambiente N° 28611.* Lima: Congreso de La Republica del Peru.

Hernández, Fernández y Batista (2016). *Metodología de la Investigación.* Ed. MC Graw hill

López Melero, M. (2011). *Los Derechos Fundamentales de los Presos y su Reinserción Social.* Alcalá: Universidad de Alcalá.

Malaver Castañeda, R. (2014). *Tratamiento penitenciario y resocialización de los internos reincidentes del centro penitenciario de Cajamarca.* Lima: Universidad Privada del Norte. Facultad de Derecho y Ciencias Políticas.

Moschella Miloslavich, P. (2011). *Impactos Ambientales de la Mineria Aurifera y Percepcion Local en La Microcuenca Huacamayo- Madre de Dios.* Lima: Pontificia Universidad Catolica del Peru.

Peru, C. d. (1993). *Constitucion Politica del Peru .* Lima: Congreso de la Republica del Peru.

Peru, C. d. (2016). *Decreto Legislativo N° 1293.* Lima: Congreso de la Republica del Peru.

Peru, C. d. (2017). *Decreto Legislativo N° 1336.* Lima: Congreso de la Republica del Peru.

Romero Calles, I. F. (2012). *Incidencia de la Politica Publica en la Regulacion de la Pequeña Mineria y Mineria Artesanal.* Quito: Facultad Latinoamericana de Ciencias Sociales-Sede Ecuador.

Rubio Correa, M. (1984). *El sistema Jurídico, Introducción al Derecho.* Lima: PUCP.

Sánchez Carlessi H. y Reyes Meza C. (2010). *Metodología y diseños en la investigación científica.*

ANEXOS

Anexo 1: Matriz de Consistencia

Anexo 2: Cuestionarios

Anexo 3: Validez y confiabilidad de los instrumentos

Anexo 4: Anteproyecto de Ley

ANEXO 1: MATRIZ DE CONSISTENCIA

TÍTULO: "IMPORTANCIA DE PROPONER MODIFICACIONES NORMATIVAS A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ 2017"

Autor: Br. Alberca Velasco, Huarmi

Problema Principal	Objetivo general	Hipótesis general	Variables	Dimensiones	Diseño Metodológico
¿Qué relación existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017? **Problemas secundarios:** a) ¿Qué relación existe entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017? b) ¿Qué relación existe entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017? c) ¿Qué relación existe entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017?	Determinar la relación que existe entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017. **Objetivos específicos:** a) Determinar la relación que existe entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017. b) Determinar la relación que existe entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017. c) Determinar la relación que existe entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017.	Existe una relación significativa entre la tipificación de conducta delictiva y la suplantación de identidad en los delitos informáticos, Piura 2017. **Hipótesis específicas:** a) Existe una relación significativa entre la tipificación de conducta delictiva y la facilidad de acceso a las redes sociales, Piura 2017. b) Existe una relación significativa entre la tipificación de conducta delictiva y la falta de control en las redes sociales, Piura 2017. c) Existe una relación significativa entre la tipificación de conducta delictiva y los elementos de prueba digital, Piura 2017.	**Variable 1:** Tipificación de conducta delictiva **Variable 2:** Suplantación de identidad en los delitos informáticos	✓ Antijuridicidad ✓ Gravedad de los hechos. ✓ Valoración de la prueba ✓ Facilidad de acceso a las redes sociales. ✓ Falta de control en las redes sociales. ✓ Elementos de prueba digital.	1. **Diseño de la investigación:** No experimental - Correlacional 2. **Tipo y Nivel de la Investigación:** **Tipo:** Básica **Nivel:** Correlacional. 3. **Enfoque de la investigación:** Cuantitativa. 4. **Método de la Investigación:** Deductivo - Inductivo. La observación 5. **Población y Muestra:** **Población:** Estudiantes de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas de Piura, matriculados el 2017. **Muestra:** 72 estudiantes de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas de Piura, matriculados el 2017. 6. **Técnicas e Instrumentos de recolección de datos:** **Técnicas:** La Encuesta **Instrumento:** Cuestionario

UAP UNIVERSIDAD ALAS PERUANAS

ANEXO 2: CUESTIONARIOS

CUESTIONARIO SOBRE TIPIFICACIÓN DE CONDUCTA DELICTIVA

OBJETIVO: Estimado estudiante de la Facultad de derecho y Ciencia Política de la Universidad Alas Peruanas de Piura. Se agradece su gentil participación en el presente cuestionario, elaborado con fines académicos, solicitando su honestidad y sinceridad en la resolución del siguiente cuestionario.

INSTRUCCIONES: El cuestionario es anónimo, por favor responda con sinceridad. Lea usted con atención y conteste marcando con una "X" en un solo recuadro. En las siguientes proposiciones marque con una x en el valor del casillero que según Ud. corresponde.

Calificación:

Sí	No
2	1

Nº	Dimensiones e indicadores	2	1
	Antijuridicidad		
01	¿Considera que el Estado a través de sus normas establece la antijuridicidad de la conducta delictiva?		
02	¿El Estado Peruano a través de sus normas establece la antijuridicidad de la conducta delictiva en derechos informáticos?		
03	¿Considera que el Estado Peruano a través de sus normas establece la antijuridicidad de la conducta delictiva con referencia a los delitos de supiantación de identidad?		
04	¿Considera que el Estado Peruano a través de sus normas establece los criterios de antijuridicidad de la conducta delictiva en delitos informáticos?		
05	¿Considera que el Estado Peruano a través de sus órganos jurisdiccionales garantiza el cumplimiento de la antijuridicidad de la conducta delictiva en delitos informáticos?		
	Gravedad de los hechos		
06	¿Considera que el Estado Peruano a través de sus órganos jurisdiccionales manifiesta la gravedad de los hechos en los delitos informáticos?		
07	¿Considera que el Estado Peruano a través de la normatividad vigente manifiesta la gravedad de los hechos en los delitos informáticos?		
08	¿Considera que el Estado Peruano a través de la normatividad vigente manifiesta la gravedad de los hechos en los delitos informáticos, en lo referente a suplantación de identidad?		
09	¿Considera que el Estado Peruano a través de sus órganos jurisdiccionales manifiesta la gravedad de los hechos en los delitos informáticos, respecto a la trascendencia de los hechos?		
10	¿Considera que el Estado Peruano a través de sus órganos jurisdiccionales garantiza la gravedad de los hechos en los delitos informáticos?		
	Valoración de la prueba		
11	¿El Sistema jurisdiccional del Perú garantiza en forma idónea la valoración de la prueba?		
12	¿Los Instrumentos de Gestión jurídica garantizan la valoración de la prueba en delitos informáticos?		
13	¿Considera que los operadores de justicia cumplen con garantizar la valoración de la prueba?		
14	¿Considera que usted que la valoración de la prueba en la administración de justicia con referencia a los delitos informáticos es idónea?		
15	L valoración de la prueba es una característica imprescindible en la administración de justicia respecto a los delitos informáticos?		

Gracias por su colaboración

UAP UNIVERSIDAD ALAS PERUANAS

CUESTIONARIO SOBRE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS

OBJETIVO: Estimado estudiante de la Facultad de derecho y Ciencia Política de la Universidad Alas Peruanas de Piura. Se agradece su gentil participación en el presente cuestionario, elaborado con fines académicos, solicitando su honestidad y sinceridad en la resolución del siguiente cuestionario.

INSTRUCCIONES: El cuestionario es anónimo, por favor responda con sinceridad. Lea usted con atención y conteste marcando con una "X" en un solo recuadro. En las siguientes proposiciones marque con una x en el valor del casillero que según Ud. corresponde.

Calificación:

Siempre	A veces	Nunca
3	2	1

N°	Dimensiones e indicadores	3	2	1
	Facilidad de acceso a las redes sociales			
01	¿Existe una facilidad sin comparación para el acceso a las redes sociales?			
02	¿Cualquier persona puede hacer uso de las redes sociales en cualquier momento y sin ninguna restricción?			
03	¿Las redes sociales para su uso tienen algún nivel de restricción?			
04	¿La Policía Nacional del Perú, cuenta con la suficiente tecnología para contrarrestar los delitos informáticos?			
05	¿El Ministerio Público y el Poder Judicial, cuentan con la suficiente tecnología para contrarrestar los delitos informáticos?			
	Falta de control en las redes sociales			
06	¿Existen medidas de Fiscalización y control en las redes sociales?			
07	¿Considera que son eficientes las medidas por parte del estado Peruano en el control de las redes sociales?			
08	¿Existe cumplimiento a las normas respecto al uso de redes sociales?			
09	¿Considera que el Estado Peruano ejerce un control adecuado en lo referente al uso de las redes sociales?			
10	¿Considera que los operadores judiciales ejercen un control adecuado en lo referente al uso de las redes sociales?			
	Elementos de prueba digital			
11	¿Considera que se ejerce una adecuada presentación de elementos de prueba digita?			
12	¿Considera que el Estado Peruano considera los elementos de prueba digital suficientes respecto a la suplantación de identidad en delitos informáticos?			
13	¿Existen medidas de Fiscalización y control por parte del Estado la presentación de elementos de prueba digital?			
14	¿Considera que existe seguimiento de inteligencia respecto a los elementos de prueba digital?			
15	¿Considera que existe seguimiento adecuado respecto a los elementos de prueba digital en el delito de suplantación de identidad?			

Gracias por su colaboración

ANEXO N° 3

Validez y confiabilidad de los instrumentos

Alfa de Cronbach del Cuestionario sobre tipificación de conducta delictiva

Análisis de Fiabilidad

Cronbach's Alpha	N de Ítems
0,904	15

Fuente: Cuestionario sobre tipificación de conducta delictiva.

Programa Estadístico SPSS 24

Alfa de Cronbach del Cuestionario sobre suplantación de identidad en los delitos informáticos

Análisis de Fiabilidad

Cronbach's Alpha	N de Ítems
0,902	15

Fuente: Cuestionario sobre suplantación de identidad en los delitos informáticos.

Programa Estadístico SPSS 24

Los valores obtenidos, nos indican que los instrumentos: Cuestionario sobre tipificación de conducta delictiva y Cuestionario sobre suplantación de identidad en los delitos informáticos, son altamente confiables y por ende pueden ser aplicados durante el desarrollo de investigación.

ANTEPROYECTO DE LEY

Fundamentos

Que con los avances de la ciencia y la Tecnología en la regulación legal en cuanto a Delitos Informáticos, cada día es ilimitado su desarrollo, la mayoría de los países van regulando cada vez mas de manera específica en tanto se presente un vacío legal para tipificar mejor una nueva conducta antijurídica, teniendo en cuenta en el caso del Perú que es miembro de diversos convenios internacionales, en el que debe adoptar políticas propias del Estado conforme vaya creciendo la diversidad digital e informática.

La Ciberdelincuencia que se configuran en las distintas modalidades de delitos informáticos existentes, ha llevado a que la legislación en el Perú estén encuadrarlas solo en figuras típicas tradicionales, tales como el robo, el hurto, los fraudes, las falsificaciones, las estafas, los sabotajes, los cuales en la actualidad la institución encargada de ver este tipo de ilícitos es la División de Investigación de Delitos de Alta Tecnología, Sin embargo, dado el uso de las Tecnologías de la Información y Comunicación y la peculiaridad del delito informático ahí la necesidad de hacer una modificatoria a la Ley de Delitos Informáticos, que regule este tipo de delitos de manera específica, sin embargo nuestra carrera profesional nos empuja a que podamos estar con todas las herramientas jurídicas para poder contrarrestar este flagelo que se viene dando en nuestro país.

Efecto de la Vigencia de la Norma sobre la Legislación Nacional

La presente ley modifica únicamente el artículo 9º de la Ley 30096, Ley de los Delitos Informáticos, el mismo que se encuentra redactado de la siguiente manera:

"Art. 9.- Suplantación de identidad

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

El mismo que queda redactado como sigue:

"Art. 9.- Suplantación de identidad

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

"La pena será privativa de libertad no menor de seis ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando la suplantación de identidad recaiga sobre Funcionario, servidor público u Autoridad representativa que afecte las funciones propias en perjuicio del Estado."

Análisis Costo Beneficio

El presente proyecto no irrogará gasto alguno para el Erario Nacional, constituyendo sólo la adecuación de la ciencia del Derecho, por esencia dinámica y cambiante, teniendo en cuenta que se trata de regular una mejor tipificación respecto del articulo nueve de la ley de Delitos Informáticos, en materia de Suplantación de Identidad, a efectos de incorporar como agravante cuando la suplantación de identidad recaiga sobre Funcionario, servidor público u Autoridad representativa que afecte las funciones propias en perjuicio del Estado, generando un alto bienestar social en la protección de este tipo de delitos.

Fórmula Legal

Texto del Proyecto

ANTEPROYECTO DE LEY QUE PROPONE LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD EN LOS DELITOS INFORMÁTICOS, PERÚ.2017.

CONSIDERANDO:

Que con los avances de la ciencia y la Tecnología en la regulación legal en cuanto a Delitos Informáticos, cada día es ilimitado su desarrollo, la mayoría de los países van regulando cada vez mas de manera específica en tanto se presente un vacío legal para tipificar mejor una nueva conducta antijurídica, teniendo en cuenta en el caso del Perú que es miembro de diversos convenios

internacionales, en el que debe adoptar políticas propias del Estado conforme vaya creciendo la diversidad digital e informática.

Que la Constitución Política del Perú en el numeral 6) de su artículo 2° reconoce el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar, facultando a todo sujeto a iniciar las acciones legales a fin de averiguar su nexo filial.

Que la ciencia del Derecho al no ser un producto exánime, estático, perenne sino dinámico, fluido, cambiante, ya que se nutre de la vida humana social en cuanto cultura dentro del ciberespacio, debe adecuar sus instituciones y normatividad en defensa de la persona de los riesgos que hayan dentro de los sistemas informáticos.

Que el derecho a hacer uso de los sistemas informáticos y que por ende nos permite tener identificación digital no debe ser suplantado, y que ante la afectación de este es el estado el que a través de los mecanismos legales está facultado en regular la conducta, ante ello es incorporar como agravante la suplantación de identidad si esta se incurra sobre Funcionario, servidor público u Autoridad representativa.

POR LO TANTO:

EL CONGRESO DE LA REPUBLICA

HA DADO LA SIGUIENTE LEY:

LEY QUE MODIFICA EL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACIÓN DE IDENTIDAD.

ARTÍCULO ÚNICO. - Modifíquese el artículo 9° de la Ley 30096, Ley de los Delitos Informáticos, el mismo que queda redactado de la siguiente manera:

Art. 9.- Suplantación de identidad

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

La pena será privativa de libertad no menor de seis ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando la suplantación de identidad

recaiga sobre Funcionario, servidor público u Autoridad representativa que afecte las funciones propias en perjuicio del Estado."

UAP UNIVERSIDAD ALAS PERUANAS

FACULTAD DE DERECHO Y CIENCIA POLITICA
ESCUELA PROFESIONAL DE DERECHO

INFORME DE OPINIÓN DE EXPERTOS DE INSTRUMENTOS DE INVESTIGACIONES CUANTITATIVAS

I. DATOS GENERALES:

1.1 Apellidos y nombres del informante: Mg. LUIS WILBERTO HERNANDEZ TORRES
1.2 Institución donde labora: UNIVERSIDAD ALAS PERUANAS
1.3 Nombre del Instrumento motivo de Evaluación: CUESTIONARIO SOBRE TIPIFICACION DE CONDUCTA DELICTIVA
1.4 Autor del instrumento: Dr. HUARMI ALBERCA VELASCO
1.5 Título de la Investigación: "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MEJOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS DE DS. 2017"

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0-16 / 01-10		BAJA 17-36 / 11-20			REGULAR 37-56 / 21-30			BUENA 57-76 / 31-40			MUY BUENA 77-100 / 41-50								
		0	16	01	10	17	26	31	36	37	46	51	56	57	66	71	76	81	86	91	95	100
		1	10	11	20	21	25	30	35	36	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado.																			X		
2.OBJETIVIDAD	Está expresado en conductas observables.																			X		
3.ACTUALIDAD	Adecuado al avance de la investigación.																			X		
4.ORGANIZACIÓN	Existe un constructo lógico en los ítems.																			X		
5.SUFICIENCIA	Valora las dimensiones en cantidad y calidad																			X		
6.INTENCIONALIDAD	Adecuado para cumplir con los objetivos trazados.																		X			
7.CONSISTENCIA	Utiliza suficientes referentes bibliográficos.																			X		
8.COHERENCIA	Entre Hipótesis dimensiones e indicadores.																			X		
9.METODOLOGÍA	Cumple con los lineamientos metodológicos.																				X	
10.PERTINENCIA	Es asertivo y funcional para la Ciencia																			X		

III. OPINIÓN DE APLICABILIDAD: ES APLICABLE

IV. PROMEDIO DE VALORACIÓN: 90%

LUGAR Y FECHA: LIMA, 20-10-2017

FIRMA DEL EXPERTO INFORMANTE
DNI ..... Teléfono .....

UAP UNIVERSIDAD ALAS PERUANAS

FACULTAD DE DERECHO Y CIENCIA POLITICA
ESCUELA PROFESIONAL DE DERECHO

INFORME DE OPINIÓN DE EXPERTOS DE INSTRUMENTOS DE INVESTIGACIONES CUANTITATIVAS

I. DATOS GENERALES:

1.1 Apellidos y nombres del informante: BARRIOS VALER, EDWIN

1.2 Institución donde labora: UNIVERSIDAD ALAS PERUANAS

1.3 Nombre del Instrumento motivo de Evaluación: CUESTIONARIO SOBRE TIPIFICACION DE CONDUCTA DOLOSA

1.4 Autor del instrumento: Bach. HUARMI ALBERCA VELASCO

1.5 Título de la Investigación: "IMPORTANCIA DE PROPONER LA MODIFICATORIA DEL ART. 9 DE LA LEY 30096 A FIN DE TIPIFICAR UNA MAYOR CONDUCTA DELICTIVA EN MATERIA DE SUPLANTACION DE IDENTIDAD EN LOS DELITOS INFORMATICOS PERU, 2017"

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje apropiado.																	X			
2.OBJETIVIDAD	Está expresado en conductas observables.																		X		
3.ACTUALIDAD	Adecuado al avance de la investigación.																		X		
4.ORGANIZACIÓN	Existe un constructo lógico en los ítems.																		X		
5.SUFICIENCIA	Valora las dimensiones en cantidad y calidad																		X		
6.INTENCIONALIDAD	Adecuado para cumplir con los objetivos trazados.																		X		
7.CONSISTENCIA	Utiliza suficientes referentes bibliográficos.																			X	
8.COHERENCIA	Entre Hipótesis dimensiones e indicadores.																		X		
9.METODOLOGÍA	Cumple con los lineamientos metodológicos.																		X		
10.PERTINENCIA	Es asertivo y funcional para la Ciencia																		X		

III. OPINIÓN DE APLICABILIDAD: EL INSTRUMENTO ES APLICABLE

IV. PROMEDIO DE VALORACIÓN: 90 %

LUGAR Y FECHA: LIMA, 20 - 10 - 2017

FIRMA DEL EXPERTO INFORMANTE

DNI: 24705026 Teléfono: 995144404