UNIVERSIDAD PRIVADA DE TRUJILLO

FACULTAD DE DERECHO

CARRERA PROFESIONAL DE DERECHO

TESIS PARA OPTAR EL TITULO PROFESIONAL DE

ABOGADO

CIBEREXTORSIÓN Y SEXTORSIÓN EN EL CÓDIGO PENAL PERUANO

AUTOR:

Bach. JOSE ALFREDO SUPO MENDOZA

ASESOR:

Mg. WALTER RAFAEL LLAQUE SANCHEZ

Trujillo – Perú

2022

HOJA D FIRMAS

PRESIDENTE

SECRETARIO

VOCAL

DEDICATORIA:

Esta Tesis esta dedicada a Dios, por dar la fuerza para continuar a pesar de las adversidades; a mi familia quienes me apoyan sin importar las circunstancias.

AGRADECIMIENTO:

Agradezco a Dios por cada día de vida, a mi familia quienes con un granito de arena han apoyado este reto académico.

INDICE DE CONTENIDOS

Páginas

RESUMEN

El presente trabajo de investigación fue desarrollado en la facultad de Derecho de la Universidad Privada de Trujillo. Su objetivo principal es determinar si es necesario regular las figuras penales de Ciberextorsión y Sextorsión en el código penal. Para alcanzar este objetivo se realizó un estudio casuístico.

El tipo de estudio es orientado al cambio y toma de decisiones, el diseño de estudio es Fenomenológico. La investigación cuenta con la variable independiente: Crimen cibernético, y la variable dependiente: Ciberextorsión y Sextorsión.

Se trabajó con un total de 12 profesionales; se ha empleado un análisis documental. El estudio permitirá entender el fenómeno social complejo que se aborda, así como comprender posibles aspectos a mejorar en nuestro ordenamiento jurídico nacional.

Se concluye que existe la necesidad de incorporar a nuestro ordenamiento jurídico penal los comportamientos de ciberxtorsion y sextorsion desarrollados a través de las nuevas tecnologías de información causando así estragos a las víctimas de esta conducta que en la presente tesis lo ha desarrollado desde su punto de vista como delito.

Palabras clave: Delito, Informático, Ciberextorsión, Sextorsión, Derecho Penal.

ABSTRACT

This research work was developed in the Faculty of Law of the Private University of Trujillo. Its main objective is to determine if it is necessary to regulate the criminal figures of Cyberextortion and Sextortion in the penal code. To achieve this objective, a casuistic study was carried out.

The type of study is change-oriented and decision-making, the study design is Phenomenological. The investigation has the independent variable: Cybercrime, and the dependent variable: Cyberextortion and Sextortion.

We worked with a total of 12 professionals; A documentary analysis has been used. The study will allow understanding the complex social phenomenon that is addressed, as well as understanding possible aspects to improve in our national legal system.

It is concluded that there is a need to incorporate into our criminal legal system the behaviors of cyberxtorsion and sextorsion developed through new information technologies, thus causing havoc to the victims of this behavior that in this thesis has been developed from his point of view. as a crime.

Keywords: Crime, IT, Cyberextortion, Sextortion, Criminal Law.

I. INTRODUCCION

1.1. Realidad Problemática

En el Perú se han reportado muchos casos con frecuencia, en donde individuos han utilizado inescrupulosamente el internet y las redes sociales para cometer un sin fin de conductas ilícitas y prohibidas.

El uso habitual del internet y las redes sociales ha dado un nuevo lugar a modernas y nuevas formas de delitos como es la "Ciberextorsión" y la "Sextorsión", que comprende el uso de mensajes de textos, correos electrónicos, páginas web en donde ha generado que los delincuentes cibernéticos consigan de mala manera información y contenidos de índole privado.

Según nuestro actual ordenamiento jurídico peruano, la constitución vigente de 1993 en el artículo 2 inciso 4 y 7 inserta como derecho fundamental protegiendo la, libertad, la intimidad y la propia dignidad personal, cualquier lesión o vulneración de estos derechos entraría a tallar el derecho penal pues este tiene como fin la protección y defensa de bienes jurídicos tutelados por el estado.

Si bien existe el tipo penal base que es la extorsión tipificada en el artículo 200 del código penal, este no es suficiente para las nuevas tecnologías en las que mediante violencia e intimidación realizan un perjuicio con carácter económico a través de medios informáticos.

En el caso de la Ciberextorsión se utilizan métodos de amenazas como virus (ransmware) donde ha evolucionado para que el usuario pague por la devolución de su información, como es el caso de grandes empresas como Adobe, Tumblr, Linkedin, Myspace y, Bitly de las que terminaron robando información como usuarios, contraseñas, fechas de nacimiento que luego fueron publicadas por un grupo de ciberdelincuentes (hackers)

en distintos sitios de Internet la cual es información importante para dichas empresas.

En el caso de la Sextorsión esta es más frecuente actualmente entre jóvenes, pues en muchos casos lo que empieza como una travesura erótica y apasionada puede convertirse en el mayor dolor de cabeza porque él envió y recepción de imágenes, cuerpos desnudos o semidesnudos, videos de contenido sexual a través de links, chats y correos electrónicos con la finalidad de amedrentar y chantajear a sus víctimas pidiéndole dinero y lucrar con este contenido privado causando un terrible daño emocional y económico.

En el Perú últimamente un caso más sonado de Sextorsión fue el de la presentadora de televisión Karen Schwartz y el cantante Ezio Oliva esta pareja afirmaron haberse grabado mientras mantenían relaciones sexuales, quienes fueron víctimas de extorsión a través de sus redes sociales, otro caso fue el de la modelo Milett Figueroa donde le pidieron dinero para no difundir la otra parte del video donde tenía intimidad con una anterior pareja, así viviendo todo un tormento.

Teniendo en cuenta los casos antes mencionados en el Perú surge la necesidad de establecer la fundamentación para tipificar las conductas “Ciberextorsión” y “Sextorsión” a fin de ser condenables penalmente, a comparación de otras legislaciones donde estas conductas son castigadas penalmente.

En una realidad como el Perú donde carece de una seguridad informática se es necesario implementar una mejor legislación con alcances y metas orientadas a la protección, prevención y a la detección de Ciberdelitos así como la identificación y realización de sus actores, creando grupos especializados en la materia que sean capaces de administrar y preservar la Ciberseguridad en el Perú.

Esta nueva corriente en delitos de cibernéticos crea un ambiente en el que jurídicamente es necesario efectuar los mecanismos de control, buscando reducir el impacto negativo dentro de la sociedad reduciendo las pérdidas económicas en una posible situación de ataques y quebrantamientos de derechos.

1.2. Formulación del problema:

¿De qué manera la tipificación del delito de "Ciberextorsión" y "Sextorsión" en el código penal peruano reduciría el índice de crimen cibernético?

1.3. Justificación

La tesis de investigación se justifica en una realidad actual y moderna en el Perú en el tema de delitos contra la privacidad, intimidad y la libertad sexual "Ciberextorsión" y "Sextorsión", porque en nuestra realidad nacional y actual es común en adultos, jóvenes y adolescentes que pueden obtener de una manera muy fácil imágenes, y videos íntimos cuyo material puede llegar a las redes sociales de mayor uso y públicos como es Facebook, Whatsapp y Instagram produciendo así daños, incalculables e irreversibles en la persona es por ello que este tema es muy interesante para poder regularizarlo en nuestro ordenamiento jurídico penal ya que se ven videos e imágenes íntimos que se exhiben en las redes sociales y lamentablemente no existe una regulación normativa debido a que es un fenómeno nuevo y actual que aparece con el avance de nuevos medios de acceso a información tecnológica.

Se justifica en su importancia jurídica se motiva en el hecho de proteger derechos fundamentales como la privacidad, la información personal y la intimidad personal, también la dignidad de la persona con la finalidad de lograr una seguridad jurídica y un fortalecimiento y amparo del derecho ante nuevas amenazas de ciberdelitos y la otra necesidad de buscar un reconocimiento en la regulación jurídica peruana otorgando medios de

protección y defensa a las personas que sean blancos de estos nuevos delitos que se perpetran a través de las redes sociales y el internet y los diferentes medios que con el tiempo puedan aparecer en el mundo.

Es de importancia el desarrollo de este proyecto, debido a que esta nueva modalidad de delitos es constante por no estar correctamente señalado y tipificado en el Código Penal Peruano. Este trabajo se justifica en la necesidad de imponer estos nuevos tipos penales debido al mayor uso de nuevas tecnologías mediante la red que permiten cometer nuevos delitos cibernéticos y en donde las victimas sociales no tengan la suficiente protección jurídica ante una inminente necesidad de penalizar.

1.4. Objetivos

1.4.1. Objetivo General:

Determinar si es necesario regular las figuras penales de Ciberextorsión y Sextorsión en el código penal.

1.4.2. Objetivo Especifico:

a. Estudiar los supuestos delictivos de Ciberextorsión y sextorsión.
b. Determinar las ventajas que tiene la implementación en el código penal las Ciberextorsiones y Sextorsiones.
c. Proponer una inserción del tipo meramente penal relacionado a la Ciberextorsión y la sextorsión.

1.5. Antecedentes.

Internacional

Soto, Sique (2012). "Necesidad de monitorear legalmente los teléfonos móviles de menores de edad en cumplimiento con el artículo 59° del decreto 27-2003 para evitar el sexting", presentada en la Universidad de San Carlos – Guatemala, tesis presentada en la Universidad Nacional Federico Villareal, para obtener el grado de Licenciado en Ciencias Jurídicas y Sociales, la cual conlleva a la siguiente conclusión: una nueva tendencia que ocurre frecuentemente entre adolescentes llamada "sexting" es un inmenso y moderno problema social en

los adolescentes y en el sistema de telefonía móvil del mismo país, si bien afirma el autor de esta tesis que existe un acaparamiento de las grandes empresas de telefonía móvil e internet, estas empresas en todo el país brindan sus servicios, pero no se brinda una suficiente seguridad a los clientes, generando incertidumbre en estos y existiendo una insuficiente supervisión con respecto a los servicios de estas empresas de telefonía, ya que al enviar correos electrónicos y mensajes no se brinda la suficiente supervisión y generando en los usuarios incertidumbre por la empresas prestadoras de servicios de telefonía y de internet en Guatemala donde se presenta y pone en práctica el "sexting" esta práctica inmoral al recibir imágenes y videos de muy alto contenido sexual se encuentran inmersos los adolescentes a estas prácticas que perturban sus mentes y se afecta la privacidad debido a las prácticas sexuales que los adolescentes utilizan con frecuencia estos pues como se menciona no existe un suficiente control y mucho menos una regulación legal que trae consigo consecuencias económicas, jurídicas y principalmente para la sociedad.

Nacional

Morí Quiroz, Francisco (2019). "Los Delitos Informáticos y la Protección Penal de la Intimidad en el distrito judicial de Lima, periodo 2008 al 2012", tesis presentada en la Universidad Nacional Federico Villareal, para obtener el grado de maestro en Derecho Penal, en esta se elaboraron las siguientes conclusiones: Es una labor de los operadores jurídicos la de brindar una protección penal al bien jurídico que es la intimidad en todos sus ámbitos, también precisa que existe un desconocimiento por parte de los magistrados y fiscales en temas de los delitos informáticos existiendo así un desacierto por parte de los operarios de justicia en la investigación y en el juzgamiento en donde estos requieren una especialización en delitos informáticos para una mejor competitividad y funcionamiento de los mismos, también está en desacuerdo con la inapropiada delimitación del daño causado pues esta es insuficiente para reparar el daño por lo que existe una indebida valoración en el cálculo del monto indemnizatorio por parte de los operadores de justicia.

1.6. Bases Teóricas

CAPITULO I

DELITOS INFORMATICOS

1. Antecedentes

Nuestro Perú de una extensa área industrializada, acumula un importantísimo sector de nuestra población dedicado a la administración pública; el cual debe encontrarse capacitado en el uso computadoras, porque esta es una herramienta indispensable para el funcionamiento de la administración publica en instituciones estatales como privadas.

Actualmente en el mundo globalizado donde nos encontramos a la informática que hoy en día es un instrumento indispensable para el correcto funcionamiento de las instituciones estatales como lo precisa (Marilina, 2013) "Los avances de las tecnologías de la información y el crecimiento constante de las operaciones comerciales mediante un medio electrónico han propiciado el surgimiento de nuevas conductas fraudulentas relacionadas con el uso de instrumentos electrónicos". De lo acotado se desprende que el constante avance de la tecnología ha propiciado el nacimiento si se podría decir así de nuevas conductas ilícitas que son cometidas a través de instrumentos tecnológicos.

Para el criminólogo y jurista (Jose, 2014) las primeras bases de los estudios sobre los delitos informáticos fueron hechas en la década de 1970, estos estudios permitieron sacar a la luz un mínimo número de nuevos delitos, pues en esos tiempos todavía el uso de computadoras no era tan frecuente y es por eso que un gran número de estos delitos que todavía no se descubrían. La perspectiva acerca de los nuevos delitos informáticos cambio de raíz en los ochenta, una amplia ola de piratería de software, manipulación de cajeros automáticos y abusos de las telecomunicaciones revelo la fragilidad de la sociedad de la información y la obligación de crear nuevas estrategias de control de estos delitos.

En nuestra actualidad no se puede obviar la existencia de delitos cometidos mediante el uso de sofisticadas herramientas informáticas, es por ello que deviene una problemática más aun en el derecho, pues se busca estructurar un nuevo bien jurídico digno de una tutela jurídica penal, ya sea por su valor económico o por su valor informacional.

En este contexto globalizado provoca un surgimiento de nuevos hechos ilícitos que vulneran bienes jurídicos en donde se realiza con la manipulación de instrumentos tecnológicos poco comunes. La nueva regulación jurídica sobre la criminalidad cometida por ordenadores es de carácter propio en innovador.

2. Conceptualización

Es de suma importancia conocer diferentes conceptos de autores que hacen mención a los llamados delitos informáticos, es por ello que la doctrina ha formulado diversos conceptos a continuación citare algunos autores que conceptualizan los delitos informáticos:

(Viega, 2003) “Define a los delitos informáticos como: toda acción típica antijurídica y culpable para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma”. En concepto se busca definir al delito informático como una conducta contraria al ordenamiento jurídico en donde se utiliza la computadora como única vía para su perpetración.

(Davara Rodríguez, 2008) Señala que “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”. Este autor y para mi preferencia es el que mejor conceptualiza el delito informático porque lo define como un delito cometido por una computadora o medio tecnológico donde implica su software como su hardware.

En conclusión los delitos informáticos vendrían a ser todo comportamiento o hecho ilícito que en su perpetración hace uso indebido de la tecnología electrónica ya sea como un fin o medio, para llevarlas a cabo, pero existen muchos delitos que no pueden penalizarse con las leyes actuales por la ausencia de un reglamento o por la falta de regulación en algunos países.

3. Características

Paso ahora a mencionar las características del delito informático:

1) Son conductas ajenas al derecho y solo una persona con conocimientos técnicos es el que puede llegar a cometerlas.

2) Puede provocar un gran perjuicio económico.

3) Sin alguna presencia física puede llegar a cometerse en lapsos muy reducido de tiempo y espacio.

4) Muy sofisticados.

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

6) Se ofrecen facilidades para su comisión en los menores de edad.

7) Tienden a esparcirse cada vez más, por lo que requieren una urgente normatividad y regulación

4. Tipos

Los tipos más comunes de delitos cometidos mediante manipulación de computadoras son:

4.1. Manipulación de los datos

Este fraude informático conocido también como sustracción de datos, representa el delito informático más común y simple, ya que es fácil de cometer y difícil de descubrir. Este nuevo delito no requiere de conocimientos

técnicos de informática y puede realizarlo cualquier persona que tenga libre acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

4.2. Manipulación de programas

Es muy difícil de descubrir y a diario pasa por inadvertido debido a que el delincuente debe tener conocimientos técnicos de informática. Este delito consiste en modificar los programas ya preexistentes en el sistema de computadoras o en insertar nuevos software o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en incluir instrucciones en una computadora de forma encubierta mediante un programa informático para que pueda realizar una función no autorizada y al mismo tiempo todo funcione con normalidad.

4.3. Manipulación de los datos de salida

Este tipo de delito se perpetra limitando un correcto funcionamiento de un sistema. Los casos más comunes es el que se presenta en los cajeros automáticos mediante la falsificación de instrucciones en la adquisición de datos.

4.4. Fraude

Es efectuado por manejo informático en donde se aprovecha las reproducciones de los procesos en los sistemas de computadoras. Esta técnica es muy especializada pues se requieren niveles sofisticados de en conocimiento de sistemas y entre las técnicas sofisticadas tenemos “la técnica salchichón” que opera en donde las transacciones financieras se sacan de una cuenta y se transfieren por arte de magia a otra cuenta.

4.5. Virus

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus se puede

ingresar en un sistema, por un conducto de una pieza legítima de soporte técnico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

4.6. Gusanos

Se fabrica de forma igual al virus con miras a infiltrarlo en programas verdaderos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus, porque no puede regenerarse. En términos de medicina se podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno.

4.7. Bomba lógica o cronológica

Este tipo de delito exige conocimientos especializados, ya que se requiere la programación de la destrucción o modificación de datos, en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas binarias son las que poseen el máximo potencial de hacer daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar el lugar en donde se halla la bomba lógica.

4.8. Piratas informáticos o hackers

A menudo en la red suele existir con frecuencia usuarios que valiendo de cualquier medio de comunicación o sistema informático se aprovecha de la falta de seguridad y obtiene accesos a diferentes sitios web en el internet o en la red en donde comúnmente emplean contraseñas comunes o que están en el propio sistema.

4.9. Reproducción ilegal de programas informáticos

Esta actividad es la más ilegal e incluso es sancionada penalmente y consiste en reproducir o copiar programas o cualquier tipo de software patentado de una manera desmesurada e ilegal sin el consentimiento de autor a través del internet.

5. Bien jurídico

Para (Salinas, 2006) comentando el Código Penal 1991 así como sus posteriores reformas en el que el legislador progresivamente ha incluido los delitos informáticos en el Código Penal. Este problema subyace en el interés que el legislador ha optado por configurar una nueva protección sobre bienes jurídicos ya existentes (por ejemplo, el patrimonio, la intimidad y otros).

CAPITULO II
DERECHO A LA INTIMIDAD

1. Definición

Para el jurista peruano reconocido internacionalmente (Espinoza Espinoza, 2011) "El Derecho a la Intimidad es una situación jurídica en la que se tutela el espacio individual y familiar de privacidad de la persona". Es por ello que el derecho que el derecho a la intimidad busca mantener una vida en completa privacidad, sin ser molestado en los diferentes aspectos de la vida.

También se reconoce en el derecho a la intimidad que comprende un conjunto de actos o circunstancias de carácter privado que no son expuestos al dominio público, esta es conocida como "la esfera íntima", e involucra una serie de situaciones personales y familiares propio de la libertad del individuo en donde no se debe alterar un mucho menos causar perturbaciones por personas ajenas o terceros.

Siguiendo nuestra legislación nacional el artículo 14 del código civil acota que: "La intimidad de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésta ha muerto, sin el de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en este orden".

Con este presupuesto se conoce que la intimidad es solo la parte interior del individuo que cada uno conoce y que por ende debe defenderse ante cualquier divulgación de hechos por tener el carácter de índole privado, siempre salvaguardando la tranquilidad de la persona.

Sin más remedio lo íntimo de cada persona no puede ser revelado salvo un consentimiento tácito de la misma persona que quiere que se sepa lo más íntimo y privado, en los caso de los personajes públicos, ellos también tiene derecho intimidad aunque su vida aparenta ser pública, son cosas inherentes

a la persona producto de la liberalidad que con mucho esfuerzo se ha venido desarrollando y amparando a través del tiempo en nuestra legislación.

En nuestra realidad peruana el derecho fundamental a la intimidad está reconocido constitucionalmente en el Perú. Amparando la protección de suministrar información personal que afecte la intimidad por parte de las personas, los nuevos avances tecnológicos contrasta una afectación al derecho en la intimidad respecto a los sistemas informáticos en un mal uso de estos.

2. Protección de la intimidad

En el Perú la constitución de 1993 acota artículo 2 inciso 7 que "toda persona tiene derecho a la intimidad personal y familiar" sin embrago existe una confrontación con otro derecho reconocido que es el de la información. Pero lo que ocurre en el caso en concreto, es que los mecanismos para proteger la intimidad, mediante la forma del control social han sido superados por las nuevas tecnologías así ocurre de modo indirecto sin conocimiento y con consentimiento del titular de la información.

Ante el conflicto de la información vs la intimidad se ha delimitado unos contornos de los mencionados derechos: espacial, subjetivo y objetivo. Cuando hay una diferencia entre las personas públicas y privadas es de carácter subjetivo, cuando hay diferencias entre conductas públicas y privadas se habla de un carácter subjetivo, el espacial es cuando se reconocen espacios propios, exclusivos y comunes.

En este caso la intimidad con la información personal deben estar equilibrados frente a los intereses de los individuos de los demás y del estado, para ello es indispensable que la legislación precise algunos limites en la defensa de los derechos del ciudadano, no pudiendo invadirse la intimidad y el derecho a la información por razones de seguridad.

También es bueno precisar el delito de violación a la intimidad es protegido por nuestro ordenamiento jurídico el cual abarca la vida personal y familiar.

3. Intimidad y su relación con la informática

Para (Frosini, 2000) establece: “La informática en el mundo globalizado es un instrumento mecánico que ofrece registros de información en archivos mecanográficos”.

La esencia radica en la informática en la cual se necesita una maquina automatizada influenciada por un individuo. Es el caso de las nuevas tecnologías que ante este hecho el derecho no se ha logrado adaptarse a este fenómeno tecnológico que ha producido un cambio social. Las diferentes modalidades en este campo han generado un abuso y la mala utilización de los medios informáticos requiriéndose así una protección penal.

La informática sirve como medio para cometer el delito en agravio del bien jurídico de la intimidad, este mal uso de los medios tecnológicos ha generado una serie de comportamientos desconocidos entre los más usuales tenemos el pishing y el hacking en donde engañan a los usuarios con software en donde se recoge los datos personales y sensibles en donde su móvil siempre es de carácter económico.

La ley 30096 propia de los delitos informáticos se promulgo en el Perú en cual busca sancionar las conductas donde utiliza las tecnologías de la información promoviendo la protección de los bienes jurídicos en diferentes modalidades.

Como manifiesta (Villavicencio Terreros, 2014) “Esta ley no responde solo a la necesidad de ejercer la función punitiva del estado enfocado en la protección de la información, si no que su objetivo principal es la estandarización de la ley penal peruana con el ordenamiento penal internacional (Convenio de Budapest). Con respecto a la ley regula los delitos informáticos contra la intimidad y el secreto de las comunicaciones es la estandarización del derecho nacional con el derecho internacional buscando siempre ese enfoque de protección y de tutela de los bienes jurídicos en delitos perpetrados a través de computadoras y del internet.

4. Datos personales

A nuestra definición datos personales es esa información grabada en lenguajes informáticos sobre cualquier aspecto de nuestra vida, como salud, costumbres, hábitos sexuales, ideas políticas, religión, aspectos sociales, u otro cualquier aspecto de la vida.

(Gonzáles Mantilla, 1993) “Como se sabe, el poder es un fenómeno general y común a todos los ámbitos de la sociedad, es la capacidad de acción, de obligar, de dirigir, de conducir”.

Este autor menciona al poder informático que tiene sobre la sociedad en donde se ve reflejado en la cantidad de información que puede tener un individuo con acceso a bases de datos o de medios tecnológicos la cual está debidamente organizada y no se debe ser difundida al exterior.

En el Perú los datos personales son “Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados”.

Los datos personales en respecto a la esfera íntima es la información propia para uno mismo, que con el avance de la tecnología se hace cada vez “más accesible” y por tanto vulnerable ante posibles ataques.

5. Datos sensibles

La intimidad, estaba caracterizada por poseer un matiz individualista, a tener un área reservada fuera del alcance de terceros, lo que hoy es prácticamente imposible mantener, desde la concepción nuestra información íntima o sensible circula en bases de datos y redes de información, pongamos el ejemplo de las ecografías compartidas por las madres gestantes en la redes sociales.

Los datos sensibles son aquellos que caracterizan únicamente a una persona cuyo contenido es de personalísima titularidad del que los genera. Pero existe un conjunto de datos sensibles que por su condición especial son de mayor importancia que otros como, por ejemplo, el nombre, la edad, el número de DNI, entre otros, nos estamos refiriendo a los datos meramente sensibles.

En el Perú los Datos Personales son: “Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; ingresos económicos, convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual”. Como se evidencia los datos sensibles son los que están más relacionados con el contenido íntimo personal que se maneja hoy en día.

CAPITULO III
SEXTORSION

1. Definición

Si bien no está acuñado el término “Sextorsion” o está relacionado al chantaje sexual cibernético o en países de habla inglesa se le conoce como “Sex Extortion”. En definitiva consiste en realizar una amenaza o chantaje o extorsión en donde la víctima es obligada a enviar imágenes en situaciones eróticas, o manteniendo relaciones sexuales, materializándose con la puesta en circulación de este contenido sexual por parte del chantajista.

El chantaje se realiza a través del internet en sitios web de contenido erótico o sistemas de información (redes sociales) esta práctica es la más frecuente porque ocurre en computadoras o en celulares y mayormente el chantajista utiliza un gado de anonimato a la hora de chantajear mediante estos medios de comunicación.

2. Tipos

Para los tipos de sextorsión pueden ser:

- Por medio de imágenes o videos producto de una relación sentimental.
- Por medio de imágenes en pleno acto sexual en donde el chantajista es un ex pareja o amantes.
- Por medio de imágenes obtenidas por chat eróticos a través de videocámaras.

Este chantaje siempre va a requerir un material de índole sexual, cualquier imagen o video en actos sexuales que normalmente la persona chantajeada brinda al chantajista o este las obtiene por astucia o por otro medio.

En el caso de imágenes o de videos sexuales este puede haberse producido por un sexting en el cual se intercambió el contenido sexual y es por ello que

se utiliza para chantajear pidiendo dinero o incluso relaciones sexuales y en caso de incumplimiento estas serán expuestas a través del internet.

3. Sexting

Para (María, 2011) “Es la unión de dos términos ingleses: sex (sexo) y texting (envío de mensajes de textos)”. Siguiendo este dos términos se puede precisar que es todo envió de mensajes de texto con un contenido sexual, pero con la llegada del celular actualmente ha procurado que esto se envié a través de estos aparatos tecnológicos en donde se tome fotografías o videos con contenido sexual que permiten las nuevas tecnologías.

Por lo general este tipo de conductas es cometido a través de un dispositivo móvil, el problema de este tipo de conducta es que la difusión de imágenes o videos sea no consentida por la parte que no consintió la difusión del contenido a través del internet.

4. Tipos de sexting

En nuestro estudio de investigación podemos encontrar dos tipos de sexting:

El sexting Activo: Consiste en donde el individuo a si mismo realiza posturas provocativas y se materializa mediante fotos y videos.

El sexting Pasivo: Es el que consiste en donde el individuo recibe el material intimo o las imágenes y se queda solo en su entorno no se expande ni mucho menos se hace de conocimiento público.

CAPITULO III
CIBEREXTORSION

1. Ciberextorsión

Conocido también cómo extorsión cibernética en qué consiste en exigir una cantidad de dinero pode valor a cambio de no llevar acabó amenazas de cometer daños en sistemas de información generando un nuevo problema para la sociedad. Es necesario precisar que existe una escasez de doctrina jurídica sobre el tema de la ciberextorsión, pero esta figura con el paso del tiempo y de las nuevas tecnologías ha ido mejorando inflando cada vez técnicas más sofisticadas con un afán de generar más dinero.

Este delito opera mediante ciberextorsionadores los cuales ocultan su identidad para adueñarse u obtener información de forma fraudulenta mayormente de empresas utilizar este información para chantajear a su víctima en pocas palabras secuestran información de su víctima.

2. Pishing

Este delito es conocido como la estafa cibernética se piensa de que éste es uno de los delitos cibernéticos qué más se cometen hoy en día esta acción consiste en generar un fraude informático en dónde mediante engaño y haciendo en incurrir en error a la víctima utilizando un medio tecnológico con un animus de lucro y de perjuicio patrimonial es donde se realiza el famoso pishing.

Esta modalidad en cuestión consiste en duplicar una página web, un usuario de esta página web que la visita genera en él un error al creer que se encuentra en el sitio web verdadero y es en donde la víctima ingresa datos usuarios y contraseñas con el fin de realizar un acceso un acceso a esta web. En la cual la página web engañosa ofrece servicios de compras Esto con un claro fin que la víctima consigne sus datos en el sitio web mayormente de compras ingrese su tarjeta de crédito y demás datos filiatorios para que luego de ello usando

maniobras tecnológicas y operaciones vía internet se aprovechen de estos datos y causen un perjuicio patrimonial.

En él código Penal español En el artículo 248 incisos 2ª. establece: “Cometen estafa los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro." El derecho español relaciona el delito de pishing con la estafa siendo la primera una modalidad y la conducta es la misma en la que un sujeto mediante una manipulación informática o sistema de red se apodera de bienes de otros así generando un perjuicio económico. Esta nueva figura lo que pretende es proteger el patrimonio frente a las nuevas tecnologías qué propicia ataques o transferencias in consentidas de patrimonio y qué provoca un lucro a la persona que causó este perjuicio es imprescindible que El engaño es el que juega una función importante en este tipo de delitos.

3. Modalidad

La modalidad en el delito de pishing normalmente página web de bancos en donde se hace creer al visitante que se encuentra en la página original siendo esto un duplicado de la página verdadera en la que el usuario accede a esta página introduciendo sus datos induciendo a error al visitante. Es comúnmente que en estos sitios se introduzca nombres y contraseñas para tener acceso a las famosas bancas móviles y de este modo como ya dije antes obtener un beneficio económico.

En la vía del delito de pishing lo más usual es la suplantación de una persona jurídica o física siendo el primer paso el spam qué es el mensaje qué se le envía a la víctima con la intención de qué sujeto pasivo entré a una web falsa en la cual es infectado de un virus y le obligue a revelar sus datos.

4. Hacking

El hacking consiste en una acción qué es llevada a cabo por un ciberdelincuente con un ánimo infiltración, esta conducta es desarrollada a

través de las nuevas tecnologías y con rasgos meramente técnicos. Proceso llevado de manera individual, este experto utiliza una computadora y un módem y en el cual es capaz de descubrir grandes sistemas informáticos de entidades públicas y empresas privadas. El Acceso ilegal a la información actualmente es una conducta perseguible en varias legislaciones del mundo la nuestra no es ajena Pues también ha decidido tipificar en una ley especial sobre delitos informáticos salvaguardando en primer lugar la propiedad intelectual y los recursos de información.

5. Ciber terrorismo

En la actualidad nuevas conductas surgen para el derecho penal que tienen que ver con el acceso a redes de información y con la violación de algunos derechos no obstante se crea una nueva forma de delito es del ciber terrorismo y ópera con la construcción de una bomba o de armas en el cual se viola los sistemas de seguridad y programas para controlar bases de datos mayormente del estado.

Con la facilidad hoy en día las instituciones prestan servicios a la comunidad mediante la red, terroristas cibernéticos aprovechan estas circunstancias para planear operaciones y desarrollar sus objetivos. Para Luciano Salellas "El ciberterrorismo es la acción violenta que infunde terror realizada por una o más personas en Internet o a través del uso indebido de tecnologías de comunicaciones". Esto representa pánico ante un evidente manipulación de banco de datos y de amenazas contra la seguridad personal y nacional también hace referencia a la utilización de computadoras para la obtención del propósito político y así amparar sus acciones bajo la violencia de propósitos terroristas. Esto significa ataques ilegales contra computadoras con el fin de coaccionar a un gobierno y qué puede producir violencia contra las cosas que generan temor y mayormente conducen a las pérdidas económicas.

1.7. Definición de Términos Básicos

Derecho a intimidad

Es un derecho derivado de la libertad y de forma personal e inherente al ser humano como tal el cual protege el bien más profundo de una persona, de lo que protegería el derecho a la intimidad así también hace mención a la privacidad de los bienes que son productos de la custodia de este derecho entre ellos la reputación, la honra y el domicilio este último el más íntimo y privado.

Derecho informático

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

Delitos informáticos

Principio por el que toda persona debe ser considerada como inocente mientras no se haya demostrado su culpabilidad en sede judicial.

Sextorsión

Acuñado para una de las nuevas formas de chantaje sexual a través de la red donde bajo amenaza la victima publica o envía imágenes de contenido sexual o semidesnudos donde se muestra una actitud erótica o de lo más clásico manteniendo relaciones sexuales que exhiben y ponen en circulación en la redes y el internet bajo amenaza.

Ciberextorsión

Trastorno psicológico por el cual un menor de edad, a causa de la programación recibida por el padre titular de su tenencia, insulta y denigra al progenitor que no convive con él, sin que existan razones objetivas que justifiquen su comportamiento.

1.8. Hipótesis:

Planteamiento de la hipótesis:

Los fundamentos jurídicos que permite tipificar penalmente los delitos de Ciberextorsion y la Sextorsion penalmente en el Perú son la protección al derecho constitucional a la información privada, a intimidad personal en el Perú.

1.9. Variables:

Variable independiente:

Crimen cibernético

Variable dependiente:

Ciberextorsión

Sextorsión

II. MATERIALES Y MÉTODOS

2.1. Materiales

DESCRIPCIÓN	UNIDAD	CANTIDAD
Papel bond A4/75g	Millar	3
Lapicero	Unid.	2
Memoria – USB	Unid.	2
Lápiz	Unid.	10
Borrador	Unid.	10
Tajador	Unid.	2
Corrector	Unid.	5
Regla	Unid.	2
Engrapador	Unid.	1
Perforador	Unid.	1
Folder Manilla A4	Unid.	25
Clips x 200 unidades	Ciento	2
Grapas Estándar 26/6	Millar	1
CD’s	Unid.	10
Computadora y equipos periféricos	Unid.	1
Fotocopias	Millar	5
Impresión	Millar	2
Internet	Mes	4
Empastado	Unid.	2

2.2. Material de estudio

2.2.1. Población

Según la plataforma INE (s/f) define a la población como el conjunto de personas que habitan una determinada área geográfica.

En estadística, según la plataforma de Educación Recursostic (s/f) la define como un conjunto de todos los elementos que verifican una característica que será objeto de estudio.

En esta presente tesis, la población está comprendida por abogados de Trujillo.

2.2.1.1.Muestra

Según Lalangui (2017) precisa que la muestra es la parte de la población que se selecciona para la obtención de la información. En ella se realizará las mediciones u observaciones de las variables de estudio.

En la presente tesis, la muestra está conformada por lo siguiente:

TECNICAS	UNIDAD	S.S	POBLACIÓN	MUESTRA
Análisis documental Fichaje de materiales	Abogados	12	12	12
		TOTAL	**12**	**12**

2.3. Técnicas, procedimientos e instrumentos.

2.3.1. Para recolectar datos

Tabla N°01

Técnicas e instrumentos del Análisis documental

Técnicas	Instrumentos
Análisis documental	Fichas de análisis del marco teórico, de la legislación, doctrina y jurisprudencia

Fuente: Investigación propia

Elaborado por: Jose Alfredo Supo Mendoza.

2.3.2. Para procesar datos

Siendo la finalidad realizar el análisis de la información obtenida, se realizó un estudio inicial de las respuestas obtenidas por los profesionales involucrados, a fin de poder determinar las definiciones más pertinentes y significativas, respecto al clima organizacional, de acuerdo a las categorías señaladas.

III. RESULTADOS

Analizaré entrevistas aplicadas a doce (12) abogados que ejercen en el ámbito de Trujillo.

PREGUNTA N° 01

Dr. ¿Cuáles son los fundamentos jurídicos que protegen la publicación de imágenes, audios videos íntimos conocido como sextorsión en las redes sociales? Es decir ¿cuáles son las normas que regulan el derecho a la intimidad y si es suficiente o existe la necesidad de tipificar el "sextorsión"?

¿EXISTE UNA NECESIDAD DE TIPIFICAR LA SEXTORSION?		
RESPUESTA	**ENTREVISTADOS**	**PORCENTAJE**
SI	08	67 %
NO	04	33 %
TOTAL	**12**	**100 %**

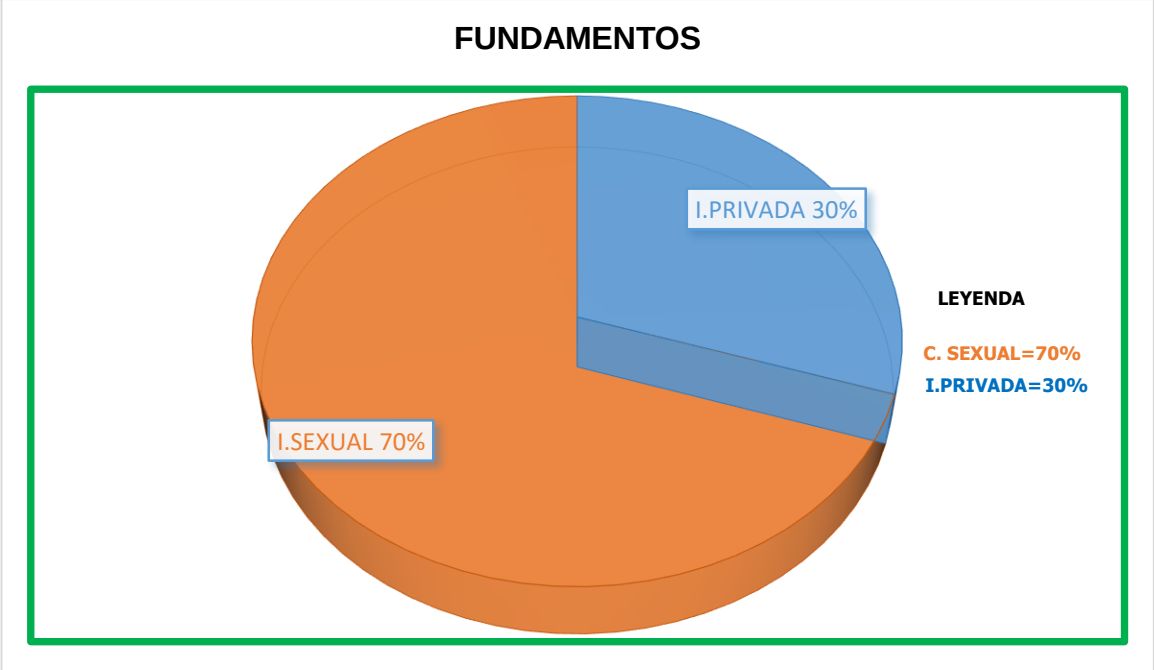
Fuente del cuadro: Elaboración propia

Obtenido el resultado de los encuestados y haber explicado cómo opera la ciberxtorsion y sextorsion, entre este grupo de Jueces, Fiscales, Abogados defensores, consideraron que si existe una necesidad de tipificar estas conductas. Siendo este resultado de un 67% a favor el que si considera su tipificación, y un 33% que no se encuentra a favor.

FUNDAMENTOS JURIDICOS QUE PROTEGEN LA PUBLICACIÓN DE IMÁGENES, AUDIOS VIDEOS ÍNTIMOS CONOCIDO COMO SEXTORSIÓN EN LAS REDES SOCIALES				
FUNDAMENTOS	**ENT.**	**%**	**∑**	**%**
El contenido de índole sexual sin autorización	05	60%	08	100%
Información Privada	03	40%		

Fuente del cuadro: Elaboración propia

Los entrevistados dieron a conocer sus diferentes puntos de vista, sobre cuál sería el fundamento jurídico que protege la publicación de imágenes, audios, videos íntimos, conocido como sextorsion, siendo uno de ellos la propagación de contenido sexual sin autorización, y el otro la información de índole privada.



Fuente del cuadro: Elaboración propia

Conforme indica el grafico en las entrevistas el 70% de la población entrevistada índico que el fundamento para el cual debería tipificarse es la propagación del contenido de índole sexual sin autorización, el cual puede ser audios, imágenes, videos etc. El otro sector de la entrevista considero que el fundamento seria la información propagada de carácter privado del contenido imágenes o videos, pues debería ser un poco más amplio y no solo bastaría con la difusión de contenido sexual sin autorización.

PREGUNTA N° 02

Para Ud. considera se debería penalizar "ciberextorsión y sextorsión"? a esto me refiero a que debería considerarse como un delito y cual serían sus fundamentos para considerarse como tal?

¿EXISTE UNA NECESIDAD DE PENALIZAR LA CIBERXTORSION Y SEXTORSION?		
RESPUESTA	**ENTREVISTADOS**	**PORCENTAJE**
SI	07	67 %
NO	03	33 %
TOTAL	**08**	**100 %**

Fuente del cuadro: Elaboración propia

En la siguiente controversia se analizó si se debería penalizar la ciberxtorsion y la sextorsion, se determinó que un 67% considera que debería penalizarse la ciberxtorsion y la sextorsion, siendo este un grupo mayoritario. La otra parte de entrevistados determino en un 33% que no debería penalizarse pues no existe una debida de necesidad y los comportamientos encuadrarían en otros tipos penales.

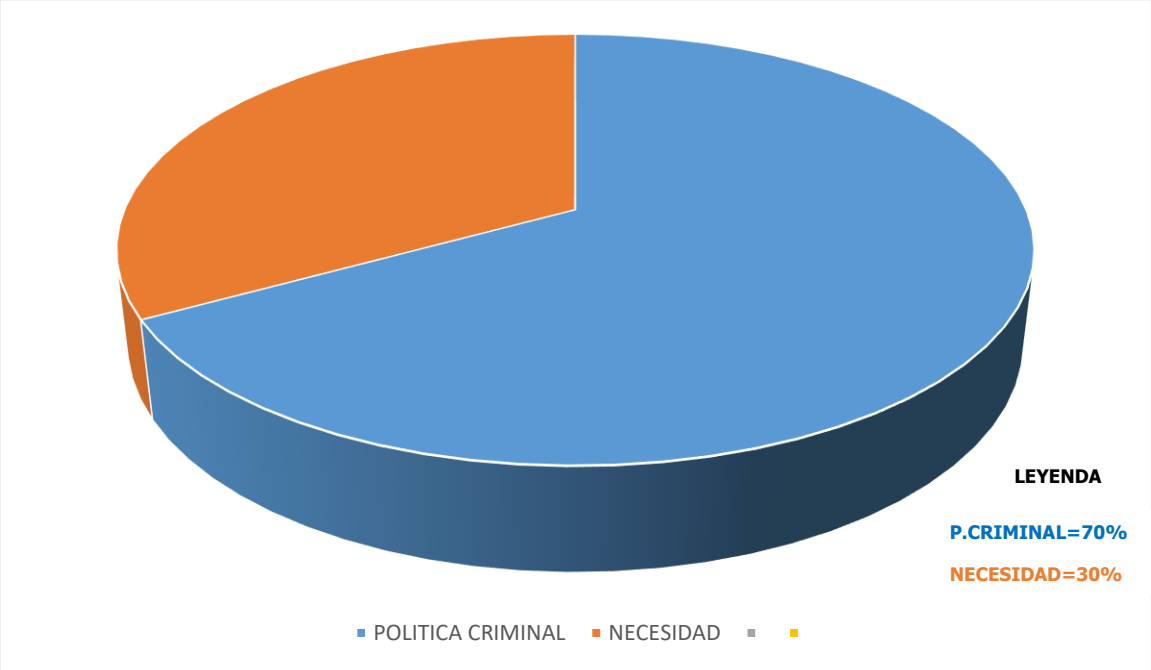
A continuación al grupo mayoritario a favor se continuó a preguntar las razones por la cual considera que debe penalizarse los delitos de ciberxtorsion y sextorsion.

¿EXISTE UNA NECESIDAD DE PENALIZAR LA CIBERXTORSION Y SEXTORSION?				
FUNDAMENTOS	**ENT.**	**%**	**∑**	**%**
Política criminal	05	67%	07	100%
Como necesidad	02	33%		

Fuente del cuadro: Elaboración propia

En el cuadro los entrevistados consideraron que los fundamentos para penalizar este tipo de delitos son la política criminal y la necesidad que existe para estos tipos de conductas, obteniendo como resultado un 67% que considera que es de política criminal pues se considera un comportamiento completamente reprochable, y otro

sector un 33% que considera que es una necesidad pues se vulneran bienes jurídicos fundamentales.



Fuente del cuadro: Elaboración propia

PREGUNTA N° 03

Si Ud. ¿consideraría el ciberextorsión y sextorsión como una agravante o como delito específico en el código penal?

En la siguiente controversia se proseguío a determinar si debería considerarse la ciberxtorsion o sextorsion como delito propio o como un agravante en algún tipo penal.

¿CONSIDERA LA CIBERXTORSION COMO AGRAVANTE O DELITO?		
RESPUESTA	**ENTREVISTADOS**	**PORCENTAJE**
DELITO ESPECIFICO	04	67 %
AGRAVANTE	03	33 %
TOTAL	**07**	**100 %**

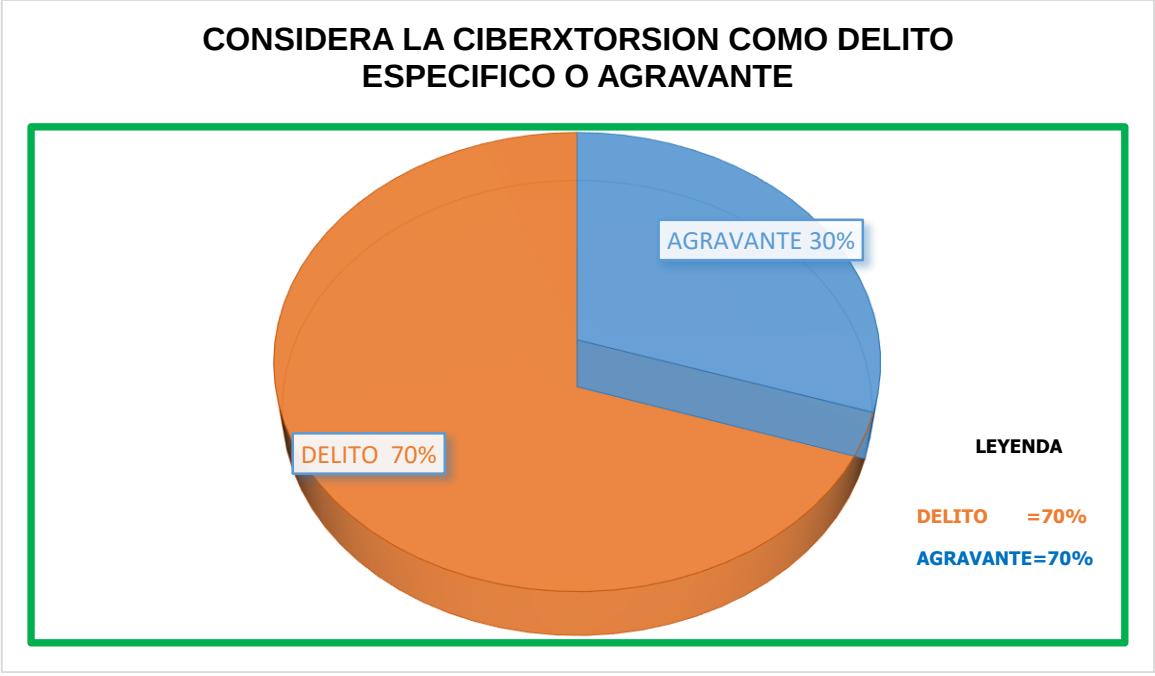
Fuente del cuadro: Elaboración propia

Teniendo como respuesta en el público entrevistado que un 67% de la población considera que debería ser un delito específico en el código penal, la otra parte un 33% considero que debería ser un agravante del tipo penal de extorsión pues las circunstancias al momento de perpetrar dicho comportamiento utilizando medios informáticos para la ejecución material determinaría un agravante para este tipo penal.

¿CONSIDERA LA CIBERXTORSION COMO AGRAVANTE O DELITO?				
FUNDAMENTOS	**ENT.**	**%**	**∑**	**%**
Delito Especifico	05	67%	07	100%
Agravante	02	34%		

Fuente del cuadro: Elaboración propia

De este resultado podemos resaltar que existe un intervalo de 34% en diferencia del 67% que se encuentra a favor que la ciberextorsión se considere como delito específico, de pequeño grupo de 33% que considera que debería ser un agravante del tipo penal de extorsión.



Fuente del cuadro: Elaboración propia

PREGUNTA N° 04

En cuanto a los fundamentos jurídicos, es decir en el código penal ¿qué es lo que acarrearía la ciberxtorsión y sextorsión en caso de no ser penado?

¿QUE ACARREARIA LA CIBERXTERSION Y SEXTORSION EN CASO DE NO SER PERNADO?		
RESPUESTA	**ENTREVISTADOS**	**PORCENTAJE**
UNA VULNERACION	03	33 %
IMPUNIDAD	04	67 %
TOTAL	**07**	**100 %**

Fuente del cuadro: Elaboración propia

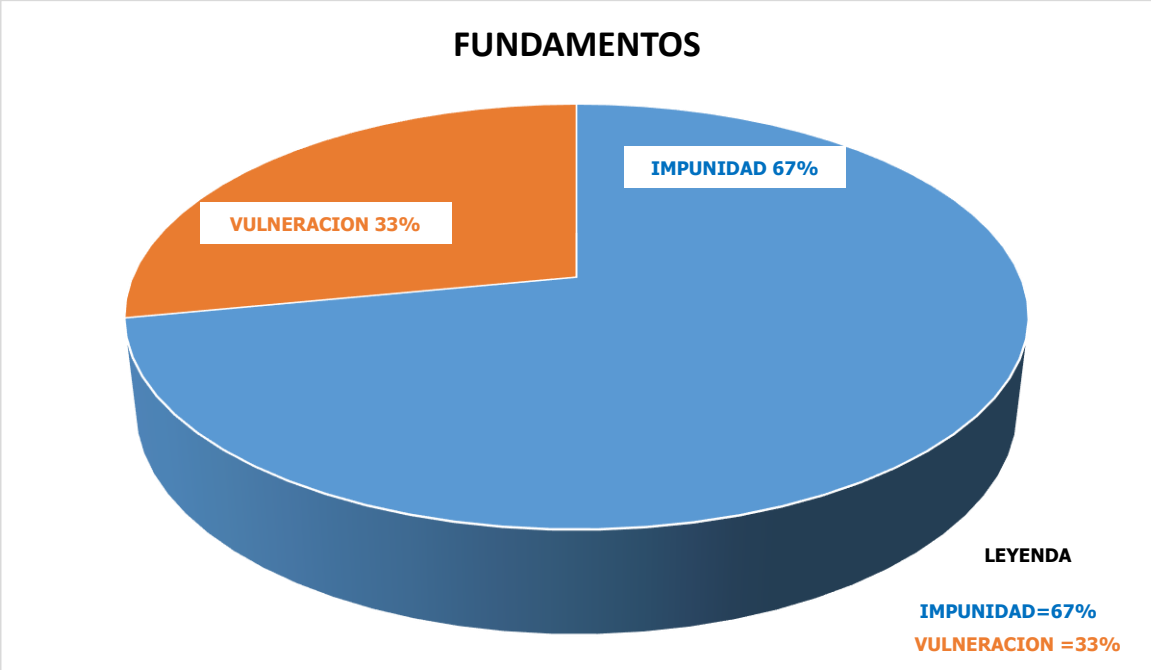
En la siguiente controversia se obtendrá cuáles son los fundamentos que acarrearía en caso de no ser penado la ciberxtorsion y sextorsion.

Entre los fundamentos que acarrearía en caso la ciberxtorsion y la sextorsion no fuera penado tenemos a la impunidad y la vulneración de un derecho.

¿QUE ACARREARIA LA CIBERXTERSION Y SEXTORSION EN CASO DE NO SER PERNADO?				
FUNDAMENTOS	**ENT.**	**%**	**∑**	**%**
IMPUNIDAD	04	67%	07	100%
VULNERACION	03	33%		

Fuente del cuadro: Elaboración propia

De esta manera se obtiene que en caso de no ser penado la ciberxtorsion y sextorsion dejaría una falta de protección a las víctimas de ciberxtorsion o sextorsion por parte del legislador acarreando así su impunidad.



IV. DISCUSIÓN

En nuestra legislación los delitos de Ciberxtorsion y Sextorsion no se encuentran regulados en nuestro código penal y mucho menos en una ley especial, sin embargo esta conducta es moderna y tiende a transformarse con el avance progresivo de la tecnología en los sistemas informáticos El cual debe penalizarse nuestro código penal y si tienen necesidad básica Qué es la protección de derechos fundamentales en caso de la sextorsión el derecho a la intimidad de las personas es la que se vulnera, y en la ciberextorsión la información privada y la data personal.

El legislador debe considerar las conductas de ciberxtorsión y sextorsión como un delito en el código penal peruano pues sé que ha comprobado mediante casos qué el intercambio imágenes, vídeos, audios de contenido sexual con consentimiento entre dos personas, luego es utilizada por una de ellas para chantajear a la otra persona a cambio de favores sexuales o de dinero para que el contenido sexual no se ha llegado en las redes sociales y medios informáticos, también en lo que hackers con avanzado conocimiento tecnológico los cuales mediante un complejo lenguaje informático ingresan a servidores donde sustraen información privada y luego a los dueños de esa información chantajean con un fin de obtener un lucro o en caso de no cumplir hacerlo púbico.

En los antecedentes internacionales, encontramos un tratado internacional sobre delitos informáticos el famoso “Convenio de Budapest” el cual recoge y hace frente a la delincuencia informática mejorando las técnicas de investigación y cooperación entre naciones, en donde se describe cómo actúan los hackers y organizaciones criminales a nivel internacional en donde lo que se busca es penalizar delitos a través de sistemas informáticos.

En los antecedentes nacionales y locales no se logra establecer algún estudio realizado sobre las conductas de ciberxtorsion y sextorsión que es análisis de nuestra investigación, existiendo mucha desinformación por parte de los

legisladores acerca de los delitos informáticos, y en el cual nuestro código penal no ha previsto nuevas conductas que se convirtieron en delitos perpetrados mayormente por jóvenes a través de la internet.

Basándome en los derechos fundamentales como es el derecho a la intimidad y a la privacidad reconocida en nuestra constitución política de 1993, considerándose en el código penal como bienes jurídicos protegidos por el estado, sin embargo nuestros operadores jurídicos no han previsto la conducta como la ciberxtorsion y sextorsion en nuestro ordenamiento jurídico, además la legislación sobre delitos informáticos es muy paupérrima y no se encuentra acorde a nuestra realidad nacional.

Es de necesidad para toda la sociedad y especialmente para los jóvenes y adultos tanto empresas como instituciones de ámbito privado y nacional en donde se utilizan ordenadores y servidores conectados a una red en donde cualquier persona con conocimientos informáticos se puede introducir y sustraer esa información. También debemos implementar nuestra unidad de la policía especializada en delitos informáticos, los cuales deben contar con lo tecnología y técnicas avanzadas pues los delincuentes se encuentran a un paso más adelante que la misma autoridad.

V. CONCLUSIONES

En este capítulo se desarrollará las conclusiones finales de mi investigación desarrollada en mi tesis. A continuación, describiré las siguientes conclusiones:

En la presente investigación se ha determinado la necesidad de incorporar a nuestro ordenamiento jurídico penal los comportamientos de ciberxtorsion y sextorsión, desarrollados a través de las nuevas tecnologías de información causando así estragos a las víctimas de esta conducta que en la presente tesis lo ha desarrollado desde su punto de vista como delito.

La información recopilada y debidamente analizada de la presente investigación confirma que se requiere urgentemente la incorporación de los delitos de Ciberxtorsion y Sextorsion debido a que vulnera derechos fundamentales reconocidos constitucionalmente; sin embargo, su incorporación es competencia de los legisladores los cuales no han tenido idea de las nuevas tendencias y modalidades de delitos a través de nuevas tecnologías, es por ello que es deber del Estado y de los legisladores peruanos penalizar los delitos de Ciberxtorsion y Sextorsion.

En relación al incuestionable crecimiento del internet en nuestra sociedad peruana en donde cada persona tiene acceso a este servicio, se debe crear una institución especializada legal en relación a delitos informáticos de alta complejidad que protejan de alguna manera los delitos cometidos a través del internet bajo un mecanismo garantizador en donde se pueda saber a ciencia cierta quienes son los responsables de haber cometido estos delitos y sean sancionados.

La regulación de los delitos de Ciberxtorsion y Sextorsion depende mucho de la intención del legislador y debe estar justificado en la evidente exigencia

de la sociedad, si bien es cierto nos encontramos en un estado de derecho y como tal debemos encontrar la justicia frente a las adversidades.

La sociedad peruana debe informarse en temas de delitos informáticos y el estado tiene la función brindar esta información concientizando a la sociedad sobre sus consecuencias, también la ciudadanía debe participar activamente para la regulación de los delitos de Ciberxtorsion y Sextorsion, pues esto conllevaría una gran ventaja en nuestro ordenamiento generando así una prioridad a los delitos informáticos que hoy en día afectan a nuestra sociedad.

VI. RECOMENDACIONES

El estado debe encargarse de las necesidades de la sociedad peruana y entre una de ellas de es la de brindar la debida protección jurídica con el fin de establecer mecanismos de protección a toda la sociedad frente a conductas delictuosas a través de la internet y medios informáticos.

Es deber de los legisladores peruanos implementar mecanismos con el fin de establecer parámetros necesarios frente a la delincuencia informática

La sociedad peruana debe estar informada sobre delitos informáticos y es necesario exigir a nuestros legisladores la implementación de nuevas políticas de seguridad en materia informática así como es el deber de ellos abordar estos temas para concientizar a nuestra sociedad.

VII. REFERENCIAS BIBLIOGRAFICAS

- Balmaceda, Q. J. (2008). Revista de investigación Jurídica.
- Baratta, A. &. (1985). La Legislación de Emergencia y el Pensamiento. Revista Doctrina Penal.
- BUSTOS RAMÍREZ, J. (1982). Bases Críticas de un Nuevo Derecho Pena. Bogota: Ed.Temis.
- Castells, M. (2001). Prólogo: la red y el yo en La era de la información: economía, sociedad y cultura. México D.F: Siglo XXI.
- DAVARA RODRÍGUEZ, M. Á. (2008). "Manual de Derecho Informático" (10ª Edición. ed.). Pamplona: ARANZADI.
- FERRAJOLI, L. (1995). Derecho y Razón Teoría del garantismo Penal. Editorial Trotta.
- Garcia, A. (1988). Manual de Criminologia, Introduccion y teorías de la criminalidad. Madrid: Espasa Calpe.
- JAKOBS, G. (1997). Derecho Penal, Parte General, Fundamentos y teoría de la imputación. Madrid: Ediciones Jurídicas S.A.
- Jose, S. C. (2014). “El llamado delito informático no. Sucre.
- Julio, T. V. (2003). Derecho Informatico. México.
- MariaJose, V. (2003). “Protección de datos y delitos. Madrid.
- Marilina, R. C. (2013). “Los desafíos del derecho Penal frente delitos informáticos y otras. revista de Instituto de Ciencias Jurídicas Puebla.
- Paravarini, M. (1993). Control y dominación. Mexico: Siglo XXI Editores.
- Peña, A. (2010). Derecho penal: parte especial. Lima: Idemsa.
- Ricardo, M. Y. (2001). Delincuencia Informática y Derecho. Madrid: Editorial Edisofer.
- Sain, G. (2015). Cibercrimen: el delito en la sociedad de la información. Ed. Eudeba.
- Sain, G. (2017). Delitos informáticos: investigación criminal.
- Salf, M. (1994). Delitos Informáticos de carácter económico. Buenos Aires: Editores del Puerto.
- Salinas, R. (2006). Delitos contra el patrimonio. Lima: Jurista Editores.

- SANCINETTI, M. (2006). Casos de Derecho penal. Parte general. Buenos Aires: Hammurabi, 3ª ed.
- SCHONFELD, L. A. (1999). La expansión del Derecho Penal comopolítica demagógica y sus límite.
- Sieber, U. (1998). “El problema: tipos comunes de delitos informáticos”. Informe de la Comisión Europea.
- SIQUE, G. F. (2OI2). “Necesidad de monitorear legalmente los teléfonos moviles de menores de edad en cumplimiento con el articulo 59 del decreto27-2003 para evitar el sexting”. Guatemala.
- Velasco, E. (2010). Delitos cometidos a través de Internet. Cuestiones procesales. Madrid: La Ley – Grupo Wolters Kluwer.
- Yar, M. (2006). Cybercrime and society. London: Sage Publications.