UNIVERSIDAD NACIONAL DE ANCASH

"SANTIAGO ANTÚNEZ DE MAYOLO"

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

FALTA DE LÍMITES DEL USO DE LAS REDES SOCIALES EN EL PERÚ COMO FACTOR QUE PROPICIA LOS DELITOS INFORMATICOS

Tesis para optar el Título profesional de Abogada

Bach. ROXANA PATRICIA ABARCA VERGARA

Asesor:

DR. ELMER ROBLES BLACIDO

Huaraz - Ancash - Perú

2019

Repositorio Institucional - **UNASAM** - Perú

FORMATO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN, CONDUCENTES A OPTAR TÍTULOS PROFESIONALES Y GRADOS ACADÉMICOS EN EL REPOSITORIO INSTITUCIONAL

1. Datos del autor:

Apellidos y Nombres: ABARCA VERGARA ROXANA PATRICIA

Código de alumno: 112.1604.397 Teléfono: 929196531

E-mail: VERGARA_R19@GMAIL.COM D.N.I. n°: 70178824

(En caso haya más autores, llenar un formulario por autor)

2. Tipo de trabajo de investigación:

- (●) Tesis
- ( ) Trabajo de Suficiencia Profesional
- ( ) Trabajo Académico
- ( ) Trabajo de Investigación
- ( ) Tesinas (presentadas antes de la publicación de la Nueva Ley Universitaria 30220 – 2014)

3. Para optar el Título Profesional de:

ABOGADO

4. Título del trabajo de investigación:

FALTA DE LIMITES DEL USO DE LAS REDES SOCIALES EN EL PERU COMO FACTOR QUE PROPICIA LOS DELITOS INFORMATICOS

5. Facultad de: Derecho y Ciencias Políticas

6. Escuela o Carrera: Derecho y Ciencias Políticas

7. Asesor:

Apellidos y nombres ROBLES BLACIDO ELMER D.N.I n°: 31674266

E-mail: elmerrobles_b@hotmail.com ID ORCID: https://orcid.org/0000-0002-7872-6982

8. Referencia bibliográfica: Tesis en formato APA

9. Tipo de acceso al Documento:

- (●) Acceso público* al contenido completo. Acceso
- ( ) restringido** al contenido completo

Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad Santiago Antúnez de Mayolo una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundirlo en el Repositorio Institucional, respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.

En caso de que el autor elija la segunda opción, es necesario y obligatorio que indique el sustento correspondiente:

10. Originalidad del archivo digital

Por el presente dejo constancia que el archivo digital que entrego a la Universidad, como parte del proceso conducente a obtener el título profesional o grado académico, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado.

Firma del autor

11. Otorgamiento de una licencia *CREATIVE COMMONS*

Para las investigaciones que son de acceso abierto se les otorgó una licencia Creative Commons, con la finalidad de que cualquier usuario pueda acceder a la obra, bajo los términos que dicha licencia implica.

El autor, por medio de este documento, autoriza a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera íntegra a todo el documento.

Según el inciso 12.2, del artículo 12º del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales - RENATI "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Recolector Digital RENATI, a través del Repositorio ALICIA".

……

12. Para ser verificado por la Dirección del Repositorio Institucional

Seleccione la
Fecha de Acto de sustentación:

Huaraz, 28/10/2019

Firma: _____

Varillas Wiliam Eduardo
Asistente en Informática y Sistemas
- UNASAM -

***Acceso abierto**: uso lícito que confiere un titular de derechos de propiedad intelectual a cualquier persona, para que pueda acceder de manera inmediata y gratuita a una obra, datos procesados o estadísticas de monitoreo, sin necesidad de registro, suscripción, ni pago, estando autorizada a leerla, descargarla, reproducirla, distribuirla, imprimirla, buscarla y enlazar textos completos (Reglamento de la Ley No 30035).

**** Acceso restringido:** el documento no se visualizará en el Repositorio.

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

SECCION DE GRADOS Y TITULOS

ACTA DE SUSTENTACION, PARA OPTAR EL TITULO DE ABOGADO, TOMO IV, FOLIO52.- FDCCPP

MODALIDAD: SUSTENTACIÒN DE TESIS

En la ciudad de Huaraz, siendo las dieciocho horas del día ventiocho de octubre del dos mil diecinueve, se presentaron en el Auditórium Nº 03 de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional "Santiago Antúnez de Mayolo" el Jurado Calificador integrado por los docentes:

Mag. Florentino Obregón Obregón	:	**PRESIDENTE**
Abog. Jesús Henostroza Suárez	:	**SECRETARIO**
Dr. Elmer Robles Blacido	:	**VOCAL**

Con el objeto de examinar en Acto Público, la Sustentación Oral de la Tesis titulada: **FALTA DE LIMITES DEL USO DE LAS REDES SOCIALES EN EL PERU COMO FACTOR QUE PROPICIA LOS DELITOS INFORMATICOS"** del bachiller **ABARCA VERGARA Roxana Patricia,** para OPTAR el Título Profesional de Abogado.

Acto seguido, el Bachiller fue llamado por su nombre e invitado a ocupar el podio a efectos de su exposición, luego de lo cual fue examinado en relación a la Tesis sustentada. Culminado el acto, el Presidente invitó a los asistentes a retirarse; para la deliberación, obteniéndose la siguiente calificación:

PROMEDIO.....Dieciseis (16).....

RESULTADO.....APROBADA POR UNANIMIDAD.....

En mérito de lo cual, el Jurado Calificador lo Declara .....APTA....., para que se le otorgue el Título Profesional de Abogado. Con lo que concluye el Acto, siendo las..diecinueve...horas del mismo día. Firman por cuadruplicado los Miembros del Jurado en señal de conformidad.

Mag. Florentino Obregón Obregón
PRESIDENTE.

Abog. Jesús Henostroza Suárez
SECRETARIO

Dr. Elmer Robles Blacido
VOCAL

AGRADECIMIENTO

A Dios, por su amor infinito, ser mi fortaleza y guía espiritual, y alimentar mi fe con su consuelo y bendiciones.

A mi madre Haydee, en donde se encuentre, por educarme con mucho amor y respeto, por creer en mí y brindarme apoyo pese a las diversas adversidades que tuvo que afrontar, apoyo que me dio tranquilidad emocional y económica; por incentivarme a seguir mis sueños con sus consejos y su dureza cuando era necesario.

A mi hermanos, Kevin y Cristian, por ser mis amigos, mis compañeros, por estar siempre conmigo cuando los necesito, por su cariño, por ser mi fortaleza ante el declive que sufrí por la pérdida irreparable de nuestra madre y ayudarme a superarlo y seguir adelante.

A mi compañero de vida Rogelio y mi hija Luciana, por ser hoy mi motor y motivo para insistir y seguir con mí proyecto de vida y mi proyecto profesional.

A mis familiares, por su apoyo, cariño y consuelo que me dan.

A los docentes de la Facultad de Derecho y Ciencias Políticas de la UNASAM por compartir sus conocimientos y coadyuvaron en mi formación académica y profesional.

Repositorio Institucional - **UNASAM** - Perú

DEDICATORIA

A mi madre, quien ha sido la promotora de mis sueños y ahora en el lugar donde se encuentre, comparte mis logros.

Repositorio Institucional - **UNASAM** - Perú

ÍNDICE

INTRODUCCIÓN 1
CAPÍTULO I 3
EL PROBLEMA Y LA METODOLOGÍA DE LA INVESTIGACIÓN 3
1.1. Descripción del problema 3
1.2. Formulación del problema 5
1.2.1. Problema general 5
1.2.2. Problemas específicos 5
1.3. Importancia del problema 5
1.4. Justificación y viabilidad 6
1.4.1. Justificación teórica 6
1.4.2. Justificación práctica 7
1.4.3. Justificación legal 8
1.4.4. Justificación metodológica 9
1.4.5. Justificación técnica 9
1.4.6. Viabilidad 9
1.5. Formulación de objetivos 10
1.5.1. Objetivo general 10
1.5.2. Objetivos específicos 10
1.6. Formulación de hipótesis 10
1.6.1. Hipótesis General... 10
1.6.2. Hipótesis Especificas. 11
1.7. Variables 12
1.8. Metodología de la investigación 12
1.8.1. Tipo, nivel y diseño de investigación 12
1.8.2. Diseño general 13
1.8.3. Diseño Específico 13
1.8.5. Unidad de análisis 15
1.8.6. Instrumentos de recolección de información 16
1.8.7. Plan de procesamiento y análisis de la información. 16
1.8.8. Técnica de la validación de hipótesis. 17
1.8.9. Validación de hipótesis. 17

Repositorio Institucional - UNASAM - Perú

CAPÍTULO II 18
MARCO TEÓRICO 18
2.1. Antecedentes 18
2.2. Bases teóricas 23
2.2.1. Las redes sociales 23
2.2.2. Los delitos informáticos 32
2.2.3. Los delitos informáticos en el Derecho Penal Peruano 37
2.3. Definición de términos 40
2.3.1. La informática 40
2.3.2. Usuario 41
2.3.3. Ordenador 41
2.3.4. Archivo 42
2.3.5. Dato 42
2.3.6. Información 43
2.3.7. Virus informáticos 43
2.3.8. Los Hacker y Cracker 44
CAPÍTULO III 46
RESULTADOS Y DISCUSIÓN DE LA INVESTIGACIÓN 46
3.1. Resultados y discusión doctrinarios 46
3.1.1. Las redes sociales y su vinculación con los delitos informáticos ... 46
3.1.2. Derechos fundamentales vulnerados por el uso indiscriminado de las redes sociales 47
3.1.3. La necesidad de limitar el uso de las rede sociales 54
3.2. Resultados y discusión jurisprudenciales 55
3.2. Resultados y discusión normativos 62
3.2.1. Derecho interno. 62
3.2.2. Derecho internacional 73
3.2.3. Derecho comparado 75
CAPÍTULO IV 87
VALIDACIÓN DE HIPÓTESIS 87
4.1. Validación de la hipótesis general 87
4.2. Validación de la hipótesis específicas 87

Repositorio Institucional - UNASAM - Perú

CONCLUSIONES 90
RECOMENDACIONES 91
REFERENCIAS BIBLIOGRÁFICAS 92

Repositorio Institucional - **UNASAM** - Perú

RESUMEN

La presente investigación tuvo por finalidad analizar y determinar si la falta de límites del uso de las redes sociales en el Perú es un factor que propicia los delitos informáticos. Por ello se realizó una investigación jurídica de carácter dogmática (normativa/teórica) y de acuerdo a su naturaleza cualitativa. Se hizo un análisis de la normatividad, de la doctrina y la jurisprudencia. Al desarrollar la investigación, respecto al Marco Teórico, empleamos la técnica del análisis documental y bibliográfico, con sus instrumentos el análisis de contenido y las fichas, respectivamente.

En la discusión de resultados, se pudo concluir que las interacciones sociales actual con el mundo virtual se pueden realizar prácticas delictivas, y por lo general se ubican en las redes social, donde al no tener ninguna limitación para su acceso se vuelven más vulnerables, bajo cualquier método utilizado según la naturaleza del delito, las mismas que son conocidas por la mayoría de la doctrina como delitos informáticos.

PALABRAS CLAVES: Redes sociales y delitos informáticos.

Repositorio Institucional - **UNASAM** - Perú

ABSTRACT

The purpose of this research was to analyze and determine whether the lack of limits on the use of social networks in Peru is a factor that promotes computer crimes. For this reason, legal research of a dogmatic nature (normative/theoretical) and according to its qualitative nature was carried out. An analysis of the normativity, doctrine and jurisprudence was made. When developing the research, regarding the Theoretical Framework, we use the technique of documentary and bibliographic analysis, with its instruments the analysis of content and the files, respectively.

In the discussion of results, it could be concluded that current social interactions with the virtual world can be carried out criminal practices, and are usually located in social networks, where having no limitation for their access they become more vulnerable, under any method used according to the nature of the crime, the same ones that are known by most of the doctrine as computer crimes.

KEY WORDS: Social networks and computer crimes.

Repositorio Institucional - **UNASAM** - Perú

INTRODUCCIÓN

El presente trabajo de investigación ha sido realizado con el objetivo de obtener el Título Profesional de Abogado, y cumplir con las exigencias de la universidad.

Se ha tenido en cuenta que hoy en día las redes sociales de una manera u otra son indispensables para la comunicación entre personas, grupos organizados, por el hecho de que son de fácil acceso y uso; el mal uso de las redes sociales puede acarrear la comisión de algún delito común o informáticos; lamentablemente hay individuos solos u organizados que se dedican a cometer delitos en redes sociales. Si bien es cierto nuestra legislación ha establecido ciertos actos reprochables como delitos informáticos, no se puede apreciar que existe alguna norma que pueda regular el uso de las redes sociales.

Garrido (2016) establece que "el hecho de participar en las redes sociales supone la implicación de diferentes sujetos y riesgos. Los principales sujetos implicados son, las redes sociales y plataformas colaborativas, los proveedores de servicios, los desarrolladores de software, empresas de marketing y publicidad, la propia Administración Pública, y los usuarios" (p. 7).

Teniendo en cuenta ello el presente trabajo que lleva como título: FALTA DE LÍMITES DEL USO DE LAS REDES SOCIALES EN EL PERÚ ES UN FACTOR QUE PROPICIA LOS DELITOS INFORMÁTICOS.

La investigación está estructurada en cuatro capítulos que comprende:

Repositorio Institucional - UNASAM - Perú

El primer capítulo contiene el problema y la metodología de la investigación, indicando la problemática en la cual gira la presente investigación; del mismo modo, precisando la metodología usada.

El segundo capítulo, compete al marco teórico en el que se sostiene el trabajo de investigación, con el que se trata de explicar el tema central.

El tercer capítulo, trata sobre los resultados y discusión de la investigación, en donde se puede advertir el estado normativo, jurisprudencial y doctrinal sobre los delitos informáticos y las redes sociales.

El cuarto capítulo, es referente a la validación o contrastación de las hipótesis, constatándose las hipótesis generales y específicas.

Finalmente, se desarrollan las conclusiones y recomendaciones respecto al trabajo de investigación.

La tesista.

Repositorio Institucional - **UNASAM** - Perú

CAPÍTULO I

EL PROBLEMA Y LA METODOLOGÍA DE LA INVESTIGACIÓN

1.1. Descripción del problema

El avance de la tecnología y el fenómeno del internet han generado nuevos medios de comunicación de fácil acceso y adaptación, que permiten la reducción de tiempo para comunicarnos con personas de todo el mundo; avance que se inició con la creación de correos electrónicos que nos permiten enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos a través del internet, los mismos que siguen vigentes, después se implementó mensajería instantánea en el año 2005 con el denominado Windows Messenger Live, surgiendo el chat, que permitía interactuar de manera casi directa con las personas de todo el mundo, durando hasta el año 2012, y fue suplantado con la creación de las redes sociales.

Las redes sociales en la actualidad son plataformas que han generado un gran impacto, porque han multiplicado exponencialmente las posibilidades de comunicación entre personas y de acceso a la información, ha creado un nuevo entorno social con interacción, permitiendo que millones de usuarios publiquen y difundan datos personales que pueden ser vistos de cualquier parte del mundo.

Fachin (2018) al respecto señala que "las redes sociales son sitios o plataformas en los que se intercambia información, datos y contenidos de diferentes formatos con un grupo de personas (y/o organizaciones) de modo tal que interactúan y crean entre ellos una comunidad virtual que persigue un

Repositorio Institucional - UNASAM - Perú

relativo interés en común" (https://josefacchin.com/lista-redes-sociales-mas-importantes-del-planeta/).

Buono, Fernadez y García (2019) han señalado lo siguiente:

En el 2019 se puede apreciar que existen un centenar de redes sociales de los cuales se puede mencionar los más comunes como Taringa, Badoo, Myspace, Vimeo, Youtube, Facebook, Messenger, Twtter, Instangram, entre otros; los mismos que desde sus orígenes han generado sin lugar a duda beneficios, pero también desventajas e inconvenientes para el Derecho en general y específicamente para el derecho penal. Si bien es cierto, las redes sociales aportan beneficios como: facilitan la comunicación instantánea ofreciendo la oportunidad de ponerse en contacto con amigos, conocidos o desconocidos de cualquier parte del mundo con el que se comparte intereses; oportunidad laboral, ya que las redes sociales pueden ser nuestra mejor carta de presentación y pueden ser aprovechados para desarrollar nuestra marca personal, y muchas empresas buscan a los posibles candidatos en redes sociales por ejemplo publicando la convocatoria; ofrecen información y entretenimiento; se puede compartir conocimientos e información; entre otros. También tienen desventajas a nivel social o personal ya que se pueden producir estafas en las redes sociales, exposición de la privacidad, suplantación de identidad, Ciberbullying y Grooming, adicción a las redes sociales (https://prezi.com/zzfbf7rjsqo2).

Las redes sociales en la actualidad están exponiendo a las personas y volviéndolas vulnerables porque se han convertido en un medio donde se presentan los delitos informáticos; además, son utilizados por delincuentes comunes como medio para realizar aquellos delitos conocidos como clásicos o delitos cometidos de manera personal como secuestros, amenazas, acoso, hurto, entre otros. Afectando de este modo derechos internacionales y derechos constitucionales de la persona humana; por ello todas las personas que participan de forma directa o indirecta en las redes sociales deberían conocer sus derechos, obligaciones y limitaciones, así como los riesgos que derivan de su uso.

Repositorio Institucional - UNASAM - Perú

Los derechos fundamentales vulnerados con el uso indiscriminado de las redes sociales son aquellos vinculados con los datos personales; la intimidad, honor y propia imagen; la propiedad intelectual e industrial, entre otros.

Ante lo indicado, me planteó los siguientes problemas de investigación jurídica:

1.2. Formulación del problema

1.2.1. Problema general

¿La falta de límites del uso de las redes sociales en el Perú es un factor que propicia los delitos informáticos?

1.2.2. Problemas específicos

- ¿Cuáles son los comportamientos que se pueden reconocer como delitos informáticos en las redes sociales, en nuestra legislación peruana?
- ¿Qué derechos fundamentales vulnera el uso indiscriminado de las redes sociales?
- ¿Existen políticas criminales nacionales encaminadas a prevenir la realización de los delitos informáticos?

1.3. Importancia del problema

Hoy en día existe una nueva forma de comunicación, estas son a través de las redes sociales, y se han convertido en un modo de acercamiento y proximidad entre las personas, es decir permite que personas en distintos lugares se reúnan en un

Repositorio Institucional - UNASAM - Perú

mismo espacio virtual e interactúen, compartan contenidos, establezcan conversaciones, se distraen, se relacionan laboral o profesionalmente; siendo un sistema abierto que permite, por un lado la optimización de los recursos de comunicación y la creación de alternativas para la resolución de problemas y la satisfacción de necesidades tanto personales como empresariales e incluso tiene influencia en la política; y por otro lado, es una puerta a una serie de peligros que afecta al individuo, es decir, que el uso de las redes sociales implica muchos riesgos. Riesgos que tienen que ver con aquellos delincuentes que hacen uso de las redes sociales y mediante éste cometen una serie de delitos, estos pudiendo ser los comunes como es el caso secuestros, extorciones, amenazas, hurtos, robos, entre otros, o la realización de los delitos informáticos como es aquellos delitos contra datos y sistemas informáticos, contra la indemnidad y la libertad sexual, contra la intimidad y el secreto de las comunicaciones, contra el patrimonio y contra la fe pública; que no solo afectan a la persona en concreto, sino que además a la sociedad. Por lo que es necesario analizar si el uso indiscriminado de las redes sociales propicia los delitos informáticos y si es necesario establecer políticas sociales que limiten su uso, por lo que es importante el desarrollo de la presente investigación.

1.4. Justificación y viabilidad

1.4.1. Justificación teórica

La presente se justificó jurídicamente, debido a que los delitos informáticos, conocido como lo establece Estrada (2015) "…todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático" (p. 10). Se encuentran prescritos de manera específica

Repositorio Institucional - UNASAM - Perú

en la Ley Nº 30096 y su modificación en la Ley Nº 30071; delitos que en la actualidad son cometidos, en su gran mayoría, mediante el uso de las redes sociales por ser ésta un medio de comunicación e información de fácil acceso, por lo que requiere de una minuciosa investigación.

Con la presente investigación se pretendió analizar respecto al uso de las redes sociales y si estas por su uso indiscriminado son factores importantes que van a propiciar la generación de los delitos informáticos, que desde las diversas dimensiones afectan bienes jurídicos de distinta naturaleza. Por ello el estudio del uso de las redes sociales y su vinculación con los delitos informáticos contribuirá a establecer si es necesario o no ciertos límites de uso de las redes sociales en nuestro país.

Además, consideramos imprescindible analizar las diversas doctrinas y legislaciones comparadas que nos van a permitir indistintamente identificar las posiciones en favor o en contra de limitar de alguna manera el uso de las redes sociales.

1.4.2. Justificación práctica

La presente investigación es útil, por cuanto nos permitirá analizar si el uso de las redes sociales requiere de límites, por cuanto su uso indiscriminado es un factor que propicia los delitos informáticos, y permitirá establecer qué derechos fundamentales son vulnerados con ese uso indiscriminado; a través del cual podremos verificar si existen políticas nacionales con el fin de prevenir de algún modo la proliferación de los delitos informáticos a través del as redes sociales.

Repositorio Institucional - UNASAM - Perú

De la revisión jurisprudencial se ha advertido que el Tribunal Constitucional en el EXP Nº 00442-2017-PA/TC ha emitido pronunciamiento sobre el desbloqueo de una cuenta en la red social de twitter, la misma que posibilitará de alguna manera establecer parámetros respecto al uso de las redes sociales en su conjunto.

1.4.3. Justificación legal

La presente, respecto al problema de investigación, tiene su justificación en las siguientes normas legales:

- ✓ Pacto Internacional de Derechos Civiles y Políticos.
- ✓ La Constitución Política del Perú.
- ✓ El Convenio de Budapest
- ✓ El Código Penal.
- ✓ La Ley Nº 30096.
- ✓ La Ley Nº 30071.

Y en cuanto al proceso de investigación se justifica en las siguientes normas legales:

- ✓ La Constitución Política del Perú.
- ✓ La Ley Universitaria.
- ✓ Ley General de Educación Nº 28044 y su modificatoria Nº 25212
- ✓ El Estatuto de la Universidad Nacional "Santiago Antúnez de Mayolo"- Huaraz.
- ✓ El Reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional "Santiago Antúnez de Mayolo"- Huaraz.

Repositorio Institucional - UNASAM - Perú

1.4.4. Justificación metodológica

En la presente se aplicó los parámetros establecidos por la metodología de la investigación científica como modelo general y la metodología de la investigación jurídica, en particular, desarrollando en sus diferentes etapas, las técnicas e instrumentos de recolección de datos y el diseño de investigación propio de esta investigación.

1.4.5. Justificación técnica

El presente proyecto técnicamente cuenta con el soporte técnico y logístico, habiendo previsto una computadora personal, impresora, scanner, y el software Microsoft Office 2016 (versión 2019).

1.4.6. Viabilidad

En cuanto a la viabilidad bibliográfica, el tema de investigación cuenta con el suficiente acceso a la información tanto en internet, revistas, trabajos de investigación, libros, ponencias, artículos, entre otros.

Respecto a la viabilidad económica, los recursos económicos son propios, de manera que no se requirió de un financiamiento mayor o ser asistido por alguna entidad.

La viabilidad temporal, el presente trabajo de investigación se realizó en un corto plazo de seis meses dentro del año 2019, por la ejecución de todos los procesos de investigación tales como: planteamiento del problema, marco teórico, diseño de la investigación, tabulación, conclusiones y recomendaciones.

Repositorio Institucional - UNASAM - Perú

1.5. Formulación de objetivos

1.5.1. Objetivo general

Analizar y determinar si la falta de límites del uso de las redes sociales en el Perú es un factor que propicia los delitos informáticos.

1.5.2. Objetivos específicos

- Analizar y explicar las bases doctrinarias y normativas respecto a que las redes sociales tienen una vinculación directa con los denominados delitos informáticos.
- Explicar los derechos fundamentales vulnerados por el uso indiscriminado de las redes sociales.
- Obtener información de las políticas criminales nacionales encaminadas a prevenir la realización de los delitos informáticos.

1.6. Formulación de hipótesis

Robles (2014) señala que "…las hipótesis en las investigaciones dogmáticas o teóricas son "opcionales", y si se plantean son solo descriptivas, constituyendo solo una hipótesis de trabajo, que nos servirá de guía en la investigación" (p. 38).

1.6.1. Hipótesis General

La falta de límites del uso de las redes sociales en el Perú ha ocasionado gran impacto en el incremento de los delitos informáticos, ya que en la actualidad las redes sociales se encuentran al alcance de todo el mundo sin ningún tipo de

Repositorio Institucional - UNASAM - Perú

discriminación; sirviendo así, como medio para la perpetración de delitos tanto por delincuentes comunes, como por aquellos conocedores de las tecnologías de información; si bien es cierto, los delitos cometidos también puede ser denominados tradicionales, en algunos casos al hacer usos de algún medio informático reviste su naturaleza a la perpetración de los denominados delitos informáticos.

1.6.2. Hipótesis Especificas

- La doctrina y en alguna medida las normas reconocen que los delitos informáticos en la actualidad se han ido incrementado por el uso de las redes sociales, por lo que tendría una vinculación directa con estos delitos; los mismo que están prescritos en la Ley Nº 30096 y su modificación en la Ley 30071, pero que evidentemente no se encuentran debidamente actualizados conforme a la realidad social cibernética.
- La falta de límites del uso de las redes sociales está vulnerando derechos fundamentales de la persona, reconocidos en la constitución, como el derecho a la intimidad, al honor y propia imagen, la propiedad intelectual e industrial, la libertad sexual e incluso la propia vida.
- No existe, políticas criminales encaminadas a prevenir la realización de los delitos informáticos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales que minimicen riesgos existentes; peor aún políticas que limiten el uso indiscriminado de las redes sociales.

Repositorio Institucional - UNASAM - Perú

1.7. Variables

INDEPENDIENTE (X): Limites del uso de las redes sociales.

Indicadores:

- Redes sociales de uso común.
- Redes sociales permitidos en el país.
- Redes sociales como medio de comunicación.

DEPENDIENTE (Y): la falta de limites es un factor que propicia los delitos informáticos.

Indicadores:

- El uso indiscriminado de las redes sociales.

1.8. Metodología de la investigación

1.8.1. Tipo, nivel y diseño de investigación

1.8.1.1. Tipo de investigación

Correspondió por su finalidad a la denominada investigación básica o teórica, cuya finalidad es ahondar y ampliar los conocimientos respecto al uso de las redes sociales y su vinculación con los delitos informáticos.

Y correspondió a una investigación Dogmática – Normativa, que posibilitó ampliar y profundizar los conocimientos respecto a las redes sociales y los delitos informáticos.

Repositorio Institucional - UNASAM - Perú

1.8.1.2. Tipo de diseño de investigación

Correspondió el denominado Diseño No Experimental, esto es debido a que carece de manipulación intencional de la variable independiente, además no posee grupo de control ni experimental. Su finalidad será estudiar el hecho jurídico identificado en el problema después de su ocurrencia, conforme lo señala Robles (2014) "cuando no existe intervención planificada del investigador (no tiene control de las variables durante el estudio, estamos frente a un diseño no experimental u observacional" (p. 47).

1.8.2. Diseño general

Se empleó el diseño Transeccional o Transversal, cuya finalidad fue recolectar datos del hecho jurídico en un solo momento o en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado.

1.8.3. Diseño Específico

Se empleó el diseño Descriptivo-Explicativo, toda vez que se estudió los delitos cometidos por medio de las redes sociales y si es necesario limitar su uso, teniendo en cuenta que este diseño se basa en la teoría organizada mediante la selección, estudio y presentación de los datos recopilados.

1.8.4. Métodos de Investigación

Se utilizaron los siguientes métodos de investigación jurídica:

Repositorio Institucional - UNASAM - Perú

Los métodos generales que se emplearán en la presente investigación serán: el método Inductivo-Deductivo y el método Analítico-sintético; y los métodos específicos empleados en la investigación son, el método dogmático, hermenéutico, método de la argumentación jurídica y el método exegético.

conforme lo establece Zelayarán (2000), quien sostiene que:

- **Método Dogmático. -** Encaminada al estudio e investigación de la doctrina con la finalidad de realizar abstracciones (instrumentos lógicos, inducción, deducción, análisis, síntesis, analogía, comparación), con la finalidad de pulir los aportes de los juristas o lo que aparece en el campo normativo, estudiar las instituciones del Derecho con la finalidad de realizar construcciones correctamente estructuradas y proponerlas para su utilización. El Derecho al estar conformado por instituciones, estos pueden ser explicados para el método dogmático en términos jurídicos sin apelar a consideraciones políticas, ideológicas o éticas.
- **Método hermenéutico. -** La hermenéutica jurídica presupone necesariamente el manejo de los conceptos, nociones y dogmas que conforman la ciencia del Derecho. Los aplicadores del derecho tienen la enorme, pero a la vez honrosa responsabilidad de otorgar sentido, a través de sus resoluciones judiciales, a la voluntad soberana del pueblo. En sentido amplio, este método trata de observar algo y buscarle significado. En sentido estricto, siempre que los datos o las partes de un todo se presten a diferentes interpretaciones. En ese sentido, siendo nuestro objeto de estudio susceptible de diversas interpretaciones será necesario para poder hacer la teorización de nuestro trabajo emplear este método. Existen muchos métodos de interpretación (sistemático, histórico, funcional, restrictivo exegético, sociológico, etcétera) empero, la solución correcta a la dicotomía debe ser siempre congruente y compatible con los anhelos e ideales de la sociedad de que se trate para que de esa forma se obtenga un sistema jurídico válido y a la vez eficaz (válido en cuanto no contraría la norma fundamental y eficaz en cuanto a que se respeta y cumpla) capaz de garantizar la vigencia del Estado de Derecho; por ello la interpretación hermenéutica niega la posibilidad de significados múltiples y contrastantes; en todo caso, la coherencia depende de la conformidad de la interpretación con el todo del sistema normativo que se presume integro, sin lagunas jurídicas; por ello el intérprete del derecho dispone con anticipación del sentido que constituyen la tradición jurídica que persiguen los sentimientos de una nación.
- **Método de la Argumentación Jurídica. -** La argumentación jurídica es el medio con el cual se sustenta el Derecho. La argumentación jurídica es la forma organizada de demostrar lógicamente por medio de un razonamiento formulado con el propósito de conseguir la aceptación o rechazo de una tesis o teoría determinada. La aceptación o rechazo de esa tesis dependerá de la eficacia o

Repositorio Institucional - UNASAM - Perú

ineficacia de la argumentación que le sirve de apoyo. En los procesos judiciales es necesario establecer por medio de la argumentación jurídica, el que se pueda probar los hechos, valiéndose de ciertos medios o indicios, que a menudo se contraponen unos a otros. La argumentación jurídica infiere, de los indicios, la existencia o inexistencia de otros hechos que son considerados, por la experiencia, como la única explicación práctica posible de tales indicios.

- **Método Exegético. -** Tiene por objeto de estudio a la norma jurídica y cuya finalidad fue captarlas y comprenderlas dirigiéndolas a la idealidad; tiene además las características de ser puramente formal o conceptual, en donde se libere a la Ciencia Jurídica de elementos extraños pertenecientes a otras disciplinas. Este método fue aplicado en nuestro trabajo, toda vez que se hará el estudio de la normatividad vigente sobre nuestro problema de investigación.

Ramos (2011), señala que, "una investigación jurídico dogmática concibe el problema jurídico desde una perspectiva estrictamente formalista, desconectando todo elemento fáctico o real que se relacione con la institución o especie legislativa…" (p. 93). Este método ha sido empleado en la presente investigación toda vez que se ha analizado el derecho positivo en función de la doctrina y las diversas propuestas teóricas de los diferentes juristas, los mismos que son apartados de consideraciones políticas, ideológicas o éticas. Asimismo, en nuestra investigación se empleó en el análisis de las normas jurídicas respecto a las redes social y los delitos informáticos; respecto a la argumentación jurídica se utilizó en el análisis de la aplicación de normatividad respecto a las redes sociales.

1.8.5. Unidad de análisis

La unidad de análisis estuvo conformada por las fuentes documentales: Doctrina, Jurisprudencia y normatividad; además la unidad de análisis que está compuesta por:

1.8.5.1. Unidad temática

Constituido por el tema del contenido a desarrollar.

Repositorio Institucional - UNASAM - Perú

1.8.5.2. Categorización de tema

Se establecerá categorías dentro del análisis. Unidad de registro.

1.8.5.3. Unidad de registro

En esta fase se dan curso al análisis de categorías.

1.8.6. Instrumentos de recolección de información

En la presente investigación se empleó las siguientes técnicas e instrumentos de recolección de datos:

TÉCNICAS	INSTRUMENTOS
Análisis documental	Guía de análisis de documentos.
Bibliográfica	Fichas: textual, comentario, resumen, crítica.

El recojo de información del trabajo de campo se realizó a través de la Técnica del análisis documental, empleándose como su instrumento el análisis de contenido; además de la Técnica bibliográfica, utilizando como instrumentos las fichas, bibliográficas, hemerográficas, especialmente las literales y de resumen, en base al cual hemos recogido la información suficiente sobre nuestro problema de estudio, para luego ser procesado y planteado a través de la argumentación.

1.8.7. Plan de procesamiento y análisis de la información.

A fin de ordenar de manera sistemática la información, en una estructura lógica coherente, reflexionando un tipo teórico que integre esa información, se ha

Repositorio Institucional - UNASAM - Perú

empleado el Método de la Argumentación Jurídica. Del mismo modo, para obtener información en la presente investigación se hizo por medio del enfoque cualitativo, la misma que posibilitó acopiar información sobre el problema planteado. Motivo por el cual en la presente investigación no se ha empleado la estadística, sino la interpretación de peculiaridades y alcances en la jurisprudencia y doctrina.

1.8.8. Técnica de la validación de hipótesis.

Al ser la presente investigación: jurídica – teórica, el diseño de contrastación fue la aplicación de la exégesis y de la dogmática penal; todo ello para llegar a determinar si las redes sociales necesitan de algún límite y si son medios por el cual se generan los delitos informáticos; así como en forma amplia, la argumentación jurídica para debatir las posturas encontradas y para plasmar las posturas que hemos asumido a lo largo de la presente investigación dogmática.

1.8.9. Validación de hipótesis.

Los datos obtenidos se han evaluado en base a la teoría de la argumentación jurídica, toda vez que el Derecho puede concebirse como argumentación, ya que desde cualquier perspectiva la actividad de todo jurista cuando aplica el Derecho consiste fundamentalmente en argumentar. La habilidad para presentar buenos argumentos a fin de justificar una postura; el fin básico de la teoría de la argumentación jurídica no es la de mostrarles cosas nuevas a los juristas, sino recordarles a los juristas lo que ya saben, pero orientándoles siempre a la mejora continua de su actuar, siempre en beneficio de la sociedad.

Repositorio Institucional - UNASAM - Perú

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

Revisado las tesis sustentadas en la FDCCPP-UNASAM y de otras universidades de nuestra región; no se ha podido encontrar algún trabajo de investigación similar o parecida a la presente por lo que podemos manifestar que la investigación será un aporte al entendimiento de la problemática jurídica sobre la falta de límites del uso de las redes sociales en el Perú como factor que propicia de delitos Informáticos.

Asimismo, realizado la búsqueda se ha podido encontrar a nivel nacional el siguiente trabajo, que contribuyen en algún punto a la presente investigación y son pertenecientes a:

Morales (2016), en su tesis titulado: *LA INSEGURIDAD AL UTILIZAR LOS SERVICIOS DE REDES SOCIALES Y LA PROBLEMÁTICA JUDICIAL PARA REGULAR LOS DELITOS INFORMÁTICOS EN EL PERÚ-2015*, para optar el título profesional de Abogado, en la Escuela Académica Profesional de Derecho, de la Universidad Señor de Sipan, arriba a las siguientes conclusiones: 1. La historia de la computación se remonta a los años 60s existiendo previamente a ello diversos aparatos rudimentarios que facilitaban las labores del ser humano como las calculadoras, instrumentos para realizar operaciones a través de tarjetas perforadas, inclusive hasta llegar al rudimentario ábaco, llegando hasta las computadoras que han sufrido diversas modificaciones a través de las denominadas “Generaciones”,

Repositorio Institucional - UNASAM - Perú

en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada. 2. La historia de la computación se remonta a los años 60s existiendo previamente a ello diversos aparatos rudimentarios que facilitaban las labores del ser humano como las calculadoras, instrumentos para realizar operaciones a través de tarjetas perforadas, inclusive hasta llegar al rudimentario ábaco, llegando hasta las computadoras que han sufrido diversas modificaciones a través de las denominadas "Generaciones", en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada. 3. La Internet ha venido a evolucionar la historia del hombre como lo han hecho diversos inventos, dándose su aplicación en diversas actividades no solo laborales si también en la comunicación, información, entre otras más, convirtiéndose en una herramienta en beneficio del hombre y todos los aspectos que lo rodean, existiendo siempre el lado negativo que es resultado del crecimiento global, la facilidad que lleva su uso, y las malas intenciones de las personas. 4. La influencia de los sistemas informáticos en el Derecho da lugar a la existencia del denominado Derecho Informático enfocado a la protección de datos informáticos o la información concentrada en medios magnéticos o digitales. 5. Con la protección de diversos bienes jurídicos en las Leyes reguladoras de los delitos informáticos se han encontrado otras leyes con las que pudieran existir algunas contradicciones para su inadecuada aplicabilidad; tal es el caso del delito de hurto y sus agravantes, que también es protegido por el

Repositorio Institucional - UNASAM - Perú

Código Penal. 6. Hoy en día la delincuencia ha crecido de manera considerada en todo el globo terráqueo y con el uso de medios más modernos para realizar sus fines delictivos como el uso de computadoras, siendo el arma más adecuada para combatir este delito es el establecimiento de legislaciones acordes con esa problemática, tanto a nivel nacional, local, así como internacional, toda vez que se está hablando de una delincuencia que se lleva a cabo en todos los rincones del mundo. 7. La problemática de la Delincuencia Informática ha sido tan complicado ya que como se ha mencionado el avance de la tecnología informática ha sido tan impresionante y rápida que ese avance se ha reflejado en los medios computacionales utilizados por la delincuencia; avances que han aparecido en los sistemas para guardar información dentro de esos sistemas informáticos con una mayor seguridad utilizando el sistema conocido de "encriptación", sin embargo la delincuencia se ha asistido de expertos en informática para violar esas seguridad, encontrando así a los denominados Hacker, Lamer, Cracker. 8. La delincuencia informática que ha generado en el mundo desde los años 70s grandes daños a personas en lo particular, a empresas, a entidades financieras y a los propios Países. Por ser una problemática de nivel mundial, esta delincuencia ha sido regulada internacionalmente tal es el caso del Convenio de Budapest, al cual no estamos inscritos, La Convención Internacional sobre la Delincuencia Cibernética, uno de los grandes problemas de toda clase de delincuencia es el de detectar el modus vivendi y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad encontramos a la Criminalística que enfocada a Los Delitos Informáticos, pues con la ayuda de La Policía Nacional se logrará la aprehensión de los delincuentes que utilizan los

Repositorio Institucional - UNASAM - Perú

grandes avances tecnológicos para sus fines delictivos y que se oculta y huye a través de las líneas alámbricas e inalámbricas de esos sistemas computacionales.

Y a nivel internacional los siguientes trabajos:

González, Bermeo, Villacreses y Guerrero (2018), realizaron la investigación: *DELITOS INFORMÁTICOS: UNA REVISIÓN EN LATINOAMÉRICA*, en la Universidad Técnica de Machala, arribaron a las siguientes conclusiones: Resulta evidente que, en la mayoría de los países estudiados, aún persisten en algunos casos los vacíos legales con respecto a la regulación del uso de la información a partir de los diferentes medios de comunicación. A pesar que han sido múltiples los esfuerzos de los gobiernos en la lucha contra este tipo de delitos, donde se incluye la piratería, difusión de pornografía infantil, así como el uso inadecuado de la información con diferentes fines; lamentablemente aún persisten este tipo de prácticas. Los delitos informáticos no se pueden erradicar de un día para otro, pero si es posible y urgente legislar y aplicarla ley para el combate a estos delitos con más rigor, pues, aunque las autoridades competentes pongan a disposición de un Ministerio Público a estas bandas delictivas o actores individuales, lamentablemente no se tienen elementos suficientes para atribuirles en algunos casos responsabilidades por la falta de claridad en las leyes. A nivel nacional se detectan varias falencias en el sistema jurídico que no prioriza el accionar publico frente a estos actos que, sumado a la falta de conocimiento de la población, ocasiona un medio fácil para los ciberdelitos gracias a que no se protege la integridad de la información virtual ni se respetan espacios intelectuales. Las medidas a tomar en el Ecuador deben ser claras, en

Repositorio Institucional - UNASAM - Perú

primera instancia capacitar a la ciudadanía sobre realidad de estos delitos, implementar reformar a su código penal para actuar libremente mediante la aplicación de leyes dinámicas que se actualicen según se detecten el modo de operar de los responsables, además mejorar los sistemas de seguridad a nivel nacional en todos los entornos virtuales no solo en bancos sino en sitios gubernamentales y aplicar códigos para regular el uso de las redes sociales al ejecutar dichos actos vandálicos.

Serrano, (2016), en su tesis titulado: *LOS DELITOS EJECUTADOS MEDIANTE LA RED SOCIAL FACEBOOK Y SU RELACION CON EL CODIGO ORGANICO INTEGRAL PENAL ECUATORIANO*, para optar el título profesional de Abogado, en la Carrera de Derecho, de la Universidad Regional Autónoma de los Andes, arriba a las siguientes conclusiones: Las redes sociales se fundamentan en la teoría de los seis grados que sustentan que con una red de 100 contactos un mensaje replicado por seis ocasiones dentro de cada uno de los integrantes de esa red seria recibido por un billón de personas. La Unión Europea delimita jurídicamente que son las redes sociales, teniendo como principales características: la inscripción de los usuarios, la interacción entre ellos y la venta de publicidad de parte del propietario. Además, clasifica a los usuarios como usuarios domésticos y comerciales, delimitando las responsabilidades de cada uno de estos e incluso exija a los proveedores de servicios de redes sociales identificados como SRS que deben proporcionar espacios para que los usuarios y no usuarios puedan reportar cuando un miembro utiliza información personal sin autorización. En países como Colombia la protección jurídica está encaminada en la defensa de la privacidad de la información, mientras que en México y en España la legislación no trata de

Repositorio Institucional - **UNASAM** - Perú

manera amplia las implicaciones jurídicas de las redes sociales. En Chile y Argentina la aplicación de tipos penales ya existentes en los delitos comunes, son interpretados por las autoridades para poder sancionar aquellos actos que se comenten en la red. Entre los delitos informáticos determinados por la ciencia tecnológica existe el phising, Pharming, el hacking entre otros los que tienen como particularidad que se cometen de manera virtual y sus consecuencias se producen en la información mas no en las personas directamente. Los tipos penales presentes en el COIP dan cuenta que existen delitos donde Facebook es un medio y no el fin por lo que se utiliza como medio probatorio para la materialidad y solo en casos de los delitos informáticos en donde se confirma que es en la red donde se da la infracción. Se determinó que la mayoría de usuarios que presencian un delito en Facebook no solo que no lo denuncian si no que lo comparten con sus contactos, dejando no solo la impunidad del delito cometido, también se determinó que quienes han sido víctimas la mayoría de las veces no realizan ninguna acción para denunciar y las pocas que se realizaron no obtuvieron resultados.

2.2. Bases teóricas

2.2.1. Las redes sociales

Sobre las redes sociales Rodríguez (2011) señala que:

> Estas redes son herramientas de comunicación que proporcionan actualizaciones automáticas, perfiles visibles, capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea. Lo que ofrece a sus usuarios un lugar común para desarrollar comunicaciones constantes. La base del funcionamiento de las redes sociales es el mismo usuario puesto que las redes sociales son construidas y dirigidas por estos, quienes además constantemente las nutren de contenido. Al ser impulsadas por la comunidad misma las redes

Repositorio Institucional - UNASAM - Perú

> sociales no solo permiten descubrir nuevos usuarios para agregar a nuestra red según diferentes clases de intereses, sino que también permiten volver a contactar viejos amigos con los que se había perdido contacto desde hace muchos años atrás (p. 3).

Por otro lado, INTECO (2008) establece:

> Como concepto de red social, y dado el contexto actual en el que Internet ocupa gran parte de los actos cotidianos, se puede afirmar que se trata de una aplicación online que permite a los usuarios, de forma completamente descentralizada, generar un perfil público, compartir información, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión (p. 3).

Para Requena (2011) señala que "una red social son la serie de vínculos que existe entre varios actores sociales que tienen como capacidad principal la interpretación de la conducta de los miembros que la componen" (p. 2).

Por otra parte, Martínez, García, & Marcos (2011) manifiestan que "las redes sociales en internet son conformadas por un grupo de amigos que, al ingresar a un portal de redes sociales, tienen la oportunidad de hacer partícipe de la misma a sus propios contactos que a su vez son puestos a consideración a los demás miembros de la red de tal manera que el acceso a este grupo se va ampliando exponencialmente se vayan integrando personas a la red" (p. 4).

Otra cualidad importante de las redes sociales en internet y que la diferencia de los demás espacios disponibles en la red es que para que una red sea funcional debe mantener vigente dos principios según el (Observatorio Nacional de las Telecomunicaciones España, 2011).

En la era tecnológica del cual somos testigos, las redes sociales han llegado a ocupar un lugar importante, de la mano del internet, por lo que se aprecia su crecimiento acelerado, siendo de uso no solo de personas naturales, sino también

Repositorio Institucional - UNASAM - Perú

por empresas y lamentablemente por personas inescrupulosas que aprovechando ese auge cometen actos delictivos en perjuicio de la persona, la sociedad, el estado, etc.

2.2.1.1. Surgimiento de las redes sociales

Franco (2017) señala:

> El origen de las redes sociales, es relativamente nuevo. Su consolidación se materializa con el surgimiento de la red de Internet, con el uso de las nuevas tecnologías de la información, mediante ordenadores y teléfonos móviles. Desde el uso cotidiano de estos elementos el uso de las redes sociales, se ha consolidado como una de las formas más comunes de interacción social, en todas las edades. Jóvenes, niños adultos, personas de la tercera edad, día a día acuden a esta nueva forma de interacción, como forma de mantener contacto con sus seres queridos o allegados (p. 2).

Marker (citado por Rodríguez, 2011) señala que:

> El origen de las redes sociales en internet se remonta a más de una década pues se estima que el origen de las redes interactivas se remonta al año 1995. Época en la que Internet había logrado convertirse en una herramienta prácticamente masificada. Randy Conrads fue el verdadero pionero del servicio, mediante la creación del sitio web que llevaba por nombre "Classmates", y el cual consistía en una red social que brindaba la posibilidad de que las personas de todo el mundo pudieran recuperar o continuar manteniendo contacto con sus antiguos amigos, ya sea compañeros de colegio, de la universidad, de distintos ámbitos laborales y demás, en medio de un mundo totalmente globalizado. Obviamente, esto fue posible gracias a la llegada de la denominada Web2.0, que en definitiva se trata de un sistema que posee una clara orientación social (p. 2).

Los conocedores de la informática, coinciden que las redes sociales tienen su origen con el envío del primer email entre dos ordenadores que se encontraban uno al lado del otro (1971); en 1978 se crea BBS (Bulletin Board Systems) que servía (y continúa sirviendo) para pasarse información entre amigos sobre reuniones, noticias y compartir información entre ellos. En 1994 y 1995 empieza incursionarse

Repositorio Institucional - UNASAM - Perú

con más auge con el lanzamiento de Geo Cities, un servicio que permite a los usuarios a hacer sus propios sitios web y alojarlos en el lugar preciso según el contenido e Internet alcanza el millón de sitios web y una web de nombre The Globe, que ofrece a sus usuarios la oportunidad de personalizar sus experiencias publicando su propio contenido e invitando a conectar a otros usuarios con intereses similares. Ya en 1997 apareció AOL Instant Messenger, uno de los servicios de chat más conocidos en EEUU y empieza a funcionar el famoso buscador, Google. Otras redes sociales como Sixdegrees (algunos consideran que fue el inicio de lo que ahora conocemos como red social). En 1998 surge Friends Reunited, que fue una fuerte inspiración para Facebook; en este mismo año, Google lanza Blogger.

En el año 2000 aparece la "Burbuja de Internet" y se llega a la impresionante cifra de 70 millones de ordenadores conectados a la red; en el 2002 nace Friendster que alcanza 3 millones de usuarios en sólo 3 meses; en el 2003 nacen MySpace, Facebook y Linkedin, a partir de 2004 nacen muchas otras Redes Sociales, tales como Hi5 o Netlog, Digg a modo de portal de noticias sociales, Bebo y Orkut, red social gestionada por Google. En el año 2005 la red más utilizada en los últimos años, Youtube, además, Myspace se convierte en la Red Social más importante de Estados Unidos; en el 2006. Nace Twitter, la red social de microblogging, en este año, Google cuenta con más de 400 millones de búsquedas al día y la red social Facebook continúa recibiendo ofertas millonarias para ser comprada. En España surge Tuenti, que fue una red social dirigida al público más joven. En este mismo año, también aparece Badoo.

Repositorio Institucional - UNASAM - Perú

En 2008, Facebook pasa a ser la Red Social más utilizada a nivel mundial, con más de 200 millones de usuarios (actualmente Facebook cuenta con más de 2167 millones de usuarios). Este año se da a conocer Tumblr a modo de Red Social para hacer la competencia a Twitter.

En 2009 Facebook llega hasta los 400 millones de usuarios y, MySpace, que en su momento fue su competencia, retrocede a la cifra de 57 millones de usuarios. En el año 2010 Google pone en marcha Buzz, la red social que estaba integrada con Gmail.

2.2.1.2. Redes sociales más utilizadas

2.2.1.2.1. Facebook

Fernández (2015) señala que "…es un sitio web de redes sociales. Fue creado originariamente para estudiantes de la Universidad de Harvard, pero ha sido abierto a cualquier otra persona que tenga una cuenta de correo electrónico" (http://ict.edu.ar/renovacion/wp-content/uploads/2015/03/diagnostico-2015-nticx-actic-2.pdf).

Aspani, Sada & Shabot (2012) señalan lo siguiente:

> Facebook es una red social cibernética creada por Mark Zuckerberg, estudiante de Harvard, en febrero del 2004; en un inicio fue utilizada para la comunicación entre alumnos dentro de la Universidad y dos años después comenzó a expandirse al público en general siendo ahora la red social más visitada a nivel mundial permitiendo desarrollos externos e incrementar aplicaciones, estableciendo un modelo que ha sido adoptado por la mayoría de otras redes (p. 108).

Repositorio Institucional - UNASAM - Perú

Facebook, es la red social más popular, que permite mantener contacto con amigos, familiares u otras personas alrededor del mundo; permite intercambiar información y crear grupos, difundir fotografías, videos, se pueden acceder a juegos online; se encuentra al alcance de todos, tiene muchas herramientas que le permiten interactuar con los usuarios, y acerca a la gente lo más posible sin diferenciar si son delincuentes o no.

2.2.1.2.2. YouTube

Bañuelos (2007) señala respecto a YouTube lo siguiente:

> Broadcast Yourself, fue fundado en febrero de 2005 por Chad Hurley, Steve Chen, y Jawed Karim y comprado por Google en noviembre de 2006 por 1,6 billones de dólares. Posee diversos acuerdos comerciales con empresas Como: CBS, BBC, Universal Music Group, Sony Music Group, Warner Music Group, NBA, The Sundance Channel (http://www. razonypalabra.org.mx/ N/n66/varia/jbanuelos.pdf).

Es un sitio web que permite a los usuarios subir, ver y compartir videos, por ello contiene una gran variedad de videos que incluyen videoclips, series, películas y shows.

2.2.1.2.3. WhatsApp

Calero (2014) señala que:

> Etimológicamente, la palabra WhatsApp viene de un juego de palabras en inglés: "*what's up*" que es una frase coloquial que significa *"¿qué pasa?";* app es la abreviatura que se usa para referirse a las aplicaciones. Este término, al trasladarse a otros idiomas, ha ido derivando en nuevas formas; lamás, común y usada en español sigue siendo la original, pero cada vez más va conviviendo con otras variantes como *whatssup, whatsap, watsap, whazap, wassup, wassap, wazap, guasap* (de donde el neologismo verbal guasapear) o incluso el ambiguo *guasa* (…) (p. 90).

Repositorio Institucional - UNASAM - Perú

Gómez (2017) señala que WhatsApp:

> Es un servicio de mensajería instantánea cuyo propósito es comunicar, vía Internet y en tiempo real, a dos o más usuarios entre sí con un mínimo coste económico y empleando mensajes de texto o archivos (audios, videos, imágenes, ubicación geográfica...). Es una aplicación que se puede instalar en todos los smartphones o teléfonos inteligentes, que se ha convertido en el sistema mundial de comunicación por excelencia entre teléfonos móviles, a través de datos o por wifi (p. 52).

2.2.1.2.4. Facebook Messenger

Es sabido que, que esta red social es una aplicación de mensajería desarrollada por Facebook, a través de ella los usuarios se puede comunicar entre sí a través de un chat completo, se puede enviar mensajes de texto, imágenes, archivos, audios, emojis, se puede realizar video llamadas y planear eventos; las conversaciones pueden ser de una persona a otra o entre varias personas, se puede bloquear usuarios en específico.

Facebook Messenger es una aplicación gratuita para teléfonos celulares que permite chatear (mensajería instantánea) entre los usuarios de Facebook y entre dispositivos móviles. Además, posee mensajes de voz, envío de imágenes, videos y emoticonos. Utiliza el protocolo de código abierto MQTT. Originalmente existía una versión Facebook Messenger para PCs, pero se dio oficialmente de baja en marzo de 2014; actualmente sólo se enfocan en su versión para móviles (http://www.alegsa.com.ar/Dic/facebook_messenger.php)

Repositorio Institucional - UNASAM - Perú

2.2.1.2.5. Twitter

Candale (2017) señala que “Twitter es un servicio de mensajería que forma parte de la categoría de los microblogs, que combinan atributos de los blogs con propiedades de las redes sociales como Facebook (https://dialnet. unirioja. es/servlet/articulo?codigo=6319192).

Del Fresno, Daly y Supovitz (citado en Candele, 2017) refiere que “Twitter es en la actualidad el medio social más rápido, simple y económico por donde circula todo tipo de informaciones, noticias, ideas, eventos, rumores, materiales multimedia, etc. emitido desde cualquier medio profesional u otros medios sociales en tiempo real” (*Ibid*.,).

La característica principal de Twitter es que hasta muy recientemente no h a permitido la creación de tweets (publicaciones que una persona quiere difundir) y de comentarios más largos de 140 caracteres, es decir, de aproximadamente una o dos oraciones (*Ibid*.,).

Twitter es una de las redes sociales más famosas en la actualidad, es un lugar donde las personas alrededor del mundo comparten información a través de mensajería instantánea.

2.2.1.2.6. Skype

DifinitiveSolutions señala que Skype es un software que permite mantener una conversación “telefónica” gratuita con otro usuario que tenga instalado el programa y se encuentre “en línea”. Permite que 2,3,4 o 5 personas mantengan una

Repositorio Institucional - UNASAM - Perú

conversación a través de su ordenador con una calidad que, según los responsables de la aplicación, es notablemente superior a la del teléfono. Como utilidad añadida permite tener una sesión de chat tipo Messenger con los usuarios que están conectados (http://recursostic.educacion.es/).

2.2.1.2.7. Linkedin

CodeDimension establece que la red social Linkedin está orientada exclusivamente al segmento laboral, el usuario cuando se registra, lo que hace es dar a conocer su Curriculum Vitae al mundo. Aparte de subir su foto y datos de contacto, podrá especificar sus trabajos actuales, trabajos anteriores, experiencias, un breve extracto, intereses, cursos realizados, que títulos posee, donde estudió y mucho más (https://www.codedimension.com.ar/noticias-sobre-tecnologia).

2.2.1.2.8. Snapchat

Rdstation precisa que Snapchat es una aplicación para compartir fotos, vídeos y texto para dispositivos móviles. Se consideró el símbolo de la posmodernidad por su propuesta de contenidos efímeros conocidos como snaps, que son eliminados unas pocas horas después de la publicación y sólo podrían ser visualizados por los usuarios por el tiempo determinado por el autor (https://www.rdstation.com/es/redes-sociales/).

2.2.1.2.9. Spotify

En su dirección https://support.spotify.com se puede observar que define como un servicio de música, podcasts y vídeos digitales en streaming que te da

Repositorio Institucional - UNASAM - Perú

acceso a millones de canciones y otros contenidos de artistas de todo el mundo. Spotify está disponible en muy diversos dispositivos, como ordenador, teléfono, tablet, altavoces, televisores o coches, y puedes pasar fácilmente de uno a otro con Spotify Connect.

2.2.1.2.10. Instagram

Instagram es una red social donde los usuarios tienen la oportunidad de compartir momentos en la vida de sus amigos mediante el uso y la publicación de fotografías capturadas al instante, las mismas que pueden ser comentadas por los seguidores del usuario posteriormente (http://e-forma.kzgunea.eus).

Los usuarios de Instagram interactúan con el contenido visual, compartiendo de manera instantánea con todos los usuarios de todo el mundo.

2.2.2. Los delitos informáticos

2.2.2.1. Definición del delito informático

De la revisión bibliográfica respecto del delito informático, se puede apreciar que no existe una definición con el que los juristas y estudiosos del derecho estén de acuerdo, por ende, no existe un concepto propio del delito informático; aun así, en el presente informe señalamos alcances conceptuales funcionales a fin de poder comprender en dónde y cómo se desenvuelven estos tipos de delitos.

Lima 1984 (citado en Estrada, 2008) dice que el delito electrónico:

Repositorio Institucional - UNASAM - Perú

> En un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin (https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf).

Miró (2012) señala:

> Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidos a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión (p. 44).

Dávara 1993 (citado en Pérez, 2019) plantea "(…) los denominados delitos informáticos o *computercrime*, definidos como la realización de acciones que, reunido las características que delimitan el concepto de delito, son llevadas a cabo utilizando un elemento informático o vulnerado los derechos del titular del mismo, ya sea de *hardware* o de *software*" (p. 79).

Alcívar, Domenech y Ortiz (2015) señalan que "el delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet" (p. 41).

Repositorio Institucional - UNASAM - Perú

A decir de Jiménez (2017), el delito informático es “una conducta típica y antijurídica, mediante el cual, el delincuente ingresando al cyber-espacio a través del sistema informático, va utilizar a este, como medio o generador de delitos, lesionando o poniendo en peligro bienes jurídicos convencionales o no convencionales culpablemente, protegida por la ley de la materia” (p. 137).

Entonces, los delitos informáticos también son conocidos como ciberdelito, y son todas aquellas acciones antijurídicas que se ejecutan mediante las tecnologías de información y comunicación, ya que estas intervienen no solo como medio, sino también como objeto o como bien jurídico protegido. Estos delitos pueden ser: ataques que se producen contra el derecho a la intimidad; infracciones a la propiedad intelectual a través de la protección de los derechos de autor; falsedades; sabotajes informáticos, fraudes informáticos, amenazas, calumnias e injurias; pornografía infantil; entre otros.

2.2.2.2. Características de los delitos informáticos

Los distintos jurisconsultos coinciden con Morillas 2017 (citado en Pérez, 2019) quien señala las siguientes características:

a) Se trata de delitos cometidos a distancia, sin contacto físico entre agresor y víctima en los que prima la separación temporal y espacial.
b) Se trata de una tipología criminal transfronteriza. La propia esencia del internet o del ciberespacio la lleva implícita. Los delitos informáticos son cometidos cada vez, en mayor medida, por las redes de telecomunicaciones internacionales, por lo que se podría afirmar que este tipo de ilícitos penales complica las técnicas de investigación, debido a su alta complejidad.
c) El creciente número de usuarios y la facilidad de acceso al medio tecnológico para alterar datos, destruir sistemas informáticos. Otro factor determinante es la rápida difusión de información a través de este medio

Repositorio Institucional - UNASAM - Perú

tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.

d) La falta de jerarquía en la red, lo que dificulta la verificación de la información que circula por este medio.

e) El anonimato del perjuicio protegido, la facilidad para encubrir el hecho y la disminución del riesgo de que el autor sea descubierto, gracias a la posibilidad de borrar todas las huellas, sin dejar rastro perceptible una vez perpetrada la acción delictiva. Esto dificulta su persecución tras la comisión de un ilícito penal por este medio.

f) La indeterminación de las víctimas, toda vez que los destinatarios del delito son una pluralidad de personas. Puede ser que el victimario realiza la acción ilícita sin siquiera conocer quiénes serán los destinatarios de esta, como sería el caso del *phishing*, el cual consiste en la búsqueda ilícita de datos personales del sujeto vinculado a claves de acceso a servicio bancarios, suplantándose la identidad de una entidad financiera, imitando o copiando su logo, con la finalidad de solicitarse la introducción de claves de acceso, lo que permite la disposición de los activos de la víctima.

g) Los autores poseen conocimientos informáticos avanzados.

h) Existe una elevada cifra de la criminalidad por las dificultades en la averiguación y de comprobación de almacenamiento, procesamiento y transferencia de datos, también por el desconocimiento o la ignorancia de haber sido víctima de un ataque informático.

2.2.2.3. Sujetos en el delito informático

2.2.2.3.1. Sujeto Activo

Jiménez (2017) señala que:

> (…) las personas que cometen los delitos informáticos son aquellas que poseen características particulares, en base al conocimiento del uno de la informática, que es elemento diferenciador de los delincuentes convencionales (…), los sujetos activos para este tipo de delitos, tienen habilidades para el manejo de los sistemas informáticos (…) (p. 97).

A decir de Lozano 2008 (citado en Jiménez, 2017) los sujetos activos:

> …por su situación laboral se encuentran en lugares estratégicos en donde se maneja información de carácter sensible, o bien son hábiles en el uso de

Repositorio Institucional - UNASAM - Perú

> los sistemas informatizados, aun cuando en muchos casos no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos (p. 99).

Si bien es cierto parte de la doctrina considera que el ciberdelincuente es aquella que posee conocimientos informáticos, no están cierto ello ya que en la actualidad cualquier individuo puede ser autor de estos delitos; por lo que coincidimos con Bramont-Arias (1997) quien señala que "ahora las personas no requieren tener grandes conocimientos de informática para cometer conductas delictuales en esta materia" (p. 71).

Entonces, las personas que cometen los delitos informáticos o ciberdelincuentes poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informático o el uso de los sistemas informatizados; en la actualidad cualquier persona sin un nivel educativo alto posee conocimientos o habilidades en el uso de los sistemas informatizados con la sola rutina que implica incluso la comunicación entre personas; pero se hará algún diferenciación exacta respecto del nivel de conocimiento, y según el delito cometido.

2.2.2.3.2. Sujeto pasivo

Jiménez (2017) señala que es el "(…) titular del derecho atacado o del bien jurídico que tutela la ley y puede ser la persona física, las personas jurídicas, el estado o incluso una pluralidad cualquiera de personas" (p. 108).

Muchos autores coinciden, que, en cuanto al sujeto pasivo, el conocimiento juega un papel importante, ya que en alguno de los casos estos no poseen

Repositorio Institucional - UNASAM - Perú

conocimientos informáticos básicos (no siendo genérico esta idea porque algunos poseen este tipo de conocimientos). Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

2.2.3. Los delitos informáticos en el Derecho Penal Peruano

2.2.3.1. El Derecho Informático

Jiménez (2017) señala que:

> El derecho informático, nació a causa de dos necesidades esenciales: primero, como un ente regulador en el uso de la informática tecnología para adquirir información básica, jurídica, transmisión de datos. Segundo por la preocupación que la sociedad tenía. Preocupación que se fundamente por la siguiente proposición: que a causa de los medios técnicos hoy existentes y los que estarán pronto en el comercio, se puede pronosticar que gran parte de la edición tradicional de obras serán sustituidas absolutamente por tipo electrónico" (p. 78).

Sumer (2019) señal que el Derecho Informático:

> Consiste en el conjunto de normas y principios que regulan los efectos jurídicos nacidos de la informática y de las tecnologías de información y comunicación (TIC). Así, la Ciencia Jurídica analiza las transformaciones que la informática produce en todos los ámbitos de la sociedad con el fin de poder regularlas adecuadamente" (http://www.informaticalegal.com.ar/ derecho-informatico/).

Repositorio Institucional - UNASAM - Perú

2.2.3.2. Ley N° 30096, de delitos informáticos

2.2.3.2.1. Finalidad y objeto de la ley

En el artículo 1° de la ley[1]de delitos informáticos, tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Villavicencio (2014) señala que:

> Esta Ley no responde político criminalmente 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 (p. 8).

Dávila (2015) señala que:

> La Ley de delitos informáticos, establece especialmente penas para atentados contra la integridad de datos informáticos, sistemas informáticos, proposiciones a niños y adolescentes con fines sexuales, incitación a la discriminación, contra la intimidad y el secreto de las comunicaciones como el tráfico ilegal de datos, la interceptación de datos informáticos, suplantación de identidad, abuso de mecanismos y dispositivos informáticos y el fraude informático (http:// resultadolegal.com).

[1] Ley N° 30096, Publicado el 22 octubre 2013.

Repositorio Institucional - UNASAM - Perú

2.2.3.2.2. Bien jurídico tutelado

Valladares 2002 (citado en Villavicencio, 2017) señala que:

> El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la "información" de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo, 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 (p. 6).

Villavicencio (2014) señala que:

> 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 equiparan a los bienes protegidos tradicionales tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), seguridad o fiabilidad del tráfico jurídico probatorio (falsificación de datos o documentos probatorios), etc.

Repositorio Institucional - UNASAM - Perú

2.3. Definición de términos

2.3.1. La informática

De la revisión bibliografía de los diferentes autores, se puede abstraer que la informática se desarrolla a partir del surgimiento de los ordenadores.

De Pablo, Joaquín, Santiago & Medina (2004) señalan que la informática es la ciencia que estudia y se ocupa del tratamiento automático y racional de la información o también como la ciencia de los ordenadores.

Jesús, Galindo, Marco, Prieto y Segret2010 (citado en Jiménez, 2017) definen la informática como:

> (…) el conjunto de conocimientos que actualmente tenemos respecto a un artilugio tecnológico al que llamamos ordenador; el ordenador, en esencia, es una máquina que manipula símbolos; estos símbolos son los que entendemos los humanos como: letras, números, notas musicales, pixeles que forman dibujos, imágenes o videos. Internamente el ordenador convierte todos estos símbolos en bits (ceros o unos), es decir, los digitaliza, y las manipulaciones que se hacen son sencillas: aritmética y lógica elemental. Como la velocidad de manipulación interna del ordenador es enorme, basado en la combinación de operaciones sencillas, nos da la sensación de que está haciendo operaciones mucho más complejas y estas son las que nos interesan a los usuarios; procesar un texto, sumar números, reproducir una melodía, proyectar una fotografía, etc. (p. 26).

De lo señalado, se puede advertir que, al originarse el ordenador, la informática se fue desarrollando de manera paulatina conforme al avance tecnológico, generando así, su fácil acceso y manipulación, pudiendo procesar de manera rápida diversas actividades informáticas, aunque sean complejas.

Repositorio Institucional - UNASAM - Perú

2.3.2. Usuario

Gonzales (2005), señal que el usuario "es el protagonista indiscutible del estudio de cualquier proceso informativo porque sus características individuales y su contexto de referencia laboral, social, económico o político, los aspectos que determinarán su comportamiento con relación a la información" (p. 40).

El usuario por lo general viene a ser, aquel que hace uso de un computador, sistema operativo, servicio informático o el conjunto productos informáticos (hardware y software), a fin de realizar algún proceso informático. El usuario, para acceder a algún servicio o sistema, necesariamente se registra con un nombre o Nick (alias o seudónimo) y a veces con una contraseña.

2.3.3. Ordenador

Jiménez (2017) refiere que "un ordenador es un sistema implementado por programas y elementos de carácter electrónico que en su conjunto permiten procesar y ordenar información. Es el conjunto del Software y hardware" (p. 43). Al ordenador también se le denomina Pcs o computadoras, que pueden clasificarse en distintas modalidades, según la funcionalidad que se darán; una de ellas, por ejemplo: El Smartphone.

En conclusión, un ordenador es un maquina tendiente a ser programado, en la actualidad son electrónicos y digitales, y están compuestos por una parte lógica (los programas de aplicación y los sistemas operativos) y la otra física (memoria, dispositivos de entrada y salida, el CPU, etc.).

Repositorio Institucional - UNASAM - Perú

2.3.4. Archivo

En informática, un archivo es un grupo de datos estructurados que son almacenados en algún medio y pueden ser usados por las aplicaciones (…). La forma en que una computadora organiza, da nombre, almacena y manipula los archivos se denomina sistema de archivos y suele depender del sistema operativo y del medio de almacenamiento (disco duro, disco óptico, etc) (http://www.alegsa.com.ar/Dic/archivo.php).

Un archivo es un conjunto organizado de información digital producidas por personas (físicas o jurídicas), que pueden ser almacenadas en una computadora u otro tipo de dispositivo; estos archivos puede ser documentos, hojas de cálculo, etc.

2.3.5. Dato

Raffino (2019), define un dato informático como:

> Un dato es la representación de una variable que puede ser cuantitativa o cualitativa, indican un valor que se le asigna a las cosas. Los datos son información. Los datos describen en su conjunto nos hablan de hechos empíricos. Un dato por sí solo no puede demostrar demasiado, siempre se evalúa el conjunto para poder examinar los resultados. Para examinarlos, primero hay que organizarlos o tabularlos. Los datos pueden ser generados de forma automática y acumulativa con diferentes tipos de programas informáticos o bien tienen que ser siempre ingresados para formar una base de datos (https://concepto.de/dato/).

Los datos (o dato), son informaciones que son recibidas por el computador por diferentes medios, los mismos que son procesados por los algoritmos de programación, conteniendo estadísticas, números, proposiciones descriptivas, que en su conjunto van a brindar una información completa y específica; siendo una

Repositorio Institucional - UNASAM - Perú

expresión va a describir las características de las entidades sobre las cuales opera un algoritmo.

2.3.6. Información

Chavenato (2006) señala lo siguiente:

> La información es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad la información es un mensaje con significado de un determinado contexto, disponible para uso inmediato y proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones (p. 365).

Para la informática, la información es un conjunto de datos organizados que van a tener una relación directa con el ordenador y que constituyen un mensaje; permite resolver problemas y tomar decisiones y cuyo fin es reducir la incertidumbre o incrementar el conocimiento sobre algo.

2.3.7. Virus informáticos

Rivero (2011) señala que:

> "Los Virus Informáticos son sencillamente programas maliciosos (malwares) que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y, por tanto, una nueva fuente de infección" (https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informáticos/).

Los virus informáticos son programas que tienen como objetivo alterar el funcionamiento de la computadora, sin que el usuario se dé cuenta; infectan archivos del sistema con la finalidad de modificar o destruir de manera intencional archivos y datos, robar, hacer copias o intentar esparcir información. Los más

Repositorio Institucional - UNASAM - Perú

conocidos son: los Troyanos, Hijackers, Spyware, Gusanos, Ransomware, Adware entre otros.

2.3.8. Los Hacker y Cracker

Un **hacker,** es un especialista informático (conoce de programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.), que se dedica a intervenir o un ordenador o equipo tecnológico, unos con el objetivo de hacer alguna alteración o sustracción de la información, y otros con el propósito de explorar los sistemas programables y como aprovecharlas.

Jiménez (2017) refiere que "un hacker es una persona especializada con profundos conocimientos sobre una tecnología, como la informática, electrónica o telecomunicaciones. El hacker conoce todos los terrenos en los que reposa la actual tecnología, pues siempre está en permanente actualización" (p. 57).

Salcedo, Fernandez y Castellanos (2012), señalaron que "los verdaderos hackers tecnológicos son individuos con un alto nivel de conocimiento teleinformático, que en algunos casos se dedican a revisar y proponer soluciones a las vulnerabilidades en redes de computadores y sitios web (p. 118).

Un **cracker**, es considerado como un vandálico virtual. Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión. Es por

Repositorio Institucional - UNASAM - Perú

ello que debemos ser extremadamente precavidos con el manejo de la información que tenemos almacenada en nuestra PC, y protegerla debidamente con algún buen sistema de seguridad (https://tecnologia-informatica.com/que-es-un-cracker/).

De ello, se deduce que un cracker es cualquier persona que viola la seguridad de un sistema informático, de forma similar a como lo hace un hacker, con la diferencia de que lo hace para hacer daño.

Repositorio Institucional - **UNASAM** - Perú

CAPÍTULO III

RESULTADOS Y DISCUSIÓN DE LA INVESTIGACIÓN

3.1. Resultados y discusión doctrinarios

De la investigación realizada, se puede señalar posiciones doctrinarias respecto al problema planteado.

3.1.1. Las redes sociales y su vinculación con los delitos informáticos

Al respecto, Oliva (2017) señala que:

> Las redes sociales pueden ser el medio para cometer delitos cuya ejecución se puede producir dentro o fuera de internet (por ejemplo, un delito de daños informáticos producidos por el envío de links desde Facebook que conducen a sitios webs maliciosos que pueden infectar tu ordenador personal y borrar datos y documentos personales valiosos; un delito de descubrimiento y revelación de secretos donde la víctima es el titular de una cuenta de LinkedIn a la que un tercero accede sin su consentimiento con el fin de conocer el contenido de sus mensajes privados); y en segundo término, las redes sociales pueden ser el lugar donde se realiza la conducta típica del delito (…) (https://www.algoritmolegal.com./).

El avance de la ciencia y la tecnología, surgió con mayor ímpetu con el inicio de internet, el mismo que conforme han transcurrido los años ha tenido un abrupto crecimiento.

Fernández & Grenni (2018) señalan que:

> Esta evolución ha tomado mayor velocidad a partir de la irrupción de las redes sociales, fenómeno que permitió que personas de diferentes lugares, sin importar la distancia, tengan contacto entre sí, pero también puso en situación de mayor vulnerabilidad a aquellos que no toman los recaudos suficientes a la hora de compartir su información. Estos avances se

Repositorio Institucional - UNASAM - Perú

> complementaron y amplificaron con la llegada de los dispositivos portátiles, tablets, smartphones y nuevas redes sociales (p. 101).

Aspis (2018) en esa misma línea señala que:

> (…) el valor de los datos, tanto en el ciberespacio como en las redes inalámbricas, se encuentra también relacionado con el cibercrimen, debido a que los delincuentes informáticos parecieran elegir nuevos objetivos para sus ataques en las nuevas plataformas móviles o las redes sociales informatizadas, donde el usuario o consumidor se encuentra menos advertido de los riesgos, e incluso los desconoce por completo (p. 150).

3.1.2. Derechos fundamentales vulnerados por el uso indiscriminado de las redes sociales

Los derechos fundamentales (personales, políticos, civiles y económicos) están establecidos en la Constitución Política del Estado, gozan del máximo nivel de protección, y son inalienables, inviolables e irrenunciables; estas se encuentran enumeradas y de forma implícita, tal como lo señala el Tribunal Constitucional en el Exp. Nº 417-2005-AA/TC "(…) a enumeración de los derechos fundamentales previstos en la Constitución, y la cláusula de los derechos implícitos o no enumerados, da lugar a que en nuestro ordenamiento todos los derechos fundamentales sean a su vez derechos constitucionales, en tanto es la propia Constitución la que incorpora en el orden constitucional no sólo a los derechos expresamente contemplados en su texto, sino a todos aquellos que, de manera implícita, se deriven de los mismos principios y valores que sirvieron de base histórica y dogmática para el reconocimiento de los derechos fundamentales".

Si bien es cierto el uso de las redes sociales posibilita la comunicación entre las personas recortando espacio y tiempo, también es cierto que al no tener un límite

Repositorio Institucional - UNASAM - Perú

en su uso se exhibe a los usuarios quienes se encuentran en riesgo y son propensos a actividades delictivas vulneradoras de derechos fundamentales; al respecto Garrido (2016) señala que:

> En efecto, si consideramos que el fin y la esencia de las redes sociales se haya en compartir información, amigos, contactos, experiencias, no resulta difícil comprender los recelos y las reservas que las redes sociales despiertan en instituciones, empresas y juristas. Obviamente, vienen a nuestra mente actividades humanas que conllevan riesgo, incluso peligro para la propia vida y la de los demás, y no por ello dejamos de realizarlas, ni desde las instituciones se recomienda abstenerse en su realización. Así el usuario debe identificar y conocer la existencia de los riesgos inherentes a las redes sociales como instrumentos de comunicación, sin que por ello deba denostarse el uso de esta herramienta, al tiempo que se ensalzan sus innegables ventajas y bondades, deben señalarse sus peligros. Además, debe informarse y educarse para una actuación prudente, ordenada y actualizada, que ayude al usuario a actuar con el sentido común y la prudencia deseables en todas las situaciones de la vida cotidiana" (p. 18).

Los derechos fundamentales vulnerados con más frecuencias son:

3.1.2.1. Derecho a la intimidad, al honor y la imagen

El derecho al honor, la intimidad y la propia imagen están reconocidos en el artículo 2 numeral 7, de la Constitución Política del Estado.

Derecho al honor, el Diccionario de la Real Academia define el honor como "la cualidad moral que nos lleva al más severo cumplimiento de los propios deberes respecto del provino y de uno mismo; gloria o buena reputación que sigue a la virtud, al mérito o a las acciones heroicas, la cual trasciende a las familias, personas y acciones mismas de quien se la granjea, (…)" (https://dle.rae.es/?id=KdBUWwv).

La jurisprudencia ha señalado que el honor está estrechamente vinculado con la dignidad de la persona, (…); su objeto es proteger a su titular contra el

Repositorio Institucional - UNASAM - Perú

escarnecimiento o la humillación, ante sí o ante loa demás, e incluso frente al ejercicio arbitrario de las libertades de expresión o información, puesto que la información que se comunique, en ningún caso puede resultar injuriosa o despectiva" (STC 2790-2002-AA/TC).

Este derecho ha sido vulnerado desde siempre, pero ha sido controlado hasta que se hizo común el uso de las redes sociales y se ha visto afectada con mayor dimensión. Al respecto, Ballesteros 2014 (citado por García, 2015) señala:

> Tradicionalmente las intromisiones en el derecho al honor provenían, de forma mayoritaria, de manifestaciones realizadas a través de los medios de comunicación escritos o audiovisuales. La aparición de Internet y la expansión de herramientas y aplicaciones de transmisión de información (especialmente de opinión, como webs, chats, foros, blogs o redes sociales, donde todos nos convertimos en arquitectos de la Red dada la facilidad para introducir contenidos en ellas por cualquier persona), suponen que las posibilidades de vulnerar el derecho al honor son mayores y pueden tener mayor repercusión (p. 13).

Las redes sociales facilitan la proliferación de injurias y calumnias que menoscaban la reputación de la persona, esta facilidad se aprecia con el anonimato que ofrece, ya que no siempre consignan su verdadero nombre o hacen uso de seudónimos, y la fácil difusión de contenidos que son compartidos por miles de usuarios de manera instantánea.

Respecto al derecho a la intimidad, el Tribunal Constitucional en reiteradas jurisprudencias ha señalado que "(…) la protección de la intimidad implica excluir el acceso a terceros de información relacionada con la vida privada de una persona, lo que incluye las comunicaciones, documentos o datos de tipo personal" (STC 09-2014-PI/TC). Riasco (1999) señala que el derecho a la intimidad:

Repositorio Institucional - UNASAM - Perú

> …es un derecho constitucional autónomo pero limitado por otros derechos de igual jerarquía, por el ordenamiento jurídico y por una serie de intereses, valores y principios igualmente constitucionales; pero por sobre todo, se ha considerado también al derecho a la intimidad como un derecho digno de excelsa protección por parte del Estado y de los particulares mismos, ante los pluriofensivos riesgos jurídico-tradicionales así como los devenidos recientemente por los avances tecnológicos de la información y la comunicación"(conocidos en las ciencias de la comunicación, como fenómeno TIC) unidos a los porosos, penetrantes y complejos desarrollos de la informática, electrónica y telemática(p. 28).

Por su parte García (2015) señala que:

> …la privacidad comprende una esfera más amplia que la de la intimidad, que protege de la tenencia y tratamiento, tanto por parte de terceros como de los poderes públicos, de todos los datos vinculados a una persona. Así, este derecho se configura como un poder de disposición de los propios datos, no sólo referidos a la vida privada, sino a cualquier otro ámbito donde una persona despliegue su actividad. En definitiva, la privacidad implica el derecho a mantener ciertos aspectos de nuestra vida fuera del alcance de otras personas. En este sentido, las redes sociales y, en general, las Tecnologías de la Información y Comunicación (TICs), permiten obtener un gran número de datos de un individuo, ponerlos en relación y obtener un perfil exhaustivo del mismo (p. 16).

El avance tecnológico en cuanto a comunicaciones se prestan o son útiles para afectar la intimidad de las personas generando diversos conflictos; este derecho es vulnerado a través del uso de las redes sociales por la exposición de los datos personales, familiares y entre otros por los propios usuarios, así acceder a las redes sociales; estas redes son de acceso de terceros que con facilidad obtienen la información insertada, las mismas que pueden ser compartidas con diversos usuarios imposibilitándose el control de la proliferación de información incluso a nivel mundial.

Al respecto Barriuso (2009) puntualiza que "cuantos más datos estén disponibles para el análisis y más poderosas sean las herramientas de análisis, más

Repositorio Institucional - UNASAM - Perú

significativa será la información que se obtenga y más riesgos habrá de vulnerar la intimidad y las prescripciones sobre protección de datos personales” (p. 304).

Este derecho tiene mayor vulneración en los menores ya que se encuentran expuestos en las redes sociales existentes en Internet.

Señala Rodríguez (2014) que:

> En su resguardo nace el "derecho a la intimidad informática", que no es más que una subespecie del derecho a la intimidad, y se lo ha caracterizado como el derecho que protege a toda persona de las irrupciones arbitrarias en su ámbito de privacidad virtual. Al registrarse y utilizar el servicio, los usuarios vuelcan sus datos particulares: domicilio, lugar de trabajo, edad, estado civil, fotos, comentarios de toda índole relacionados con su vida. Si bien el sistema permite modificar ciertos parámetros de política de privacidad que será necesario configurar según las preferencias del usuario, el principio general que utiliza la red es el de mayor amplitud, ya que permite ver a cualquier persona todo lo ingresado, salvo que sea restringido (configurado en sentido contrario) por el interesado. La realidad es que las opciones predeterminadas permiten el acceso al “muro” personal a más personas que las que el usuario imagina. Así, el derecho a la intimidad de cada uno de los integrantes de la familia, puede verse vulnerado por la publicación por parte de un tercero de datos no deseados (https://p3.usal. edu.ar/index. php/aequitasvirtual/article/view/2382/2959).

El derecho a la propia imagen, se concibe como un derecho de la personalidad, con un contenido propio, específico y diferenciado de los demás, derivado de la dignidad humana y dirigida a proteger la dimensión moral de las personas. Al respecto Alegre (1997) sostiene que:

> Este derecho es concebido por una parte de la doctrina como integrante de la faceta externa del derecho al respeto de la vida privada de la persona, constituyendo el aspecto más externo que es el de la figura humana, que garantiza también un ámbito de autonomía y control respecto de sus atributos más característicos y definitorios de la propia persona, posesión irreductible e inherente a ella. La protección de la imagen de la persona señala esta doctrina, salvaguarda la intimidad y "el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a

Repositorio Institucional - UNASAM - Perú

través de su imagen, su identidad o su voz", nos dirá un autor español (p. 85).

Se puede concluir con lo dicho por Rico (2012) que:

> Desde el punto de vista de los derechos fundamentales, las principales vulneraciones en este ámbito son cometidas por los propios usuarios, aunque en algunos casos los PSRS también asumen responsabilidad, sobre todo en lo que respecta a la privacidad de los participantes. Las violaciones más frecuentes se relacionan con intromisiones ilegítimas en el honor, intimidad y respeto al derecho de la imagen de los usuarios, a los que se suman cuestiones derivadas de la protección de datos de carácter personal, el ejercicio abusivo de la libertad de expresión, violaciones al derecho de la propiedad intelectual, a la protección de los consumidores y de los niños y adolescentes, entre otros aspectos. Siguiendo el objetivo de nuestra investigación, a continuación, nos centraremos en el estudio de la libertad de expresión en Internet, particularmente en las redes sociales que se desarrollan en este entorno (p. 336).

3.1.2.2. Derecho a la propiedad intelectual e industrial

Las obras literarias, las obras artísticas, los productores de fonogramas y los organismos de radiodifusión, están protegidos por el derecho de autor.

La propiedad industrial, se caracteriza por la protección de signos distintivos, en particular marcas de fábrica o de comercio (que distinguen los bienes o servicios de una empresa de los de otras empresas) e indicaciones geográficas (que identifican un producto como originario de un lugar cuando una determinada característica del producto es imputable fundamentalmente a su origen geográfico) (https://www.wto.org/spanish/tratop_s/trips_s/intel1_s.htm).

La protección de esos signos distintivos tiene por finalidad estimular y garantizar una competencia leal y proteger a los consumidores, haciendo que puedan elegir con conocimiento de causa entre diversos productos o servicios. La

Repositorio Institucional - UNASAM - Perú

protección puede durar indefinidamente, siempre que el signo en cuestión siga siendo distintivo (https://blog.derecho-informatico.org/publicaciones/propiedad-intelectual/adpic/).

Respecto a la vulnerabilidad de estos derechos en redes sociales, Diez (2011) señala que "el creciente uso de Internet en la sociedad ha favorecido considerablemente la publicidad, circulación, así como la difusión de determinados derechos de propiedad intelectual, tales como, marcas, avisos comerciales, obras en general e incluso patentes, pero al mismo tiempo fomenta la violación de tales derechos, por lo que constantemente se desarrollan nuevos ilícitos por parte de los particulares…" (https://www.cecamagan.com/la-propiedad-intelectual-en-internet-ciberpirateria/).

3.1.2.2. La libertad sexual y la vida

El ciberacoso sexual se ha convertido en una práctica cotidiana por parte de los ciberdelincuentes que amenazan, hostigan y humillan a sus víctimas; los acosadores sexuales también se han adaptado a las nuevas tecnologías y han encontrado un medio para abordar a sus víctimas sin el mayor reparo. Las víctimas son más fáciles de contactar, porque tanto la víctima como el acosador son usuarios de las diferentes redes sociales.

En ese entendido, no solo la persona adulta sufre ante este ilícito, sino con mayor lesividad los menores de edad, porque son sujetos de máxima vulnerabilidad al estar expuestos haciendo uso de las redes sociales que no tienen parámetros

Repositorio Institucional - UNASAM - Perú

controlados, ni límites ejecutados por los órganos competentes, por lo que puede pasar desapercibido.

El ciberacoso sexual es la persecución de un individuo a otro a través de mensajes, fotografías o videos de carácter sexual. El ciberacosador puede haber accedido a esas fotografías o videos, a través de las redes sociales, con el fin de abusar sexualmente de la víctima, de explotación pornográfica de uso privado o difundirlas en las redes de pedofilia y comercializar con ese material, para extorsionar económicamente o cualquier otro tipo de coacción; todo ello a través dl envió de mensajes amenazantes, la publicación de fotos, videos, rumores para deshonrar la reputación de la víctima online, o enviándolos al entorno de la víctima denigrándola, produciendo miedo con amenazas de daño o de muerte.

3.1.3. La necesidad de limitar el uso de las rede sociales

La violencia digital como la pornografía, captación para trata de personas, ciberbullying (o ciberacoso), trata y tráfico, grooming, que es la seducción ejercida por un adulto para establecer una relación con un infante que finaliza en abuso sexual; sexting, la divulgación de imágenes privadas; que se han convertido en delitos modernos, por así llamarlos, y que necesariamente hacen uso de las tecnologías de información como son las redes sociales.

Estos delitos por su naturaleza son considerados como delitos informáticos, por el solo uso de las tecnologías de información; en nuestro país si bien es cierto existe un catálogo de delitos prescritos en una ley especial, esta no está debidamente actualizada de acuerdo a la magnitud y la época en la que nos encontramos, de los

Repositorio Institucional - UNASAM - Perú

pocos delitos prescritos en la Ley de Delitos Informáticos se puede advertir que solo tiene carácter sancionador, más no preventivo, siendo necesarios para erradicar delitos de esta naturaleza.

De acuerdo a la bibliografía obtenida son los países sub desarrollados o en desarrollo los que más hacen uso de las redes sociales, y son estos países los que notablemente cuentan con un sin fin de actos delictivos que están acabando incluso con el desarrollo normal de la persona y la están llevando a creer que toda violencia permitida es buena.

Establecer algunos límites como prohibir el anonimato en el internet, como prohibir la recolección y tratamiento de información personal sin consentimiento y de una u otra manera monitorear o establecer parámetros para el acceso a las redes sociales mediante la aplicación de estrictos estándares de necesidad y proporcionalidad, evitarían no solo la proliferación de actividades delictivas, como es el delito informáticos, sino también disminuiría la estrecha vinculación de las redes sociales con los delitos comunes.

3.2. Resultados y discusión jurisprudenciales

1) EXP N ° 00442-2017-PA/TC

Se observa:

Que, con fecha 24 de agosto de 2016, don Erick Américo Iriarte Ahón interpone recurso de agravio constitucional contra la resolución de expedida por la Primera Civil de la Corte de la Superior de Justicia de Lima, que declaró

Repositorio Institucional - UNASAM - Perú

improcedente la demanda de amparo contra don Pedro Álvaro Cateriano Bellido, en su calidad de presidente del Consejo de Ministros del Perú, con el objeto de ser desbloqueado de su cuenta personal de Twitter @PCaterianoB, pues, a través de ella, comparte información sobre la institución que dirige. Alega la vulneración de sus derechos fundamentales al acceso de información pública, y a las libertades de información y expresión. (párr. 2 y 3).

El TC señala en sus fundamentos:

El derecho fundamental de acceso a la información pública

6. La demanda señala que, al ser bloqueado del acceso a la cuenta personal de Twitter del expresidente del Consejo de Ministros Cateriano Bellido, denominada @PCaterianoB, se ha vulnerado su derecho de acceso a la información pública.

7. El artículo 2, inciso 5, de la Constitución dice que toda persona tiene derecho a: solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido.

8. Ahora bien, como refiere el recurrente en su demanda (folio 9) y confirma el titular de la cuenta en escrito de 26 de octubre de 2017, esta cuenta fue creada por el demandado en octubre de 2013, es decir, antes de asumir el cargo de presidente del Consejo de Ministros el 2 de abril de 2015.

9. Por otro lado, la PCM tiene su propia cuenta institucional de Twitter: @pcmperu, creada en julio de 2010, la cual constituye el canal del gobierno -

Repositorio Institucional - UNASAM - Perú

conjuntamente con @presidenciaperu, creada en marzo de 2010- para trasmitir información oficial.

10. Según lo informado por la jefa de Prensa e Imagen Institucional de la PCM, mediante Oficio D000129-2019-PCM-OPII de 21 de marzo de 2019, esta entidad en ningún caso ha puesto restricciones o bloqueos a algún usuario, sea a través de la mencionada cuenta o de las que corresponden a sus distintas secretarías.

11. Ciertamente, el artículo 123, inciso 1, de la Constitución establece como primera responsabilidad del presidente del Consejo de Ministros: Ser, después del Presidente de la República, el portavoz autorizado del gobierno.

12. El presidente del Consejo de Ministros, empero, ejerce su función de portavoz del gobierno a través de los canales institucionales destinados a ello. La transmisión de información de asuntos de interés público a través de canales personales no está sometida a las exigencias de acceso propias de canales oficiales.

13. El uso que un funcionario público le dé a su cuenta personal de Twitter no altera su naturaleza privada, es decir, el hecho de que mediante aquella se transmita información que pueda ser de interés público no convierte dicha cuenta en una oficial o institucional.

14. El ciudadano que asume temporalmente un cargo público y hace uso de las herramientas de control de su cuenta privada, a fin de personalizar las formas de interacción con otros usuarios en Twitter, está ejerciendo legítimamente su derecho fundamental a la libertad personal.

Repositorio Institucional - UNASAM - Perú

15. Obligar a alguien a aceptar seguidores en su cuenta personal de Twitter, mediante el desbloqueo de cuentas -sea que se trate de un funcionario o no, e independientemente de las motivaciones que hayan generado el bloqueo de algún usuario - vulneraría su libertad personal.

16. Ciertamente, el escrutinio ciudadano del desempeño de los funcionarios públicos es indispensable para el correcto cumplimiento de sus responsabilidades en una democracia. Sin embargo, ello no debe menoscabar su derecho fundamental a la libertad personal.

17. El hecho de bloquear el acceso a una cuenta personal de Twitter cuya titularidad corresponde a un funcionario público no significa denegarle al bloqueado la información que posee una entidad pública. Los tuits emitidos en dichas cuentas no son comunicaciones oficiales de la entidad pública a la que pertenecen.

18. En tal sentido, el bloqueo de la cuenta @coyotegris, cuyo titular es el recurrente, por parte del aludido expresidente del Consejo de Ministros Cateriano Bellido en su cuenta personal de Twitter no es una actuación constitucionalmente reprochable.

19. La Constitución no permite forzar a nadie - incluyendo a quien ha cumplido en algún momento de su vida funciones públicas de la más alta responsabilidad, como es el caso del demandado en este caso- a interactuar en las redes sociales con quien no quiere.

Repositorio Institucional - UNASAM - Perú

20. Twitter es, esencialmente, una red social. Que, eventualmente, incluya contenido oficial de agencias estatales no altera dicha esencia - y, por tanto, el carácter voluntario de las interacciones que se den en ella.

El derecho fundamental a las libertades de información y de opinión

21. La demanda, además, señala que, al ser bloqueado del acceso a la cuenta personal de Twitter del expresidente del Consejo de Ministros Cateriano Bellido, se ha vulnerado su derecho a la libertad de información y de expresión.

22. El artículo 2, inciso 4, de la Constitución dice que toda persona tiene derecho a: las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley.

23. Este derecho incluye, pues, dos libertades que deben ser distinguidas: de un lado, la de información, que garantiza la libre difusión de hechos que son conocidos por una persona; de otro, la de opinión, que asegura la libre difusión de juicios de valor sobre tales hechos.

24. Ahora bien, un mensaje que transmite información a través de cualquier medio de comunicación puede ser sometido a un test de veracidad, pero no ocurre lo mismo con uno que transmite opiniones o juicios de valor, ya que estas son eminentemente subjetivas.

Repositorio Institucional - UNASAM - Perú

25. La información puede ser calificada de falsa o veraz, según corresponda, o no, a lo ocurrido en el mundo. Ello no sucede con las opiniones. Estas pueden ser calificadas, en todo caso, de acertadas o equivocadas, según se sustenten, o no, en una apreciación correcta de los hechos, utilizando conceptos y criterios pertinentes.

26. Patrick Baylis ha mostrado la correlación entre sentimientos expresados en Twitter y temperatura (https://www.patrickbaylis.com/pdf/BaylisTT.pdf). En esta red social, predominarían las opiniones y juicios de valor, más que la información. Los tuits de Cateriano Bellido podrían no ser la excepción, pero es su derecho.

27. En todo caso, la Constitución protege tanto lo primero como lo segundo. Quien conoce (o cree conocer) algo, puede comunicarlo libremente, si así lo desea; sin embargo, las personas pueden transmitir también sus opiniones con toda libertad, así sean absurdas, prejuiciosas o mal sustentadas.

28. Enfáticamente, el artículo 2, inciso 3, de la Constitución dice que: No hay delito de opinión. A lo más, hay faltas - cuando se emiten juicios de valor disfrazados de información, que vulneran el derecho al honor y buena reputación de las personas.

29. La Constitución protege las libertades de información y de opinión porque entiende que, en los asuntos humanos, nadie es dueño de la verdad, la cual es compleja y elusiva. Además, entiende que, para aproximarse a la verdad, es indispensable que se permita concurrir distintas perspectivas sobre ella.

Repositorio Institucional - UNASAM - Perú

30. El ser bloqueado de la cuenta personal de Twitter del expresidente del Consejo de Ministros demandado no implica que el recurrente esté impedido de difundir o compartir libremente, a través de su propia cuenta en esta misma red social, toda la información que quiera.

31. Tampoco significa que no pueda manifestar libremente todas las opiniones sobre asuntos públicos o privados que estime pertinentes incluyendo juicios de valor respecto al desempeño no solo del expresidente del Consejo de Ministros Cateriano Bellido sino también de este Tribunal Constitucional.

32. Tales libertades de información y de expresión constituyen los cimientos de una sociedad libre como la nuestra.

Si bien es cierto, el Tribunal constitucional en el Exp. N° 00442-2017-PA/TC, se pronunció sobre la naturaleza de una cuenta personal en la red social Twitter, pero solo respecto a un funcionario público y sus repercusiones en los derechos de acceso a la información pública, libertad de información y de opinión en los casos que se bloquea la cuenta de un ciudadano; en sus fundamentos señala que la transmisión de información de asuntos de interés público a través de canales personales no estaría sometida a las exigencias de acceso propias de medios oficiales; y hace referencia a que los derechos predominantes están la libertad de expresión, la libertad de información y el derecho al acceso de una información pública, esto es en tanto y en cuanto tenga una naturaleza pública, es decir, sea esta información de interés social por ser información de un funcionario público que implique dar cuenta de una u otra manera de las actividades que se desarrolla desde cualquier esfera direccional del gobierno, ello no implica que las personas

Repositorio Institucional - UNASAM - Perú

individuales que no tienen que dar cuenta respecto a la vida privada tengan esa facilidad de publicar y encontrar información personal que pone en bandeja para los delincuentes cibernéticos.

Asimismo, el Tribunal Constitucional dentro de sus fundamentos de la sentencia en comento, ha señalado que la Constitución no obliga a nadie a interactuar en las redes sociales con quien no desee, entonces esta al libre albedrío de la persona decidir interactuar o no en redes sociales, es ese libre albedrio que permite al delincuente tener un abanico de posibilidades para cometer sus fechorías y perpetrar delitos que ponen en riesgo la dignidad, la intimidad e incluso la vida de las personas de diferentes edades.

3.2. Resultados y discusión normativos

3.2.1. Derecho interno. -

Se tiene, la Ley especial de delitos informáticos,

3.2.1.1. Ley Nº 30096 y su modificatoria a Ley Nº 30171

"Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."

Repositorio Institucional - UNASAM - Perú

Este tipo penal va a proteger o tutelar la seguridad informática de carácter individual o colectivo; la doctrina coincide en señalar que la norma penal en comento intenta tutelar la "confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos", de conformidad con el Convenio de Budapest.

Jiménez (2017) refiere que respecto a este tipo penal que:

> La descripción legal del presente tipo penal al señalar "El que…", permite determinar el siguiente criterio: nos encontramos ante un delito común, toda vez que el tipo penal no exige ninguna cualidad especial, razón por la cual el sujeto activo en el delito de acceso ilícito, en principio va a ser cualquier persona; no obstante, por la exigencia para el manejo de la informática, es necesario que el sujeto activo tenga las condiciones técnico suficientes para el conocimiento y uso de la informática (p. 405).

De otro lado Pérez (2019) señala que:

> En efecto, la actual descripción típica exige que el autor vulnere unas medidas de seguridad establecidas, en todo o en parte, de un sistema informático. Si la red no lo tuviera, sería de libre acceso, por lo que no podrá darse la figura típica en examen. El hecho de que la medida de seguridad sea de fácil vulneración no libera al agente de responsabilidad penal (no se exige necesariamente un genio de la informática) (p. 108).

Por su parte Villavicencio (2015) indica que:

> …se le puede calificar como un delito de mera actividad, porque esta figura exige el acto de acceder (entrar en un lugar o pasar a él) sin autorización a un sistema informático, vulnerar (transgredir, quebrantar, violar una ley o precepto) las medidas de seguridad, de esta manera se configura el ilícito; por tanto el delito queda consumado en el momento que se vulnera las medidas de seguridad establecida para impedir el acceso ilícito, y para ellos es necesario que se realice esta conducta con dolo. Vgr. el acceso a la cuenta de correo electrónico ajeno protegido mediante una contraseña de seguridad, el acceso no autorizado al sistema informático de una entidad aprovechando las debilidades inadvertidas por la programación (p. 11).

Repositorio Institucional - UNASAM - Perú

Con relación al sujeto pasivo, la doctrina coincide que va a ser cualquier persona, ya sea una persona natural o jurídica, la misma que ejerza la titularidad sobre el derecho de acceso al dato o al sistema informático.

"Artículo 3. Atentado a la integridad de datos informáticos

> El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

La doctrina coincidentemente señala que, en el delito de atentado a la integridad de datos informáticos se va a proteger la integridad, confidencialidad y disponibilidad de los datos; y el sujeto activo va a ser cualquier persona, como lo señala Jiménez (2017) que, "…se encuentre dentro de la clasificación del delincuente informático, pero quienes cometen este tipo de delitos son los crackers o los virucker…" (p. 412).

Para Pérez (2019), "el delito de daño informático se configura cuando el agente ingresa indebidamente a una base de datos, con la finalidad de alterarla, dañarla o destruirla. Aquí el autor o sujeto activo de la conducta busca borrar, suprimir o modificar, sin autorización del propietario o titular, datos de la computadora" (p. 116).

Por otro lado, Villavicencio (2015) señala lo siguiente:

> Esta figura penal sanciona la conducta de dañar (causar detrimento, perjuicio, menoscabo), introducir (entrar en un lugar), borrar (desvanecer,

Repositorio Institucional - UNASAM - Perú

> quitar, hacer que desaparezca algo) deteriorar (empeorar, degenerar), alterar (estropear, dañar, descomponer), suprimir (hacer cesar, hacer desaparecer) y hacer inaccesible los datos informáticos a través de la utilización de las TIC; por la característica que presenta este tipo penal –atentado a la integridad de los datos informático- es clasificado como un delito de mera actividad, porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior, por tanto el delito queda consumado al realizarse cualquiera de estos actos (p. 12).

Es coincidente también que, el sujeto pasivo va a ser cualquier persona, sea esta natural o jurídica, comprendidas las empresas o instituciones públicas o privadas.

> **"Artículo 4. Atentado a la integridad de sistemas informáticos**
>
> El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

Respecto a este tipo penal de la revisión bibliográfica se puede concluir que, tiene como bien jurídico protegido no solo sería la seguridad, sino también la intangibilidad del tráfico de información e la red.

En cuanto al sujeto activo, según Salinas 2013 (citado en Pérez, 2019) el delito de atentado a la integridad de sistemas informáticos podría ser realizado por cualquier persona, pues el tipo penal no exige ninguna cualidad especial en el agente. No obstante, a ello un sector de la doctrina es de opinión de que, dada la

Repositorio Institucional - UNASAM - Perú

naturaleza del aquel delito, solo podrían ser autores quienes tengan avanzados conocimientos de informática; al respecto Palomino 2014 (citado en Pérez, 2019) ello no es una exigencia legislativa, sino un dato que -desde una perspectiva criminológica -puede tomarse en consideración en aras de su investigación.

Por su parte Villavicencio (2015) indica que:

> Está figura penal sanciona las conductas que están dirigidas a inutilizar (hacer inútil, vano o nulo algo) total o parcialmente un sistema informático, entorpecer (retardar, dificultar) e imposibilitar (quitar la posibilidad de ejecutar o conseguir algo) su funcionamiento o la prestación de sus servicios utilizando las TIC; por la característica que presenta este tipo penal -atentado contra la integridad de sistemas informáticos- se clasifica como un delito de resultado, porque para la configuración de este injusto penal no basta con cumplir el tipo que es (inutilizar o perturbar), sino además es necesario que la acción vaya seguida de un resultado (impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios), por tanto el delito se consuma cuando se impide el acceso, imposibilita su funcionamiento, etc., del sistema informático, caso contrario el hecho solo dará lugar a la tentativa.

El sujeto activo, para Jiménez (2017):

> Puede ser cualquier persona natural o jurídica, ya sea institución pública o privada, aunque mayormente en este tipo de delitos, los sujetos pasivos serán las personas jurídicas, ya que estos guardan en sus sistemas una cantidad de información u otros elementos de suma importancia. En otras palabras, el sujeto pasivo va ser el titular de los derechos del sistema informático (sujeto pasivo del delito) o el responsable o administrador de los derechos de aquel sistema informático (sujeto pasivo de la acción).

"Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

Repositorio Institucional - UNASAM - Perú

> El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal".

El bien jurídico que se protege a través de este tipo penal conforme a la revisión bibliográfica es la indemnidad sexual o libertad sexual, la misma que es discutible respecto a que ya se encontraba protegido en el Código Penal.

En esta figura penal el sujeto activo, como señala Jiménez (2017):

> No va a ser aquella persona que tiene grandes conocimientos de informática ni su conducta va a tener como objetivo el de romper medidas de seguridad para sapear o dañar algún dato o sistema informático; sino que el sujeto activo en este tipo penal basta que tenga conocimientos generales de los medios tecnológicos, caracterizándose por sentirse atraído por menores de edad, en la cual son considerados o denominados no como hackers ni crackers sino como pedófilos, pervertidos, desviado sexual o sujeto que comete el "child grooming " (p. 426).

De otro lado Villavicencio (2015) indica que:

> Este tipo sanciona el acto de contactar que significa "establecer contacto o comunicación con alguien", y el término "para" es un elemento subjetivo que determina la intención del sujeto activo y es este elemento que convierte

Repositorio Institucional - UNASAM - Perú

> a la figura penal en un tipo de tendencia interna trascendente (delitos de intención), porque este ilícito "parte interna" requiere de una intención especial, que no corresponde a la parte externa objetiva que en este caso es obtener material pornográfico y/o tener actividades sexuales con el menor; por consiguiente, el tipo legal queda consumado cuando se produce el resultado típico, no siendo necesario que el agente consiga realizar su especifica tendencia trascendente, por estas características se clasifica a esta figura como un delito de resultado cortado, porque en este ilícito el agente persigue un resultado que está más allá del tipo y que ha de producirse por sí solo, sin su intervención y con posterioridad (p. 15).

El sujeto pasivo del delito es el menor de edad que ve afectada su libertad o indemnidad sexual. Es importante resaltar que cada vez es más generalizado el uso de Messenger, chat y redes sociales entre los niños y adolescentes, lo que podría generar la recepción de propuestas de tipo sexual a través de internet (Pérez, 2019, p. 139).

> **"Artículo 7.- Interceptación de datos informáticos**
>
> El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
>
> La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

Repositorio Institucional - UNASAM - Perú

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

Este tipo penal tiene como bien jurídico protegido la intimidad y el secreto de las comunicaciones. El sujeto activo puede ser cualquier persona y respecto al sujeto pasivo Pérez (2019) refiere que "en el delito de interceptación de datos informáticos, puede ser cualquier persona a la que se le intercepten datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, incluidas las emisiones electromagnéticas" (p. 150).

Por su parte Villavicencio (2015) sostiene que:

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

- El primer agravante se aplica cuando la interceptación recaiga sobre información clasificada como secreta, reservada o confidencial, de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública. cuya penalidad oscila entre cinco a ocho años.

- El segundo agravante se aplica cuando la interceptación recaiga sobre información que compromete a la defensa, seguridad o soberanía nacional, cuya penalidad oscila entre ocho a diez años.

- La tercera agravante consiste en la calidad del agente -integrante de una organización criminal- comete el delito como cuya penalidad se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Repositorio Institucional - UNASAM - Perú

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

"Artículo 8. Fraude informático

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

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

Pérez (2019) señala que "el bien jurídico tutelado en el delito de fraude informático es el "patrimonio", desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo respecto a su base de datos informáticos y/o el adecuado funcionamiento de un sistema informático".

Para Villavicencio (2015), este injusto penal –fraude informático- sanciona diversas conductas, entre ellos: diseñar (proyecto o plan), introducir (entrar en un

Repositorio Institucional - UNASAM - Perú

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

"**Artículo 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".

Este tipo penal tiene como bien jurídico protegido la "fe pública". El sujeto activo vendría a ser según Jiménez (2017) el phisher, quien "se hace pasar como una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas" (p. 470). El sujeto pasivo será aquel titular del derecho patrimonial informático vulnerado.

Al respecto Villavicencio (2015) señala que "este tipo penal sanciona el hecho se suplantar (ocupar con malas artes el lugar de alguien, defraudándole el

Repositorio Institucional - UNASAM - Perú

derecho, empleo o favor que disfrutaba) la identidad de una persona natural o jurídica causando algún perjuicio".

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

Con relación a este tipo penal Jiménez (2017) señala que "el convenio de Budapest ha determinado que el bien jurídico sería "la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos" …" (p. 476). Del mismo modo, "el agente del delito va a ser toda persona que tenga la condición técnica suficiente para "fabricar, diseñar, desarrollar, vender, facilitar, distribuir, importar u obtener" software de hacking, contraseñas, programas informáticos o similares, con el fin de cometer alguno de los delitos informáticos…" (p. 478).

Por su parte Villavicencio (2015) sostiene respecto a este tipo penal que:

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

Repositorio Institucional - UNASAM - Perú

mercancía: valer o llegar a cierta cantidad) y obtener (alcanzar, conseguir y lograr algo que se merece, solicita o pretende), para la utilización de mecanismos, programas informáticos, contraseñas, etc., diseñados específicamente para la comisión de los delitos previstos en esta ley. Este artículo es una expresión del adelantamiento de las barreras punitivas porque se sanciona la participación y más aún el sólo hecho de ofrecer un servicio que facilite la comisión de algún delito previsto en la presente ley" (p. 20).

3.2.2. Derecho internacional

Se tiene:

3.2.2.1. El convenio de Budapest

Es un instrumento internacional vinculante en materia penal, que establece herramientas legales para perseguir penalmente aquellos delitos cometidos ya sea en contra de sistemas o medios informáticos, o mediante el uso de los mismos. El Convenio se firmó el 23 de noviembre de 2001 y entró en vigor el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría. Se trata del primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo.

Convenio que en los preámbulos considera tener en cuenta entre otros, el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y trasmitidas por medio de dichas redes (párrafo 6).

Repositorio Institucional - UNASAM - Perú

Así mismo se considera necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se define en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable (párrafo 9).

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Concejo de Europa para la Protección de los Derechos Humanos y de las Libertades fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internaciones aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto a la vida privada (párrafo 10).

Pastorino (2017) refiere que:

> El convenio tiene cuatro capítulos, en los que además de definirse una serie de terminologías en común, se establecen tres ejes esenciales para hacer frente a los delitos informáticos:
>
> En el primer eje se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades

Repositorio Institucional - UNASAM - Perú

de criminalidad informática. Es decir, en este capítulo se definen los delitos y se los clasifica en 4 categorías:

- Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.
- Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
- Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
- Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

El último eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición (https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/).

3.2.3. Derecho comparado

Normatividad jurídica respecto a las redes sociales virtuales:

3.2.3.1. Las Redes Sociales y su regulación en la comunidad europea

Cuenta con las siguientes normas:

Repositorio Institucional - UNASAM - Perú

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Artículo 1.

1. (…) establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. (…) protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales (…)

Artículo 2. Ámbito de aplicación material.

1. (…) se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (…)

Artículo 6. Licitud del tratamiento.

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra

Repositorio Institucional - UNASAM - Perú

persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño (…)

Artículo 7. Condiciones para el consentimiento.

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

Repositorio Institucional - UNASAM - Perú

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Repositorio Institucional - UNASAM - Perú

Artículo 9. Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado; c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se

Repositorio Institucional - UNASAM - Perú

refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, j) el tratamiento es necesario con fines de archivo en interés público,

Repositorio Institucional - UNASAM - Perú

fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. 3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. Tratamiento de datos personales relativos a condenas e infracciones penales.

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Repositorio Institucional - UNASAM - Perú

Artículo 11. Tratamiento que no requiere identificación.

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

Repositorio Institucional - UNASAM - Perú

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del

Repositorio Institucional - UNASAM - Perú

tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará

Repositorio Institucional - UNASAM - Perú

toda la información indicada a continuación: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a

Repositorio Institucional - UNASAM - Perú

presentar una reclamación ante una autoridad de control; e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Repositorio Institucional - UNASAM - Perú

CAPÍTULO IV

VALIDACIÓN DE HIPÓTESIS

4.1. Validación de la hipótesis general

La falta de límites del uso de las redes sociales en el Perú ha ocasionado gran impacto en el incremento de los delitos informáticos, ya que en la actualidad las redes sociales se encuentran al alcance de todo el mundo sin ningún tipo de discriminación; sirviendo así, como medio para la perpetración de delitos tanto por delincuentes comunes, como por aquellos conocedores de las tecnologías de información; si bien es cierto, los delitos cometidos también puede ser denominados tradicionales, pero en algunos casos por el hecho de hacer usos de algún medio informático reviste su naturaleza al perpetración de los denominados delitos informáticos.

Esta hipótesis queda validada con los argumentos doctrinales, normativos y jurisprudenciales, toda vez que las redes sociales van a propiciar el incremento de los delitos informáticos, las nuevas tecnologías de información están adecuadas al fácil acceso e incluso manejo de estas, este fácil acceso no limita que personas que se dedican a delinquir busquen todo tipo de mecanismos para seguir perpetrando delitos.

4.2. Validación de la hipótesis específicas

La doctrina y en alguna una medida la norma reconocen que los delitos informáticos, en la actualidad se han ido incrementado por el uso de las redes sociales, por lo que tendría una vinculación directa con estos delitos; los mismo que

Repositorio Institucional - UNASAM - Perú

están prescritos en la Ley Nº 30096 y su modificación en la Ley 30071, pero que evidentemente no se encuentran debidamente actualizados conforme a la realidad social cibernética. El Código Penal, ni la ley especial para delitos informáticos, no hacen definiciones concernientes a los ciberdelitos, no tiene establecido con exactitud si es solo un medio por el cual se cometen delitos o son delitos con propia naturaleza, lo mismo que ha generado en los diferentes conocedores de la materia discusión coincidiendo pocas veces, pero no dejan de coincidir al señalar que por el uso de las redes sociales se han incrementado incluso nuevas formas de delinquir generándose nuevos conceptos penales que solo han sido adecuadas a los delitos comunes, sin hacer separaciones por el impacto que estos ocasionan.

La falta de límites del uso de las redes sociales está vulnerando derechos fundamentales de la persona, reconocidos en la constitución, como el derecho a la intimidad, al honor y propia imagen, la propiedad intelectual e industrial, la libertad sexual e incluso la propia vida; no es para nadie una novedad que los delincuentes cibernéticos pueden acceder sin ningún desparpajo a la información que se tiene en las diferentes redes sociales existentes, debido a que hasta el momento no existe parámetros que establezcan que tipos de información se pueden añadir, es decir, por ejemplo cualquier persona, incluso haciéndose pasar por otra, puede crear una o varias cuentas en la red social de Facebook, no existiendo ningún tipo de limite por edad, por cantidad de cuentas que se pueda crear, y se te tiene la disponibilidad para incluso para compartir información, imágenes, entre otras cosas, sin ninguna autorización de los afectados.

Repositorio Institucional - UNASAM - Perú

No existe, políticas criminales encaminadas a prevenir la realización de los delitos informáticos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales que minimicen riesgos existentes; si bien es cierto se tiene medios alternos de protección como los delitos informáticos, pero ninguna que limiten el uso indiscriminado de las redes sociales a fin de prevenir ilícitos, existe una gran necesidad de establecer normas que pongan parámetros que protejan al usuario respecto de conductas peligros por la indiscriminada accesibilidad que implica el uso de las redes sociales; claro está, que establecer parámetros o lineamientos no implica afectar la libertad de expresión, el derecho a la información y a la privacidad (esto en cuanto el Estado pueda pretender cierta interceptación o vigilancia legal con el pretexto de establecer parámetros).

El análisis e interpretación doctrinal, jurisprudencial y normativa en los resultados y discusión de resultados respecto a la realidad social cibernética, existen normas penales que castigan ciertos comportamientos realizados mediante medios informáticos (redes sociales) pero que no se encuentran debidamente actualizadas y solo tienen un carácter de castigo que no permitirá reducir estos delitos conocidos como informáticos a través de las redes sociales; no existen medidas preventivas que protejan la privacidad, la seguridad, la integridad, la dignidad y hasta la vida de personas y los más vulnerables como son los niños.

Repositorio Institucional - UNASAM - Perú

CONCLUSIONES

1) La revisión y análisis de la literatura jurídica relacionada a nuestras variables de estudio nos permiten concluir que, las redes sociales, juegan un papel importante como medio de la comisión de delitos informáticos, ya que está al acceso de todas las personas sin distinción de edad; si bien es cierto nuestra legislación ha tenido en consideración el avance de las tecnologías de comunicación e información y las repercusiones que causan con la interacción de la sociedad, es decir, las tecnologías de información han generado nuevas formas de perpetrar delitos, específicamente los delitos informáticos, estas nuevas formas a través delas redes sociales.

2) No hay uniformidad en la doctrina con respecto a que, si las redes sociales son un medio para la comisión de los delitos informáticos, por ello algunos consideran que no es necesario adoptar políticas con respecto a limitar de algún modo el uso de las redes sociales, sin considerar que en la actualidad es de conocimiento de la mayoría de la población que los delitos a través de las redes sociales van en auge, por lo que incluso algunos países a adoptado medidas respecto a su indiscriminado.

Repositorio Institucional - UNASAM - Perú

RECOMENDACIONES

Se recomienda a los legisladores, docentes universitarios, estudiantes que tomen mayor conocimiento con respecto avance de las tecnologías de comunicación, específicamente las redes sociales; para que de una manera u otra se pueda tener amplios aportes al respecto, ya que su crecimiento viene siendo de forma acelerada debido al acceso sin ninguna regulación que los limite, poniendo a los delincuentes cibernéticos en ventaja, vulnerando derechos fundamentales como la propia dignidad e incluso la vida.

Se recomienda a los legisladores tener más responsabilidad con respecto a la protección de víctimas, que se exponen al uso indiscriminado de las redes sociales y se ponen a merced de los victimarios que por una u otra razón conforme a su actuar delictivo vienen sacando provecho a esa falta de algún límite legal de acceso a las redes sociales; establecer límites no implica que se tenga que vulnerar otros derechos como la libertad de expresión o el acceso a la información.

Repositorio Institucional - UNASAM - Perú

REFERENCIAS BIBLIOGRÁFICAS

Alarcón, V. (2018). *GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?* Disponible en: <https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos> [Consultado: 20 de abril del 2019].

Alegre, A. (1997). El derecho a la propia imagen. España: Editorial Tecnos.

Alcivar, C., Domenech, G. y Ortiz, K. (2015). *La seguridad jurídica frente a los delitos informáticos*. Avances, Vol. 10, Nº 12, 41-57.

Barriuso, C. (2009). *Las Redes Sociales y la Protección de Datos Hoy.* Anuario Facultad de Derecho, núm. II, Universidad de Alcalá.

Bramont-Arias, L. (1997). *El delito informático en el Código Penal Peruano*. Lima: Biblioteca de Derecho comparado Vol. 6. Pontificia Universidad Católica del Perú.

Blog de Derecho Informático. *ADPIC – Propiedad Intelectual y Comercio.* Disponible en: < https://blog.derecho-informatico.org/publicaciones/propiedad-intelectual/adpic/> [Consultado: 15 de mayo del 2019].

Chavenato, Ch. (2006). *Introducción a la teoría general de la administración*. México: McGraw-Hill Interamericana.

De Pablo, C., Joaquín, J., Santiago, H. y Medina, S. (2004). *Informática y comunicaciones en la empresa*. Madrid: Esic Editorial.

Repositorio Institucional - UNASAM - Perú

Estrada, M. (2008). *Delitos informáticos*. Disponible en: <https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf> [Consultado: 09 de mayo del 2019].

EUR-Lex (2019). *Diario Oficial de la Unión Europea*. Disponible en: <https://eur-lex.europa.eu/oj/direct-access.html> [Consultado: 25 de mayo del 2019].

García, L. (2015). *El derecho al honor, la intimidad y la propia imagen, en las redes sociales: Especial referencia a los menores de edad.* Trabajo de fin de grado en Derecho. Salamanca: Universidad de Salamanca.

Garrido, E. (2016). Derechos *Fundamentales en las Redes Sociales*. Salamanca: Universidad DSalamanca.

Gonzales, A. (2005). *Los estudios de necesidades el uso de la información; fundamentos y perspectivas actuales*. España: Edickiones TREA.S.L.

Informática Legal. (2019). *Derecho Informático.* Disponible en: < http://www.informaticalegal.com.ar/derecho-informatico/> [Consultado: 03 de mayo del 2019].

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Pérez, J. (2019). *Delitos regulados en leyes penales especiales.* Perú: Gaceta Jurídica.

Ramos, C. *Como hacer una tesis de derechos y no envejecer en el intento.* Lima: Grijley.

Repositorio Institucional - **UNASAM** - Perú

RESOLVING. (2019). *Aspectos legales y leyes que rigen las redes sociales.* Disponible en: <https://resolving.es/leyes-redes-sociales/> [Consultado: 15 de abril del 2019].

Riasco, L. (1999). *El derecho a la intimidad, la visión iusinformática y el delito de los datos personales.* Tesis para optar el título de Doctor en Derecho. Lleida: Universidad de Lleida.

Rico, M. (2012). *El impacto de Internet y las redes sociales en el derecho a la libertad de expresión*. Fronesis. Vol. 19, Nº 3, 331-349.

Rivero, M. (2011). *¿Qué son los virus informáticos?* Disponible en: <https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/> [Consultado: 15 de marzo del 2019].

Robles, L. (2014). *Guía metodológica para la elaboración del proyecto de investigación jurídica.* Perú: FFECAAT.

Salcedo, O., Fernández, C. y Castellanos, L. (2012). *Hackers en la sociedad de la información: análisis de su dinámica desde una perspectiva social*. Visión Electrónica. Vol. 6. N° 1, 115-125.

Sanchez, R. (2018). *El proyecto y la tesis jurídica.* Lima: FFECAAT.

Tecnología Informática. (2015) *¿Qué es un Cracker?* Disponible en: < https://tecnologia-informatica.com/que-es-un-cracker/> [Consultado: 09 de abril del 2019].

Repositorio Institucional - **UNASAM** - Perú

ANEXO

Repositorio Institucional - **UNASAM** - Perú

TITULO: "FALTA DE LIMITES DEL USO DE LAS REDES SOCIALES EN EL PERÚ COMO FACTOR QUE PROPICIA LOS DELITOS DE INFORMATICOS"

FORMULACION DEL PROBLEMA	OBJETIVO DE INVESTIGACION	HIPOTESIS DE INVESTIGACION	VARIABLES	METODOLOGIA
PROBLEMA GENERAL	**OBJETIVO GENERAL**	**HIPOTESIS GENERAL**	**VARIABLE INDEPENDIENTE**	**METODO**
▪ ¿La falta de límites del uso de las redes sociales en el Perú es un factor que propicia los delitos informáticos?	▪Analizar y determinar si la falta de límites del uso de las redes sociales en el Perú es un factor que propicia los delitos informáticos.	▪ La falta de límites del uso de las redes sociales en el Perú ha ocasionado gran impacto en el incremento de los delitos informáticos, ya que en la actualidad las redes sociales se encuentran al alcance de todo el mundo sin ningún tipo de discriminación; sirviendo así, como medio para la perpetración de delitos tanto por delincuentes comunes, como por aquellos conocedores de las tecnologías de información; si bien es cierto, los delitos cometidos también puede ser denominados tradicionales, pero en algunos casos por el hecho de hacer usos de algún medio informático reviste su naturaleza al perpetración de los denominados delitos informáticos.	Límites del uso de las redes sociales **INDICADORES:** ▪ Redes sociales de uso común. ▪ Redes sociales permitidos en el país. ▪ Redes sociales como medio de comunicación.	Tipo. - Dogmática – Teórica Diseño. - No experimental, transversal y descriptivo – explicativo. Métodos: Dogmático, Argumentación Jurídica - Sociológico, Exegético.
PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**	**HIPOTESIS ESPECIFICO**	**VARIABLE DEPENDIENTE**	**TECNICAS E INSTRUMENTOS**

Repositorio Institucional - UNASAM - Perú

▪ ¿Cuáles son los comportamientos que se pueden reconocer como delitos informáticos en las redes sociales, en nuestra legislación peruana? ▪ ¿Qué derechos constitucionales vulnera el uso indiscriminado de las redes sociales? ▪ ¿Existen políticas criminales nacionales encaminadas a prevenir la realización de los delitos informáticos?	▪Analizar y explicar las bases doctrinarias y normativas respecto a que las redes sociales tienen una vinculación directa con los denominados delitos informáticos. ▪Explicar los derechos fundamentales vulnerados por el uso indiscriminado de las redes sociales ▪Obtener información de las políticas criminales nacionales encaminadas a prevenir la realización de los delitos informáticos.	▪ La doctrina y en alguna una medida la norma reconocen que los delitos informáticos, en la actualidad se han ido incrementado por el uso de las redes sociales, por lo que tendría una vinculación directa con estos delitos; los mismo que están prescritos en la Ley Nº 30096 y su modificación en la Ley 30071, pero que evidentemente no se encuentran debidamente actualizados conforme a la realidad social cibernética. ▪ La falta de límites del uso de las redes sociales está vulnerando derechos fundamentales de la persona, reconocidos en la constitución, como el derecho a la intimidad, al honor y propia imagen, la propiedad intelectual e industrial, la libertad sexual e incluso la propia vida. ▪ No existe, políticas criminales encaminadas a prevenir la realización de los delitos informáticos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales que minimicen riesgos existentes; peor aún políticas que limiten el uso indiscriminado de las redes sociales.	INDEPENDIENTE (X): Limites del uso de las redes sociales. **Indicadores:** Redes sociales de uso común. Redes sociales permitidos en el país. Redes sociales como medio de comunicación. DEPENDIENTE (Y): la falta de limites es un factor que propicia los delitos informáticos. Indicadores: El uso indiscriminado de las redes sociales. Acciones ilegales realizadas a través de las redes sociales.	Encuestas Análisis documental (Análisis de contenido) Bibliográfica (Fichas: Textual, de resumen, de comentario)

Repositorio Institucional - UNASAM - Perú

Repositorio Institucional - **UNASAM** - Perú