UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

INSTITUTO DE INVESTIGACIONES, SEMINARIOS Y TESIS

TESIS DE GRADO

(Tesis de grado para optar el grado de Licenciatura en Derecho)

"DELITOS INFORMÁTICOS QUE SE DAN CON MAYOR FRECUENCIA EN LAS REDES SOCIALES EN LA CIUDADANÍA DEL MUNICIPIO DE LA PAZ DURANTE LOS AÑOS 2012 AL 2021; Y SU REGULACIÓN JURISDICCIONAL PENAL"

Postulante: Esteban Janco Morales
Tutor: Dr. Israel Hugo Centellas Vargas

La Paz - Bolivia
2023

DEDICATORIA:

A mi papá, Teófilo Janco Huarayo

A mi mamá, Emiliana Morales Vasques

A mi esposa, Jenny Lima Pérez

Y, a mi suegra Ganará Pérez Bautista

AGRADECIMIENTOS:

Dra. Maby Gema Arias Flores

Dr. Israel Hugo Centellas Vargas

Dr. Justiniano Segales Dante Fedor

Dr. Marcelo Fernández Iraola

Ph. D. Karina Medinaceli Díaz

Dr. Luis Fernando Zegarra Castro

RESUMEN

Con el crecimiento vertiginoso de las tecnologías de la información y la comunicación (TIC), y actualmente con la Inteligencia Artificial, las redes sociales se han convertido en un nuevo contexto social de relacionamiento (proximidades virtuales), convirtiéndose en un componente indispensable para la humanidad, en la cual, las personas pueden comunicarse desde cualquier parte del planeta e intercambiar todo tipo de información.

En ese contexto, los delitos informáticos en las redes sociales han evolucionado exponencialmente, creando nuevas y sofisticadas formas de delinquir desde el anonimato, dificultando su descubrimiento, persecución y prueba; asimismo, el derecho no puede ir a la par de las nuevas tecnologías y por ende no puede regularlas, dejando en la indefensión de las víctimas.

En cuanto a la Constitución Política del Estado Boliviano (2009) garantiza el derecho a la comunicación y a la información; asimismo, garantiza el derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad; por otro lado, el Código Penal Boliviano hace referencia únicamente a la: manipulación informática y a la alteración, acceso y uso indebido de datos informáticos.

En consecuencia, los delitos informáticos más frecuentes en redes sociales en el municipio de La Paz, son: estafa y fraude, acoso cibernético, suplantación de identidad, trata y tráfico de personas, sexting, difamación, calumnia y amenazas, pornografía infantil, phishing, grooming y la violación a la propiedad intelectual, etc.; todo esto se

desarrolla en las redes sociales más utilizadas en Bolivia como ser: WhatsApp, Facebook, YouTube, TikTok, Instagram, Telegram, Linkedln, etc. y otras redes sociales en gestación, como la Inteligencia Artificial.

Por lo tanto, los delitos informáticos en las redes sociales surgen con la evolución de las Tecnologías de Información y Comunicación, y últimamente con la Inteligencia Artificial, conformando un nuevo panorama social (proximidades virtuales), y con ella, la aparición de nuevas y sofisticadas formas de delinquir desde el anonimato; en la cual, el derecho no puede ir a la par de las nuevas tecnologías y por ende no puede regularlos adecuadamente, dejándolos en la indefensión de las víctimas.

ABSTRACT

With the rapid growth of information and communication technologies (ICT), and currently with Artificial Intelligence, social networks have become a new social context of relationship (virtual proximity), becoming an essential component for humanity. , in which people can communicate from anywhere on the planet and exchange all kinds of information.

In this context, computer crimes in social networks have evolved exponentially, creating new and sophisticated forms of crime from anonymity, making it difficult to discover, prosecute and prove it; likewise, the law cannot keep up with new technologies and therefore cannot regulate them, leaving the victims defenseless.

Regarding the Political Constitution of the Bolivian State (2009), it guarantees the right to communication and information; likewise, it guarantees the right to privacy, intimacy, honor, self-image and dignity; on the other hand, the Bolivian Criminal Code refers only to: computer manipulation and alteration, access and improper use of computer data.

Consequently, the most frequent computer crimes in social networks in the municipality of La Paz are: scam and fraud, cyber bullying, identity theft, human trafficking and trafficking, sexting, defamation, slander and threats, child pornography, phishing, grooming and violation of intellectual property, etc.; All this is developed in the most used social networks in Bolivia such as: WhatsApp, Facebook, YouTube, TikTok, Instagram, Telegram, Linkedln, etc. and other social networks in the making, such as Artificial Intelligence.

Therefore, computer crimes in social networks arise with the evolution of Information and Communication Technologies, and lately with Artificial Intelligence, shaping a new social panorama (virtual proximities), and with it, the appearance of new and sophisticated forms of crime from anonymity; in which, the law cannot go hand in hand with new technologies and therefore cannot regulate them adequately, leaving them defenseless for the victims.

ÍNDICE

DISEÑO METODOLÓGICO

CAPÍTULO II

LOS DELITOS INFORMÁTICOS MÁS FRECUENTES EN LAS REDES SOCIALES DE BOLIVIA, Y SU REGULACIÓN JURISDICCIONAL PENAL

CAPÍTULO III

MARCO PRÁCTICO

LOS DELITOS INFORMÁTICOS MÁS FRECUENTES EN LAS REDES SOCIALES EN EL MUNICIPIO DE LA PAZ

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

DISEÑO METODOLÓGICO

1 Enunciado del Título del Tema

Delitos informáticos que se dan con mayor frecuencia en las redes sociales en la ciudadanía del municipio de La Paz durante los años 2012 al 2021; y su regulación jurisdiccional penal.

2 Identificación del Problema

Los delitos informáticos en las redes sociales surgen gracias al internet y el crecimiento vertiginoso de las tecnologías de la información y la comunicación; según Téllez (2008), el internet en los últimos años se ha convirtió en un recurso vital para la humanidad en muchos aspectos; y la revolución digital de las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimiento en todo el planeta. Por lo tanto, el internet y las TIC se han convertido en un componente indispensable para la humanidad, y en ese contexto, las redes sociales conforman un nuevo panorama social, dando lugar a la aparición de nuevos tipos de delitos.

En cuanto a su conceptualización y/o definición de los términos: “delitos informáticos” y “redes sociales”, no se puede encontrar un único concepto generalizado; según Hernández (2009) la doctrina no encuentra un concepto unitario de delito informático, incluso algunos autores admiten la imposibilidad de dar una definición; de igual manera, el termino red social es conceptualizado por las diferentes disciplinas, por el

cual no se cuenta con un concepto generalizado (Bastida, 2019). En síntesis, no se tiene una clara conceptualización de los términos de delitos informático y redes sociales.

Por último, el Código Penal Boliviano hace referencia a los delitos informáticos en sus artículos 363 bis y 363 ter de forma anticuada, como se cita a continuación:

> Artículo 363 bis. - (Manipulación informática). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procedimiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días. Artículo 363 ter. - (Alteración, acceso y uso indebido de datos informáticos). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.

Por lo tanto, en los artículos citados anteriormente hace referencia a los delitos cometidos exclusivamente por ordenadores, y no hace referencia a las nuevas Tecnologías de Información y Comunicación; asimismo, no menciona en ninguna parte del Código Penal sobre los delitos informáticos en redes sociales, dando lugar a la impunidad de los delincuentes.

3 Problematización

¿Cuáles son los delitos informáticos más frecuentes que se dan en las redes sociales en la ciudadanía del municipio de La Paz durante los últimos diez años; y cuál es su regulación jurisdiccional penal?

4 Delimitación de la Investigación

4.1 Delimitación Temática

En el presente estudio de investigación nos basaremos en el método cualitativo; asimismo, se realizara una descripción y análisis de los delitos informáticos más comunes que se dan en las redes sociales en la ciudadanía del municipio de La Paz durante los últimos diez años; y, su descripción de su tratamiento jurisdiccional penal boliviano.

En una primera instancia, trataremos de conceptualizar los términos de “delito informático” y “redes sociales”; posteriormente, pasaremos a clasificar los delitos más comunes que se dan en las redes sociales en el municipio de La Paz durante los últimos diez años. En segunda instancia, revisaremos y analizaremos toda la normativa que tenga relación con el tema de investigación.

4.2 Delimitación Espacial

El tema a investigar: los delitos informáticos que se dan con mayor frecuencia en las redes sociales, es amplio y universal; por ello y por la amplitud geográfica y temática que incumbe a la investigación, nos abocaremos únicamente en el municipio de La Paz como delimitación espacial de investigación.

4.3 Delimitación Temporal

La presente investigación toma como delimitación temporal el lapso de diez años, es decir, se recabará toda la información y datos disponibles entre los periodos 2012 hasta el año 2021; en efecto, en estos últimos años se incrementó el uso de las redes sociales y con ello los delitos informáticos.

5 Fundamentación e Importancia de la Investigación

Con respecto a los fundamentos de nuestra investigación tenemos; por una parte, el avance gigantesco del internet conjuntamente con las nuevas tecnologías de información y comunicación que se incrustan en toda la sociedad, cambiando de forma radical la forma de vivir; en este contexto, los delincuentes encuentran nuevas y sofisticadas formas de delinquir, dando lugar a un incremento vertiginoso de los delitos informáticos en las redes sociales.

A su vez, la importancia del tema radica en poner al descubierto: por un lado, clasificar los delitos más comunes que se cometen a través de las redes sociales; por otro lado, dejar al descubierto su escasa regulación jurisdiccional penal con la que cuenta; y, por último, proponer una propuesta de ley que pueda mitigar dichos delitos.

Por lo tanto, el internet y los grandes avances tecnológicos en la información y las telecomunicaciones, deslumbran nuevas y sofisticadas formas de delinquir en las redes sociales, al mismo tiempo que las normativas no estarían pudiendo estar a la par de estos nuevos tipos de delitos; de ahí que, nuestra carrera profesional nos obliga a poder

contrarrestar estos nuevos tipos de delitos que se manifiestan a través del internet y las nuevas tecnologías de comunicación.

6 Objetivos de la Investigación

6.1 Objetivo General

Determinar los delitos informáticos que se dan con mayor frecuencia en las redes sociales en la ciudadanía del municipio de La Paz durante los años 2012 al 2021; y precisar su regulación jurisdiccional penal.

6.2 Objetivos Específicos

- Describir sus características, conceptos y evolución de los delitos informáticos en las redes sociales.
- Identificar los delitos informáticos más frecuentes que se dan en las redes sociales en la ciudadanía del municipio de La Paz.
- Determinar la situación jurídica de los delitos informáticos en redes sociales.
- Proponer una propuesta de ley.

7 Marco Histórico que Sustenta la Investigación

Los inicios del internet se remontan a los años 60 en plena guerra fría entre Estados Unidos y la ex Unión Soviética, es así que los Estados Unidos en 1958 crea ARPA (Advanced Research Projects Agency) exclusivamente militar para tener acceso a la información militar desde cualquier parte de su territorio; todo esto debido a que la Unión Soviética lanza el primer satélite Sputnik en 1957.

> Así, en 1969 se estableció ARPANET, la primera red sin nodos centrales de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Angeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI). La primera transmisión tuvo lugar el 29 de octubre de 1969, entre UCLA y SRI. (Trigo, 2004, p. 23).

Asimismo, para 1971 ya había 15 ordenadores conectados en todo el territorio Norte Americano; y en 1973 ARPANET se conectaría con las universidades de Gran Bretaña (College of London) y Noruega (Norwegian Seismic Array), dando lugar a la internacionalización del internet. De ahí que, para 1982 ARPA manifiesta como protocolo estándar el TCP/IP (Transfer Control Procotol/Internet Protocol), dando lugar al nacimiento del internet (Trigo, 2004).

> Cuando arrancó la década del ´90 se estandarizaron los protocolos de conexión TCP/IP y fue entonces que Berners-Lee diseño el primer sistema de comunicación entre un servidor y el cliente. Aquello fue el inicio de la *World Wide Web* (WWW). Poco después, en 1993, se unificó el lenguaje Web gracias al *Hypertext Markup Languaje* (HTML), que aún hoy se usa. (Zanoni, 2008, p.22)

Por consiguiente, con el gran avance del internet y las tecnologías de la información y la comunicación se acrecientan los delitos informáticos, como señalan Loredo y Ramírez (2013) “Entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes se encuentran: la capacidad de cometer delitos en y desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros” (p. 45).

De hecho, durante la década de los setenta hay un incremento en la utilización del internet y como consecuencia un incremento de los ordenadores (sobre todo en el ámbito empresarial), de ahí que nace la delincuencia informática, como afirma Hernández (2009) "la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia económica, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc." (p. 229).

En la década de los noventa aparecen nuevas formas de delitos informáticos, como lo señala Hernández (2009):

> La expansión de Internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán justamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la Red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba. (p. 230)

En este panorama de auge del internet y las computadoras, surgen las redes sociales y como "primer antecedente se remonta a 1995, cuando un ex estudiante universitario de los Estados Unidos creó una red social en Internet, a la que llamó classmates.com (compañeros de clase.com), justamente para mantener el contacto con sus antiguos compañeros de estudio" (Morduchowicz et al., 2010, p. 3).

Asimismo, dos años más tarde "en 1997, cuando aparece SixDegrees.com (seis grados.com) se genera en realidad el primer sitio de redes sociales, tal y como lo

conocemos hoy, que permite crear perfiles de usuarios y listas de “amigos”” (Morduchowicz et al., 2010, p. 3).

De hecho, las primeras redes sociales basadas en círculos de amigos en línea aparecieron entre los años 2001 y 2002, como relaciones sociales en las comunidades virtuales; y se popularizaron en el 2003 como espacios de intereses afines (Morduchowicz et al., 2010).

8 Marco Teórico que Sustenta la Investigación

En el año de 1969, se produjo la primera conexión entre computadoras, conocida como “ARPANET”, de ahí que surgió lo que hoy conocemos como internet, dando lugar a una gran revolución tecnológica global, una red que mantiene conectados a millones de usuarios por todo el planeta.

En la actualidad, gracias a internet y a los avances tecnológicos de los últimos tiempos, podemos obtener y publicar información, así como comunicarnos, desde cualquier lugar y en cualquier momento; de ahí que, las redes sociales han supuesto un cambio en el modo que tenemos de relacionarnos en sociedad, pasando a conformar un nuevo contexto social, siendo un componente indispensable en la vida de las personas.

> Se puede afirmar que el crecimiento de las redes sociales en internet ha sido exponencial a partir de la etapa de la Web 2.0, donde el usuario de internet dejó de ser un simple observador y consumidor de contenidos a un verdadero generador de los mismos. El usuario asumió entonces un doble papel: el de consumidor y el de creador. Son los propios usuarios los que crearon una gran base de datos propios y

> ajenos con información relativa a edad, sexo, localización, intereses, etc. (Sanz, 2014, p. 7)

Bajo esa tendencia, y tomando en cuenta que el ser humano es un ser social por naturaleza, las redes sociales pueden ser entendidas como estructuras sociales integradas por diferentes grupos de personas, que se conectan entre sí, por uno o varios tipos de motivaciones, tales como relaciones interpersonales, laborales, promoción política; además de compartir experiencias, fotografías, vídeos, así como opiniones e información.

En la actualidad, internet cuenta con un sin número de páginas web y dominios diferentes, con aplicaciones y servicios disponibles para cualquier usuario; entre dichos servicios se encuentran las muy nombradas, redes sociales tales como: Facebook, WhatsApp, YouTube, TikTok, Telegram, Twitter, etc.

En este contexto y tomando en cuenta de que:

> En todas las facetas de la actividad humana existe el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia. (Camacho, 1987, como se citó en Chávez, 2012, p. 25)

Además, se podría decir que en las sociedades modernas el delito y su sanción son impuestos por los Estados, como afirma Machicado (2010):

> El delito es una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena. Es la ley la que establece que hechos son delitos, es la ley la que nomina que hecho va ser considerado como delito, es la ley la que

> designa y fija caracteres delictuales a un hecho, si en algún momento esta ley es abrogada el delito desaparece. El delito es artificial. (p. 3)

De ahí que, podemos concluir que los delitos informáticos en redes sociales se incrementan exponencialmente a la par de la Tecnología de Información y Comunicación; la misma que mantiene conectado a millones de personas por todo el mundo (obteniendo y publicar información, como un nuevo modo de relacionarnos); bajo este contexto, las leyes deben estar a la par de estos nuevos tipos de delitos.

9 Marco Conceptual

El delito para Machicado (2010), "Esta concepción de delito fue desarrollada por Karl Binding, Ernst von Beling, Max Ernest Mayer, Edmundo Mezger. El delito es la acción u omisión voluntaria típicamente antijurídica y culpable" (p. 6). De modo semejante, el delito es una acción típica, antijurídica, imputable, culpable, sometida a una acción penal (Wikipedia).

Por otro lado, tenemos el concepto de Internet, que es una red informática mundial, un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP (Wikipedia); para Belloch (2012) el internet "Es básicamente un sistema mundial de comunicaciones que permite acceder a información disponible en cualquier servidor mundial, así como interconectar y comunicar a ciudadanos alejados temporal o físicamente" (p. 2).

Del examen anterior se advierte (u observa) que los delitos informáticos según Hernández (2009) afirma lo siguiente:

> Las definiciones que a lo largo de los últimos cuarenta años se han aportado del concepto de delito informático van necesariamente unidas a la evolución que ha sufrido la implantación de las TICs en la sociedad y a las propias conductas delictivas, o merecedoras de serlo, vinculadas con las nuevas tecnologías de la información y de la comunicación. (p. 230)

Así mismo el profesor Téllez (2008) afirma que “los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico) (p. 188).

Otra definición destacable es la establecida por Loredo y Ramírez (2013) quien tomo como referencia a:

> Camacho Losa, citada por Leyre Hernández, quien considera como delito informático: “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas”. (p. 45)

Con respecto a las redes sociales, Morduchowicz et al (2010) afirman lo siguiente:

> Las redes sociales son “comunidades virtuales”. Es decir, plataformas de Internet que agrupan a personas que se relacionan entre sí y comparten información e intereses comunes. Este es justamente su principal objetivo: entablar contactos con

gente, ya sea para re encontrarse con antiguos vínculos o para generar nuevas amistades. (p. 3)

"Una red social es una estructura social compuesta por un conjunto de actores y uno o más lazos o relaciones definidos entre ellos" (Wikipedia); además, "las redes sociales en Internet son sistemas que permiten establecer relaciones con otros usuarios a los que se puede o no conocer en la realidad (Prato y Villoria, p. 18)

En otras palabras, más técnicas:

> Una red social es una estructura social que se puede representar en forma de uno o varios grafos en el cual los nodos representan individuos (a veces denominados actores) y las aristas, relaciones entre ellos. Las relaciones pueden ser de distinto tipo, como intercambios financieros, amistad, o rutas aéreas. (Prato y Villoria, p. 18)

Por consiguiente, podemos terminar diciendo que los delitos informáticos en redes sociales, son aquellos delitos cometidos en las comunidades virtuales, con la utilización de las Tecnologías de Información y Comunicación, provocando un perjuicio a las personas.

10 Hipótesis de Trabajo de Investigación

Los delitos informáticos más frecuentes que se dan en las redes sociales en la ciudadanía del municipio de La Paz, durante los últimos diez años, cuentan con una escasa regulación jurisdiccional penal, dando lugar a la impunidad de los delincuentes.

11 Variables de la Investigación

11.1 Variable Independiente

Escasa regulación jurisdiccional penal por parte del Estado boliviano, en los delitos informáticos en las redes sociales.

11.2 Variable Dependiente

Gran parte de los delitos informáticos cometidos por las redes sociales quedan en la impunidad y a expensas de las víctimas.

12 Metodología de Investigación

Esta investigación se realizó bajo un enfoque cualitativo mediante un diseño descriptivo interpretativo; asimismo realizaremos la recopilación de información, con la cual, demostraremos los objetivos trazados, así como la problemática, en función de la hipótesis.

12.1 Métodos

Método Descriptivo. Como método principal que utilizaremos para nuestra investigación, será el método descriptivo, con el cual podremos describir los delitos informáticos más comunes que se dan en las redes sociales; al mismo tiempo que describiremos su regulación jurisdiccional penal. Sampieri (1998) afirma: “El propósito del investigador es describir situaciones y eventos. Esto es, decir cómo es y cómo se manifiesta determinado fenómeno” (p. 60).

Método Deductivo. Nos permitirá partir de conocimientos generales hacia situaciones particulares; según Rodríguez (1994) “La deducción es el razonamiento mental que conduce de lo general a lo particular y permite extender los conocimientos que se tienen sobre una clase determinada de fenómenos a otro cualquiera que pertenezca a esa misma clase” (p. 37). Por lo tanto, el método deductivo es una estrategia de razonamiento empleada para deducir conclusiones lógicas a partir de una serie de premisas o principios.

Método Inductivo. Nos permitirá dar conclusiones universales partiendo de los estudios particulares de los hechos. “Según Bacon, las observaciones se hacían sobre fenómenos particulares de una clase y luego a partir de ellos se hacían inferencias de la clase entera” (Rodríguez y Pérez, 2017, p. 187). Por lo tanto, el método inductivo es una estrategia de razonamiento que se basa en la inducción, para ello, procede a partir de premisas particulares para generar conclusiones generales.

Método de Análisis. Es un proceso cognoscitivo de los hechos, Rodríguez y Pérez (2017) afirman: “El análisis es un procedimiento lógico que posibilita descomponer mentalmente un todo en sus partes y cualidades, en sus múltiples relaciones, propiedades y componentes. Permite estudiar el comportamiento de cada parte” (p.186). En síntesis, el método analítico es un método de investigación que consiste en la desmembración de un todo descomponiéndolo en sus partes o elementos para observar las causas, naturaleza y los efectos.

Método Dogmático Jurídico. Tiene como objeto de estudio el derecho positivo vigente, “lo que se investiga es la norma jurídica en su contenido abstracto, su fin es la

determinación del contenido normativo del orden jurídico en el contexto de validez" (Clavijo et al., 2014, p. 48). Por lo tanto, el método de investigación dogmático propone investigar el ordenamiento jurídico para saber si está acorde con lo que necesita la sociedad y, de este modo, poder mejorarlo.

12.2 Técnicas

Revisión Bibliográfica. Una revisión bibliográfica, es un trabajo que analiza y discute artículos e informes, generalmente científicos y académicos. Mediante esta técnica, realizaremos una investigación documental, es decir, extraer información valida y confiable de libros, referencias electrónicas o de la web, así como de códigos y leyes vigentes que contengan información, ideas, datos y evidencias sobre nuestro tema de investigación, así como la evaluación efectiva de estos documentos.

Entrevistas. Se define como una conversación que se propone con un fin determinado distinto al simple hecho de conversar, para recabar datos. En este contexto, las entrevistas estarán dirigidas a expertos en la temática de nuestra investigación, así como a autoridades que tengan una relación directa con el tema a investigar; con el propósito de conocer su posición, y de esta manera, responder las preguntas de nuestra investigación.

Encuesta. La encuesta es una técnica que se lleva a cabo mediante la aplicación de un cuestionario previamente diseñado a una muestra de personas. Por lo tanto, con el objetivo de tener un panorama general de nuestro tema de investigación, realizaremos una encuesta a la ciudadanía del municipio de La Paz, mediante una muestra representativa, con la cual recopilaremos datos e información sobre nuestro tema de investigación.

DESARROLLO DEL DISEÑO DE PRUEBA DE LA TESIS

INTRODUCCIÓN

Con el crecimiento vertiginoso de las Tecnologías de la Información y la Comunicación (TIC) y actualmente con la Inteligencia Artificial, las redes sociales se han convertido en un nuevo contexto social de relacionamiento (proximidades virtuales); en ese contexto, los delitos informáticos en redes sociales también han evolucionado creando nuevas y sofisticadas formas de delinquir, y que el derecho no está regulando, dejando en la indefensión de las víctimas.

Por las siguientes razones, nuestro objetivo general es determinar los delitos informáticos más frecuentes que se dan en las redes sociales en la ciudadanía del municipio de La Paz durante los últimos diez años; asimismo, precisar su regulación jurisdiccional penal; para tal efecto, describiremos sus características y conceptos de los delitos informáticos en las redes sociales, así como los delitos más frecuentes; y por último, propondremos una propuesta de ley.

De manera que, para cumplir con nuestro objetivo de investigación, utilizaremos el método cualitativo mediante un diseño descriptivo interpretativo; asimismo, las técnicas que utilizaremos son: revisión bibliográfica de libros, artículos, referencias electrónicas y la normativa vigente; posteriormente, realizaremos entrevistas a los expertos en delitos informáticos en redes sociales, así como a instituciones; y por último, realizaremos una encuesta a la jóvenes del municipio de La Paz.

Por consiguiente, el trabajo de investigación está conformado por los siguientes partes: en primer lugar, tenemos el “Diseño Metodológico” de la investigación; y en

segundo lugar, tenemos el “desarrollo del diseño de prueba de la tesis” que consta de los siguientes capítulos:

Capítulo I. “Delitos Informáticos y Redes Sociales”, en este capítulo desarrollamos sus antecedentes, características, definiciones, elementos, tipos de redes sociales y las principales redes sociales en la actualidad.

Capitulo II “Los Delitos Informáticos Más Frecuentes en las Redes Sociales de Bolivia, y su Regulación Jurisdiccional Penal”, en la misma desarrollamos los antecedentes del internet en Bolivia, los delitos informáticos más frecuentes que se dan en las redes sociales de Bolivia, legislación nacional y la regulación jurisdiccional penal en Bolivia.

Capitulo III “Marco Práctico” de “los delitos informáticos más frecuentes en las redes sociales en el municipio de La Paz”, en este capítulo desarrollaremos un análisis e interpretación de los resultados de las encuestas; así como del análisis de las entrevistas.

Capitulo IV “Conclusiones y Recomendaciones”; en la conclusión final del trabajo de investigación presentamos la información más relevante de todo el trabajo de investigación; asimismo, las recomendaciones más pertinentes; y por último se presenta una propuesta de ley para su tratamiento en el parlamento boliviano.

CAPÍTULO I

DELITOS INFORMÁTICOS Y REDES SOCIALES

1.1 Delitos Informáticos

1.1.1 Antecedentes

Uno de los antecedentes más remotos de los "delitos informáticos", según Sain (2018), surgió con el telégrafo durante el siglo XIX, en la cual interceptaban comunicaciones y transmitían información falsa. Luego, con la aparición del teléfono durante la década de los 60, los diferentes programadores informáticos intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam, mediante el uso gratuito del servicio.

En cuanto a las computadoras, Sain (2018) refiere que una de las principales preocupaciones estaba en el manejo de la información a partir del almacenamiento y procesamiento de datos personales. Las primeras conductas ilícitas con computadoras comenzaron en la década de los 70 de tipo: económico, espionaje informático, la piratería de software, el sabotaje a base de datos digitalizados y la extorsión.

Asimismo, Noriega (2011) afirma que uno de los primeros delitos informáticos se dio como un juego en el año 1959 con: Robert Thomas Morris, Douglas Mcllory y Víctor Vysottsky (programadores de la compañía Bell Computer), mismos que idearon un sistema denominado "Corewar" en la cual consistía en crear un programa que disminuyera la memoria de la computadora hasta lograr la eliminación completa de esta.

Y en 1972 aparecieron los primeros virus que afectaron a los sistemas informáticos, denominados “Creeper” (enredadera), creado por el ingeniero Bob Thomas, que afectaron a las computadoras de IBM; al mismo tiempo que aparecieron los primeros antivirus denominados “Cegadora” (Noriega, 2011).

1.1.2 Definición

Antes de entrar a la definición del delito informático, primeramente debemos definir lo que es el “delito”, según la concepción dogmática del delito de Machicado (2010) afirma que “Esta concepción de delito fue desarrollada por Karl Binding, Ernst von Beling, Max Ernest Mayer, Edmundo Mezger. El delito es la acción u omisión voluntaria típicamente antijurídica y culpable” (p. 6).

De modo semejante, el delito es una acción típica, antijurídica, imputable, culpable, sometida a una acción penal (Wikipedia). Asimismo, el diccionario de Oxford define el delito como una acción que va en contra de lo establecido por la ley y que es castigado con una pena; en ese mismo contexto, la RAE define el delito como la acción u omisión voluntaria o imprudente penado por la ley.

Por otro lado, la “informática” es el “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores” (RAE, 2001). Igualmente la informática “es el área de la ciencia que se encarga de estudiar la administración de métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir información y datos en formato digital” (Wikipedia, 2022); por lo tanto, “la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales” (Wikipedia, 2022).

En ese contexto y dentro de las diversas definiciones que dan los diferentes autores, tomaremos en cuenta las definiciones más precisas y claras en la actualidad, una de ellas es la de Téllez Valdés, citado por Acurio Del Pino (2016):

> Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". (p. 11)

Otra de las definiciones a tomar en cuenta es la de Camacho Loza, citado por Hernández (2009):

> Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas. (p. 231)

Asimismo, tenemos a Marcelo Huerta y Claudio Líbano, citado por Acurio Del Pino (2016) afirmando lo siguiente:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana

> técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro. (p. 14)

Y por último, como escribe el profesor Chinchilla Sandi, citado por Espinoza (2019) quien define el delito informático como una "Acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas -hardware- o de los programas –software" (p. 10).

En síntesis, el delito es la acción que va en contra de lo establecido por la ley y es castigado con una pena; y la informática es el procesamiento automático de información mediante dispositivos electrónicos. Bajo esa tesitura, los delitos informáticos son aquellos que se cometen, con la utilización de tecnología y medios electrónicos.

1.1.3 Características

Para el tratadista Julio Téllez Valdés los delitos informáticos tienen las siguientes características (Téllez, 2008, p. 188):

1. Son conductas criminales de cuello blanco (*white collar crimes*) en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.

3. Son acciones de oportunidad porque se aprovecha una ocasión creada altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
10. Ofrecen a los menores de edad facilidades para su comisión.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.

De manera muy similar, el Magistrado Jorge Jiménez Martin en su conferencia sobre delitos informáticos realizado el 16 de septiembre del 2015 en Colombia, afirma lo siguiente (Jiménez, 2015, pp 14-15):

1. Son delitos DIFICILES DE PROBAR ya que, en muchos casos, es complicado encontrar las pruebas. Se conoce la acción criminal pero no a su autor.
2. Son actos que pueden llevarse a cabo de forma RÁPIDA Y SENCILLA. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando

sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

3. Los delitos informáticos tienden a PROLIFERAR Y EVOLUCIONAR, lo que complica aún más la identificación y persecución de los mismos.
4. A distancia: problemas de territorialidad.
5. Comisión instantánea.
6. Delitos en masa.
7. Autores expertos usuarios, jóvenes y menores de edad.
8. Bien jurídico complejo.

Y por último, según PERPLEXITY (2023) los delitos informáticos son acciones ilegales que se realizan en el espacio digital, con el fin de vulnerar o dañar los bienes, patrimonios o no, de terceras personas o entidades; algunos de los delitos más comunes son:

1. Suplantación de identidad
2. Espionaje informático
3. Acceso ilícito a redes informáticos
4. Estafa para obtener datos personales
5. Delitos sexuales (integridad sexual)
6. Delitos contra la libertad de las personas
7. Delitos contra la propiedad
8. Delitos contra la seguridad publica
9. Delitos contra la administración publica
10. Delitos económicos

11. Robar propiedad intelectual

12. delitos en el comercio electrónico

Por consiguiente, los delitos informáticos son actos ilegales que se realizan en el entorno digital (internet), con el fin de dañar o perjudicar a las personas (Perplexity.ai, 2023); asimismo, se caracterizan por las múltiples dificultades en ser revelados, probarlos y perseguirlos; además que resulta difícil poder tipificarlos penalmente por la constante evolución tecnológica de la información y la comunicación; y actualmente con la Inteligencia Artificial en su pleno apogeo (Castillo y Espinoza, 2015).

1.1.4 Elementos

Los elementos de los delitos informáticos en derecho penal son dos: sujeto activo y sujeto pasivo; el sujeto activo es aquel que realiza la conducta que se considera prohibida (sea de acción o de omisión) mientras que el sujeto pasivo es aquella persona que ha sido afectado o puesto en peligro.

Sujeto Activo. El sujeto activo del delito, lo constituye la persona física que con su conducta produce el resultado lesivo para el pasivo, lesionando o poniendo en peligro el bien jurídicamente tutelado por el Estado.

Antiguamente se consideraba que los delincuentes informáticos poseían ciertos conocimientos en sistemas informáticos, o con cierto status socioeconómico, catalogados como “delincuentes de cuello blanco”. En la actualidad, algunos autores consideran que los delitos cometidos por los hackers podrían ser considerados como sujetos altamente calificados (Acurio, 2016).

Actualmente, la computadora al ser parte indispensable del ser humano, cuenta con sistemas y programas que facilitan su uso para cualquier persona, incluso para aquellas personas que no cuentan con un mínimo de conocimiento en computación. En ese contexto, los delitos informáticos pueden ser cometidos por personas que recién se inician en la informática o por niños que están aprendiendo individualmente en sus hogares (Acurio, 2016).

Sujeto Pasivo. (Víctima) Es la persona titular del bien jurídico protegido por el Estado, sobre la cual recae la actividad típica del sujeto activo. En el caso de los delitos informáticos, las victimas pueden ser: personas, instituciones, gobiernos etc., que utilizan sistemas informáticos.

Además, el sujeto pasivo es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Por lo tanto, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

1.2 Redes Sociales

El internet y las redes sociales conforman un nuevo contexto social, caracterizado por el alcance temporal y espacial de las comunicaciones, creando “proximidad virtuales”,

cambiando el modo en que nos relacionamos en sociedad; de ahí que, con sus particularidades y especificidades han surgido conductas hasta ahora inéditas y ha tenido lugar una importante mutación en las relaciones sociales (Pifarré et al., 2013).

1.2.1 Antecedentes

Para algunos autores, el inicio del telégrafo fue el inicio de las comunicaciones a distancia. En 1844 Samuel Morse envió el primer telégrafo desde Washington DC a Baltimore (Val, 2019). El telégrafo es uno de los primeros antecedentes remoto de las redes sociales.

De hecho, las redes sociales tienen su origen con el nacimiento del internet en los Estados Unidos en 1958 cuando se crea ARPA (Advanced Research Projects Agency) de uso exclusivamente militar, para tener acceso a la información militar desde cualquier parte de su territorio.

De ahí que en 1969 se estableció ARPANET (Advanced Research Projects Agency Network), la primera red sin nodos centrales, de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI) (Trigo, 2004).

Posteriormente en 1971 Tomlinson envió el primer correo electrónico, con el objetivo de garantizar el control remoto de las computadoras en diversas partes de los centros bélicos del país norteamericano (Val, 2019).

A todo esto, según Carballar (2011) las primeras redes sociales online se crearon en base a un antiguo sistema informático conocido como BBS (Bolletin Board System o tablón de anuncios). La primera BBS se creó en 1977 y permitía que sus usuarios intercambiaran textos y archivos; posteriormente estos sistemas fueron sustituidos por el uso del internet, apareciendo distintos tipos de comunidades como listas de correo electrónico, grupos de noticias, chat, etc.

Luego, en 1982, ARPA declaró como estándar el protocolo TCP/IP (Transfer Control Procotol/Internet Protocol) y es entonces cuando aparece la primera definición de Internet (conjunto de internets conectadas mediante TCP/IP) (Trigo, 2004).

En la década de los 90 se estandarizaron los protocolos de conexión TCP/IP, y Tim Berners-Lee diseño el primer sistema de comunicación entre un servidor y el cliente, dando inicio de la World Wide Web (WWW); posteriormente, se unificó el lenguaje Web gracias al Hypertext Markup Languaje (HTML) (Zanoni, 2008).

Y en 1997, cuando aparece "SixDegrees.com" (seis grados.com) se genera en realidad el primer sitio de redes sociales, que permite crear perfiles de usuarios y listas de amigos; de hecho, las primeras redes sociales basadas en círculos de amigos en línea aparecieron entre los años 2001 y 2002, como relaciones sociales en las comunidades virtuales; y se popularizaron en el 2003 como espacios de intereses afines (Morduchowicz et al., 2010, p. 3).

Luego, en el año 2004 se acuño el termino Web 2.0 por Tim O'Reilly, haciendo referencia a una segunda generación en el desarrollo de la tecnología Web, dando lugar a

una mayor participación de los usuarios como productores y consumidores de la información (Wikipedia, 2022).

A mayor abundamiento, la Web 1.0 se caracteriza por ser una web en la que el usurario solamente podía leer y buscar contenido; por lo tanto, el usuario era solamente consumidor de contenidos y no podía participar. Por otra parte, la Web 2.0 es un tipo de web abierta y participativa, en donde se pasa de ser simples lectores a creadores de la misma e interactuar con todo el mundo.

1.2.2 Definición

Antes de dar una definición de 'red social', primeramente examinaremos el origen del vocablo; según Barriuso (2009) "el germen teórico-sociológico de las redes sociales fue propuesto inicialmente por Frigyes Karinthy (1929) con la teoría de los 'seis grados de separación'" (p. 302), fundamentando de que cualquier persona puede conectarse vía internet e interactuar con cualquier persona del planeta con tan solo seis enlaces.

Asimismo, para Wikipedia (2022) el término "red social" fue acuñado por el antropólogo John Arundel Barnes en un artículo publicado en 1954, en la cual quería unificar los conceptos tradicionales de las ciencias sociales como ser: grupos sociales (tribus o familias) y categorías sociales de (género o etnia). Desde entonces se fue utilizando la palabra red social sistemáticamente.

Ahora, "una red social es una estructura social formada por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común. El término se

atribuye a los antropólogos británicos Alfred Radcliffe-Brown y John Barnes" (IAB Spain, 2020, p. 12).

De igual manera, para la enciclopedia Wikipedia (2022) "Una red social (en plural, redes sociales, abreviado como RR. SS.) es una estructura social compuesta por un conjunto de actores y uno o más lazos o relaciones definidos entre ellos"; adicionalmente y como escribe Alemañy citando a Wikipedia (2009) una red social "es una estructura social que se puede representar en forma de uno o varios grafos en el cual los nodos representan individuos (a veces denominados actores) y las aristas relaciones entre ellos".

Según Carballar (2011) una red social es un grupo de personas que se comunica online con algún tipo de interés común, como ser: un tema social, coleccionismo, nueva tecnología, una afición, etc. En ese contexto, la red le ofrece la posibilidad de compartir sus conocimientos y experiencias mediante el uso de aplicaciones basadas en el internet.

De igual manera, Rallo y Martínez (2010) manifiestan que las "redes sociales online" (conexión a internet) son:

> Aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción. (p.24)

A mayor abundamiento, para Perplexity.ai (2023) una red social es una estructura o plataformas digitales formadas por personas o comunidades con intereses comunes, con el fin de comunicarse e intercambiar información, y se caracterizan por:

1. Conexión e interacción entre diversas personas de todo el mundo.
2. Funcionan en tiempo real y permiten la difusión de información de manera inmediata.
3. Punto de encuentro para millones de personas de todo el mundo.
4. Cada red social cuenta con su propia configuración, y son ajustables en función de las preferencias de cada persona.
5. Ofrecen cada vez más funcionalidades para que el usuario pueda disponer de prácticamente todos los servicios que ofrecen las redes sociales en una sola plataforma.

Como resultado de lo expuesto, una red social es una estructura social formada por personas u organizaciones que se conectan a través del internet, la misma, comparten intereses o valores comunes, como ser: amistad, parentesco, trabajo, etc. del mismo modo, comparten sus conocimientos y experiencias (intercambio de información).

1.2.3 Tipos de Redes Sociales

Redes Sociales Directas. Son "aquellas cuyos servicios prestados a través de Internet en los que existe una colaboración entre grupos de personas que comparten intereses en común y que, interactuando entre sí en igualdad de condiciones, pueden controlar la información que comparten" (Urueña et al., 2011, p. 13); asimismo, los usuarios gestionan o controlan su información personal y su relación con los otros usuarios.

Redes Sociales Indirectas. Los "servicios prestados a través de Internet cuentan con usuarios que no suelen disponer de un perfil visible para todos, existiendo un

individuo o grupo que controla y dirige la información o las discusiones en torno a un tema concreto" (Urueña et al., 2011, p. 16); asimismo estas se clasifican en foros y blogs.

Redes Sociales Horizontales o Genéricas. Ponce (2012) afirma que "las redes sociales horizontales no tienen una temática definida, están dirigidas a un público genérico, y se centran en los contactos. La motivación de los usuarios al acceder a ellas es la interrelación general, sin un propósito concreto" (p. 11). En efecto, están dirigidas a generar un colectivo genérico de usuarios, sin tener una temática definida.

Redes Sociales Verticales o Específicas. "Es un tipo de red social que se caracteriza por estar especializada en un determinado tema o actividad, y por facilitar la interacción y la comunicación entre usuarios con un interés común" (Wikipedia, 2022). Por lo tanto, las redes sociales verticales están dirigidas a un público específico, y con una temática definida.

1.2.4 Principales Redes Sociales en la Actualidad

Facebook. Es un servicio de redes y medios sociales en línea estadounidense con sede en Menlo Park, California. Su sitio web fue lanzado el 4 de febrero de 2004 por Mark Zuckerberg, junto con otros estudiantes de la Universidad de Harvard. Se puede acceder desde una amplia gama de dispositivos con conexión a Internet, como ser computadoras, laptops, tablets y teléfonos inteligentes. Una vez registrados con sus datos personales y su número de celular, los usuarios pueden crear un perfil personalizado (Wikipedia, 2022).

Facebook es una red social para conectar personas e interactuar con personas de todo el mundo (en especial con amigos y familiares). También se puede compartir información, noticias, imágenes, textos, videos; al igual que enviar y recibir mensajes, hacer contactos, realizar búsquedas, hacer anuncios, unirse a grupos específicos de su interés etc.

En marzo de 2018, Facebook contaba con más de 2,700 millones de usuarios activos mensuales en todo el mundo. En los últimos años, la compañía se ha enfrentado con una intensa presión sobre la cantidad de fake news[1], la incitación al odio y las representaciones de violencia que prevalecen en sus servicios (Wikipedia, 2022).

WhatsApp. Fue fundado el 24 de febrero de 2009 por Jan Koum; y el 19 de febrero de 2014, la aplicación fue adquirida por la empresa Meta (Facebook). WhatsApp es una aplicación de mensajería instantánea para computadoras, laptops, tablets y teléfonos inteligentes, permitiendo enviar y recibir mensajes mediante internet, además de imágenes, videos, audios, grabaciones de audio, documentos, ubicaciones, contactos, gifs, stickers, así como llamadas y video llamadas con varios participantes a la vez. WhatsApp se integra automáticamente a la libreta de contactos, y no es necesario ingresar alguna contraseña para acceder al servicio (Wikipedia, 2022).

WhatsApp permite al usuario crear una red de contactos con los números de teléfono guardados en el dispositivo; por consiguiente, ofrece la posibilidad de crear un perfil propio, conversar con sus contactos, compartir archivos y, sobre todo, crear grupos; incluso, a través de los grupos se puede llegar a tener contacto con usuarios que no

[1] Fake news. Son noticias falsas, con el único objetivo de desinformar.

forman parte de la lista de contactos original del usuario. Y por último, tiene los denominados “estados”, que permiten subir fotos y videos, con los cuales pueden interactuar los contactos de ese usuario (Bastida 2019).

Adicionalmente, según datos del año 2020, WhatsApp es líder en mensajería instantánea en gran parte del mundo, superando los 2,000 millones de usuarios en todo el mundo, superando a otras aplicaciones como Facebook Messenger o Telegram, entre otros (Wikipedia, 2022).

YouTobe. Fue fundado por Chad Hurley, Steve Chen y Jawed Karim en febrero de 2005 en San Bruno, California Estados Unidos, y en octubre de 2006 fue adquirido por Google Inc. YouTobe es una red social que permite alojar y compartir videos que han sido creados por los usuarios. Permite a los usuarios subir una variedad de videos, como ser: películas, programas de televisión y videos musicales, así como video blogs y YouTube Gaming (Wikipedia, 2022).

YouTube permite a los usuarios registrarse y crear un canal, que es una página en que se contiene información del perfil del usuario, los vídeos subidos, las listas de reproducción creadas por el usuario, los vídeos favoritos, etc. que el resto de usuarios registrados pueden ver; también cabe la posibilidad de dejar comentarios de los videos y responder a los mismos, además de votar a favor o en contra de un video con un: “me gusta” o “no me gusta”; y por último, estos videos pueden compartirse a través de otras redes sociales (Bastida, 2019).

Asimismo en agosto de 2018, el sitio web está clasificado como el segundo sitio más popular del planeta tierra, desde mayo del 2019, se suben a YouTube más de 500 horas de contenido de vídeo cada minuto (Wikipedia, 2022).

Twitter. Creado por Jack Dorsey en 2006, y en 2002 fue adquirido por el empresario estadounidense Elon Musk, es una empresa de comunicación estadounidense con sede en San Francisco, California. Su principal producto es la red social de microbloggimg Twitter; la red permite enviar mensajes de texto con un máximo de 280 caracteres (originalmente 140), llamados "tuits"; sus usuarios comparten información y opiniones, dando también la posibilidad de publicar fotos y vídeos (Wikipedia, 2022).

Adicionalmente, la red ha ganado popularidad mundial y se estima que tiene más de 300 millones de usuarios, generando 65 millones de tuits al día y maneja más de 800.000 peticiones de búsqueda diarias. Ha sido denominado como el "SMS de Internet" (Wikipedia, 2022).

TikTok. Es una red social de origen Chino y conocido como Douyin, lanzado por ByteDance en Pekín, China, en septiembre de 2016, originalmente con el nombre A.me, posteriormente se lanzó en 2017 para iOS y Android, y en septiembre de 2017 se lanzó a nivel internacional al fusionarse con otros servicios de redes sociales. TikTok es una App de redes sociales que permite grabar, editar y compartir videos corto y vertical, con una duración de 1 segundo hasta 10 minutos, con la posibilidad de añadir fondos musicales, efectos de sonido y filtros o efectos visuales (Wikipedia, 2022).

En febrero de 2019 TikTok alcanzó mil millones de descargas a nivel mundial, los medios de comunicación citaron a TikTok como la séptima aplicación móvil más

descargada de la década; también fue la aplicación más descargada en la App Store de Apple en 2018 y 2019, superando a Facebook, YouTube e Instagram (Wikipedia, 2022).

Instagram. Es una red social de origen estadounidense, propiedad de Meta. Creada por Kevin Systrom y Mike Krieger, lanzado al mercado el 6 de octubre de 2010, y no fue hasta abril de 2012 cuando salió la aplicación final para Android, tanto fue su éxito que el 9 de abril de 2012, fue adquirido por la empresa de Facebook. En el año 2016, Instagram estrenaría su aplicación para Windows 10, aunque sin posibilidad para subir fotos (Wikipedia, 2022).

Instagram es una red social muy popularizada entre jóvenes que ofrece la posibilidad de compartir fotografías con otros usuarios y poder recibir comentarios o "me gustas" (likes) de tus seguidores; además, es una red social que permite a sus usuarios subir imágenes y vídeos con múltiples efectos fotográficos como filtros, marcos, colores retro, etc., para posteriormente compartir esas imágenes en la misma plataforma o en otras redes sociales (GEEKNETIC, 2020).

Telegram. Es una plataforma de mensajería instantánea de origen ruso, desarrollada por los hermanos Nikolái y Pável Dúrov, lanzado el año 2013, disponible para su instalación en Windows, MacOS, Linux y los sistemas operativos de Smartphone como Android e iOS (es una aplicación disponible para prácticamente todos los dispositivos de hoy) (Wikipedia, 2022).

Con Telegram puedes enviar mensajes, fotos, videos y archivos de cualquier tipo (Doc, Zip, Mp3, etc.), como también crear grupos de hasta 200.000 personas o canales para hacer difusiones a audiencias ilimitadas; también brinda llamadas de voz y video

llamadas, así como chats de voz en grupos que permiten miles de participantes; asimismo, se puede encontrar a una persona con solo su nombre de usuario (Telegram, 2022).

Linkedln. Es una plataforma para encontrar empleo o compartir tu desarrollo y crecimiento profesional; fundada en diciembre de 2002 por Reid Hoffman, Allen Blue, Konstantin Guericke, Eric Ly y Jean-Luc Vaillant, fue lanzada en mayo de 2003; y en junio del 2016 fue adquirida por la empresa Microsoft. Linkedln es una red social orientada al uso empresarial, a los negocios y al empleo; partiendo del perfil de cada usuario, quien libremente revela su experiencia laboral además de sus destrezas, la web pone en contacto a millones de empresas y empleados en todo el mundo (Wikipedia, 2022).

CAPÍTULO II

LOS DELITOS INFORMÁTICOS MÁS FRECUENTES EN LAS REDES SOCIALES DE BOLIVIA, Y SU REGULACIÓN JURISDICCIONAL PENAL

El 10 de marzo de 1997 se lleva a cabo la tercera reforma del Código Penal Boliviano Ley Nº 1768 denominado "Reforma Blattman" en la cual se incorpora el capítulo XI "Delitos Informáticos" con los siguientes artículos: Art. 363 bis.- Manipulación informática y Art. 363 ter.- Alteración, acceso y uso indebido de datos informáticos.

Después de la reforma Blattman de 1997, aparecieron las primeras redes sociales entre los años 2001 y 2002, popularizándose en el año 2003 (Morduchowicz et al, 2010), dando lugar a la aparición de nuevos tipos de delitos informáticos en redes sociales a nivel mundial. Bajo este contexto la legislación boliviana deja un enorme vacío jurídico en relación a los delitos informáticos en redes sociales.

Frente al surgimiento de estas nuevas figuras delictivas en redes sociales, el diputado del Movimiento al Socialismo (MAS) Juan José Huanca presento el "Proyecto de Ley (Nº 304-2023) que regula y sanciona el uso indebido de las redes sociales en todo el territorio del Estado Plurinacional de Bolivia".

El proyecto de ley 304 que regula y sanciona el uso indebido de las redes sociales como Facebook, WhatsApp, YouTobe Instagram, Twitter, etc. estableciendo una pena de 5 a 7 años de cárcel por el uso inadecuado de las redes sociales; pero, por la presión social de diferentes organizaciones sociales se dejó sin efecto dicha ley.

Como resultado de un vacío jurídico de los delitos informáticos en redes sociales, algunos autores mencionar que estos delitos cuando se cometen, casi siempre van de la mano de otros delitos antiguos ya tipificados en el Código Penal, calificándolos como "viejos delitos envasados en nuevas botellas"; asimismo, en algunos casos solo se aplican por analogía algunas figura penales establecidos en el Código Penal Boliviano.

2.1 Antecedentes

En la década de los 80 en Bolivia no existían redes de transmisión, ni canales de salida vía satélite; el avance de la tecnología desembocó en el uso del teléfono para la transmisión de datos. En 1989 el Programa de las Naciones Unidas para el Desarrollo (PNUD) se propuso establecer redes de comunicación en Bolivia, con el fin de mejorar el intercambio de información entre las instituciones del Estado y las instituciones de desarrollo en Latinoamérica (Eabolivia.com).

De manera que se constituyó en un proyecto experimental denominado BOLNET, bajo el programa regional RLA/031/88 de la Oficina Regional para América Latina y el Caribe del Programa de Naciones Unidas para el Desarrollo; posteriormente se conforma el comité impulsor conformado por: el departamento de red troncal digital de ENTEL; el Instituto de capacitación ENTEL (ICAPTEL); la carrera de ingeniería electrónica de la UMSA; el Instituto de Desarrollo Andino Tropical IDAT y Servicios múltiples de tecnologías apropiadas SEMTA (Eabolivia.com).

En agosto de 1990 se realizó la conexión a los usuarios de SEMTA, del Programa de Naciones Unidas para el Desarrollo - PNUD y de la Carrera de Ingeniería Electrónica de la UMSA Se instaló los módems y se accedió a la primera línea telefónica a través de

COTEL e ICAPTEL. En septiembre de 1990 con la participación de Steve Framme, Vincenzo Puliatti y los representantes del Comité se definió el nombre para el proyecto boliviano denominado BOLNET, se envió los primeros correos electrónicos en Bolivia, el primer correo perteneció al consultor extranjero Steve Frank (steve@unbol.bo). Asimismo, en octubre de 1990 se realizó el cambio de menús del idioma inglés al idioma español, mediante manejo de programación software UNIX (Eabolivia.com).

El 16 de julio de 1993 BOLNET ya tiene conexión a internet, logrando conectarse con 91 países, constituyendo una red que conecta a 200 computadoras las 24 horas del día. La red física se instaló en la facultad de ingeniería de la UMSA, asimismo, la UMSA es responsable de la red física y lógica de BOLNET; y para 1994, BOLNET se convirtió en la única red que prestaba servicios a más de 1,000 usuarios. Y en 1995 se instaló nodos de BOLNET en Santa Cruz (Universidad Gabriel René Moreno), Cochabamba (Universidad Mayor de San Simón) y Sucre (Universidad Andina Simón Bolívar) (Eabolivia.com).

En 1996, el NIC BOLIVIA inicia sus servicios para el registro territorial ".bo", la primera página web en Bolivia fue: http://www.BOLNET.bo/ que prestó los servicios de información académica e institucional; asimismo, se dio inicio a la World Wide Web (www) como canal de comunicación dentro del ámbito de investigación y enfocado a las personas (Eabolivia.com).

En 1997 se diseñó e instaló los Nodos de ENTEL: La Paz (UMSA), Cochabamba (UMSS), Santa Cruz, (UGRM) Chuquisaca (UASB) y Tarija (UJMS). Se realizó la transferencia de usuarios de los nodos de BOLNET a Entel. Se diseñó la red ENTELNET

bajo la supervisión de BOLNET. Asimismo, en 1997 se instaló los primeros Nodos gubernamentales para la conexión a Internet; también se diseñó la primera biblioteca virtual de Bolivia para la Universidad Andina Simón Bolívar con sede en Sucre (Eabolivia.com).

En 1998 se diseñó el sitio web "www.nic.bo" para la administración de dominios ".bo". Y entre los años de 1999 y el 2002 se diseñan los primeros sistemas de Información gubernamental en Bolivia (portales web); posteriormente se implementó un nuevo nodo para La Paz, para la prestación de servicios de acceso a usuarios "Dial Up y OnLine"; Además, se aplicó el servicio de "web hosting". Y por último, se reestructuró el Sistema "OnLine" para la Administración de Dominios Internet y se realizó los sistemas de administración para clientes de Dial Up y correo electrónico (Eabolivia.com).

Entre el 2002 y el 2004 la Red más alta del mundo es la primera Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB. Bolivia participa de la Cumbre Mundial de la Sociedad de la Información realizada en Ginebra el 2003. Se realizó proyectos estratégicos como: la Estrategia de Tecnologías de Información y Comunicación – ETIC (Eabolivia.com).

2.2 Los Delitos Informáticos Más Frecuentes en las Redes Sociales de Bolivia

Según el Observatorio de Delitos Informáticos Bolivia (ODIB), citado por García de la prensa de Pagina Siete, los delitos informáticos en redes sociales siguen siendo los mismos que antes, como ser: "Amenazas, difamación, coacción", "Fraude o Estafa Informática" y "Grooming" (acoso sexual a menores de edad) siendo los tres tipos de delitos con mayor concurrencia en Bolivia (Comunidad Derechos Humanos, 2020).

Un reportaje del periódico de circulación nacional La Razón de 7 de mayo de 2012 titulado: Los ciberacosadores ya operan en Bolivia; La Policía, la Fiscalía y una empresa investigadora revelan casos en los que se usa las redes sociales para "hostigar, agredir, amenazar y extorsionar"; todo comienza con una amistad por las redes sociales, posteriormente llegan a amenazas de muerte, robo y extorción. (Flores et al., 2014).

En el informe emitido por el Estado Boliviano a la ONU en su septuagésimo cuarto período de sesiones tema 109 del programa provisional sobre "lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos" (2019), establece los siguientes delitos informáticos en las redes sociales de Bolivia:

1. Acoso, injurias, calumnias, hostigamiento y exclusión social a través de las redes sociales.
2. Estafas y fraudes, entre ellos el phishing[2]. En la cual, los delincuentes se apropian de información confidencial para acceder a sus cuentas bancarias. Por otro lado, tenemos el, reclutamiento de gente para empleos, que actuaban como tapadera de redes involucradas en la trata de personas y la pornografía infantil.
3. Correos basura. uso indebido de bases de datos con fines comerciales, incluyendo campañas de prostitución.
4. Pornografía infantil, que se comercializan en forma de fotos y videos por las redes.
5. Propiedad intelectual. Vulneración de los derechos de autor en múltiples formas.

[2] El phishing es un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal en sitios web que fingen ser sitios legítimos.

6. Ventas en Internet, como supuestos intermediarios de loterías y concursos.

Para Antezana del diario Opinión (2021) identifica 12 delitos informáticos que se dan en redes sociales en contra de las mujeres, como ser: el ciberacoso o ciberbullying, (que es el uso de diferentes medios para molestar o perseguir a una persona); el grooming (o engaño pederasta); phishing (que es una técnica de engaño para robar información confidencial); sextorsión (que se conoce como una forma de explotación sexual a través de la presión y chantaje); craking (también conocido como hacking, que es el acceso a información sin permiso); asimismo, se suman los delitos de violencia mediática y en línea; la pornografía infantil; la captación para trata, tráfico y delitos conexos; la adicción a internet; la suplantación de identidad digital; y la difusión no consentida de contenido sexual. Y por último, tenemos el "lolicon/shotacon" (conocido en Japón como el "complejo de Lolita", y se describe como una atracción por las niñas menores de edad); asimismo, tenemos el "complejo de shotaro" (haciendo referencia a un personaje del anime, se refiere a la atracción hacia niños, a quienes los presentan de forma erotizada).

Y, según la abogada Karina Medinaceli menciona como delitos nuevos en las redes sociales de Bolivia: el grooming (cuando un adulto se acerca a los menores de edad para ganarse su confianza y luego involucrarlos en actividades sexuales), sexting (envío de mensajes, fotos o videos de contenido sexual) o ransomware (secuestro de archivos para pedir rescate por ellos) (Guardiana, 2021).

Asimismo, los delitos informáticos más comunes en redes sociales en el departamento de Cochabamba son: delincuencia económica y extorsión (compra-venta de objetos y de bienes que nunca son entregados o no tienen la calidad o cantidad ofrecida);

captar personas para proxenetismo, trata y tráfico de personas y extorsión; y la afectación al honor y dignidad de una persona (Red Uno, 2022).

Por lo tanto, podemos advertir que los delitos informáticos más frecuentes que se dan en Bolivia son: trata y tráfico de personas, pornografía infantil, violencia mediática en línea, suplantación de identidad digital, delincuencia económica y extorción, afectación al honor y dignidad de una persona, amenazas, difamación, coacción, fraude o estafa informática, vulneración de derechos de autor, Grooming, phishing, sexting, sextorsion, ciberacoso o ciberbullyng, craking o hacking; y últimamente, el Lolicon/shotacon y Shotaro.

2.3 Legislación Nacional

2.3.1 Constitución Política del Estado Boliviano

La Constitución Política del Estado Boliviano (2009) "es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa" (Art. 410 pàrr. II); por lo que, el texto constitucional se encuentra en la cumbre del ordenamiento jurídico boliviano, constituyéndose en el sustento o fundamento de los demás preceptos legales.

Bajo esa tesitura, la Constitución Política del Estado Boliviano establece en su artículo 106, parágrafo I y II lo siguiente:

> **I**. El Estado garantiza el derecho a la comunicación y el derecho a la información.
> **II.** El Estado garantiza a las bolivianas y los bolivianos el derecho a la libertad de expresión, de opinión y de información, a la rectificación y a la réplica, y el

derecho a emitir libremente las ideas por cualquier medio de difusión, sin censura previa.

Asimismo, en su artículo 21 numeral 2 de la CPE, las bolivianas y los bolivianos tienen el derecho "a la privacidad, intimidad, honra, honor, propia imagen y dignidad"; de igual modo, en su artículo 130 parágrafo I de la CPE, nos indica que:

> Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

Por lo tanto, la Constitución Política del Estado Boliviano, como norma suprema, garantiza el derecho a la comunicación, información y la libertad de expresión por cualquier medio de difusión; también, garantiza la privacidad, intimidad, honra, honor, propia imagen y dignidad.

2.3.2 Código Penal Boliviano

En cuanto al Código Penal Boliviano, en su Libro Segundo, Parte Especial, Título XII – Delitos contra la Propiedad, Capítulo XI – DELITOS INFORMÁTICOS, establece lo siguiente:

> **Artículo 363 bis. -** (MANIPULACIÓN INFORMÁTICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento

o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Artículo 363 ter. - (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.

Por ende, según los Art. 363 bis.- y Art. 363 ter.- del Código Penal Boliviano, podemos inferir que la manipulación de datos informáticos y el acceso sin autorización a los datos informáticos, hacen referencia únicamente a las computadoras; además, son los dos únicos artículos que hacen referencia a los delitos informáticos.

2.3.3 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación

La ley general de telecomunicaciones, tecnologías de información y comunicación (Ley Nº 164 de 8 de agosto de 2011), tiene como objeto "establecer el régimen general de telecomunicaciones y tecnologías de información y comunicación" (Art. 1); asimismo, "establece el acceso universal a las telecomunicaciones y tecnologías de información y

comunicación" (Art. 5, núm. 1); además, en su parágrafo II del artículo 8 de la Ley Nº 164 establece lo siguiente:

> La administración, asignación, autorización, control, fiscalización y supervisión del uso de las frecuencias electromagnéticas en redes de telecomunicaciones, radiodifusión y otras en el territorio nacional corresponde al nivel central del Estado a través de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, de acuerdo al Plan Nacional de Frecuencias.

Y por último, el artículo 1 del DS 1391 de 24/10/2012 aprueba el reglamento general de la ley y dispone que "todos los aspectos complementarios que se requieran para la aplicación de la ley Nº 164 y del Reglamento General para el Sector de Telecomunicaciones serán establecidos mediante Resolución Ministerial por el Ministerio de Obras Públicas, Servicios y Vivienda".

Por lo tanto, esta ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, con el fin de garantizar el derecho humano de las personas a la comunicación; de igual manera, tiene como objeto la regulación del comercio electrónico, correo electrónico, firma digital, etc.

2.4 Regulación Jurisdiccional Penal en Bolivia

2.4.1 Órgano Judicial

En la Tabla 1 se puede ver las cifras de los delitos informáticos en los asientos judiciales de los nueve departamentos, incluyendo la jurisdicción de El Alto; información provista por las autoridades judiciales, y recabado por el investigador Fabián Espinoza

Valencia entre el primer trimestre de la gestión 2014 hasta el último trimestre de año 2017.

Tabla 1

Cifras de los Delitos Informáticos en el Órgano judicial

	Delitos con vinculación a internet	Delitos Informáticos
Beni	2	2
Cochabamba	299	4
El Alto	5	-
La Paz	93	42
Oruro	3	4
Potosí	5	1
Santa Cruz		
Sucre	25	1
Tarija	4	-
Pando	5	3

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 19), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

*El órgano judicial de Santa Cruz no provee información.

En la Tabla 1 se puede apreciar que los “delitos vinculados al internet” tiene una enorme proporción en el departamento de Cochabamba con 299 casos; asimismo, se evidencia un alto grado de violencia contra las mujeres vinculado directamente con el internet, principalmente en el área rural (Espinoza, 2019).

Por otro lado, el departamento de La Paz cuenta con 93 casos sobre “delitos vinculados al internet” (Tabla 1); asimismo, se evidenciando que una gran cantidad de dichos delitos, está vinculado directamente con el artículo 363 bis (manipulación informática) del código penal; además, el departamento de La Paz cuenta con el mayor índice en cuanto a “delitos informáticos” con un total de 42 casos registrados (Espinoza, 2019).

Y por último, en el departamento de Pando se evidencia una sentencia según el art. 363 bis (manipulación informática) del Código Penal (Espinoza, 2019). A mayor abundamiento, en el departamento de Oruro se observa varios procesos judiciales contra los funcionarios de Derechos Reales por la manipulación de seguridad a nivel técnico como logístico (Espinoza, 2019).

2.4.2 Órgano Ejecutivo

Ministerio Público. En la Tabla 2 podemos observar los datos estadísticos de los delitos de acción penal de competencia del Ministerio Público (y no así de los delitos de acción privada), proporcionados por las Fiscalías Departamentales y Jefaturas de Informática, elaborados entre los periodos desde enero de 2013 hasta enero de 2017 por el investigador Fabián Espinoza Valencia (2019).

Tabla 2

Cifras de los Delitos Informáticos en el Órgano Ejecutivo

TOTAL CASOS	
GESTIÓN	**CASOS**
2013	883
2014	1,455
2015	3,166
2016	1,045
2017	1,254
TOTAL	**7,803**

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 35), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

Según los datos del ministerio público, en el año 2015 se registraron 3,166 casos sobre delitos informáticos en el Órgano Ejecutivo (Tabla 2), siendo el año con mayor cantidad de casos. Por otro lado, tenemos datos complementarios que hacen referencia a la prosecución de la ciberdelincuencia:

Tabla 3

Descubrimiento de Organizaciones Criminales

Número de casos	Delito	Gestión
0	0	0

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 35), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

Como se puede observar en la Tabla 3, no se registran ningún caso sobre el descubrimiento de organizaciones criminales por parte del Ministerio Público.

Tabla 4

Ataques Cibernéticos a Plataformas Digitales Estatales

Número de casos	Delito	Gestión
0	0	0

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 36), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

De igual forma, el ministerio público no registra ningún caso sobre ataques cibernéticos a plataformas digitales del Estado boliviano, tal como se puede observar en la Tabla 4.

Tabla 5

Actividad del Cibercrimen en Redes Sociales

GESTIÓN	CASOS
2013	1
2014	3
2015	19
2016	8
2017	13
TOTAL	**44**

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 36), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

En cuanto a los delitos informáticos en las redes sociales, según la investigación realizada por el Dr. Espinoza Valencia entre el primer trimestre de la gestión 2014 hasta el último trimestre de año 2017, la Tabla 5 muestra que en la gestión 2015 se registró la mayor cantidad de casos registrados (19 casos), seguida por la gestión 2017 (13 casos).

Tabla 6

Resolución de casos con medios probatorios digitales

GESTIÓN	CASOS
2013	0
2014	3
2015	12
2016	5
2017	7
TOTAL	**27**

Nota. Adaptado de "*Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*" (p. 36), por Espinoza Valencia, F. 2019. https://www.fundacionconstruir.org/wp-content/uploads/2021/02/Boleti%CC%81n-Ciberdelincuencia.pdf

Y por último, en la Tabla 6 podemos observar que las resoluciones de casos con medios probatorios digitales por parte del Ministerio Público se dan con mayor incidencia en la gestión 2015 con 12 casos, seguido por la gestión 2017 con 7 casos.

Ministerio de Relaciones Exteriores. Comenzaremos por hacer una breve descripción del "Convenio de Budapest"; el Convenio de Budapest es el primer tratado internacional que busca hacer frente a los "Delitos Informáticos" mediante la armonización de leyes entre Estados (Wikipedia, 2022); el convenio se suscribió en su Sesión Nº 109 del 08 de noviembre de 2001, presentada para su firma en Budapest,

Hungría el 23 de noviembre de 2001, la misma, entro en vigor el 1 de julio de 2004 (Espinoza, 2019).

Por cuanto, Bolivia no forma parte del Convenio de Budapest; asimismo, Bolivia no participo en la negociación de dicho Convenio, ni siquiera está en proceso de adhesión (Espinoza, 2019).

Ministerio de Obras Públicas, Servicios y Vivienda. Según la estructura organizacional del Órgano Ejecutivo del Estado Plurinacional de Bolivia, es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), dependiente del Ministerio de Obras Públicas, Servicios y Vivienda, es la encargada de gestionar solicitudes concernientes al acceso a la información en plataformas digitales de telecomunicaciones.

En ese contexto, para solicitar un informe con valor probatorio a corporaciones del ámbito informático con sede en el exterior, la ATT no cuenta con un procedimiento y/o protocolo para solicitar información; además que no se menciona en ninguna norma como potestad de la ATT para realizar requerimiento de manera oficial; de hecho, no existe ninguna instancia Estatal habilitada para realizar requerimientos oficiales de datos personales a corporaciones del ámbito digital con sede en el extranjero (Espinoza, 2019).

CAPÍTULO III

MARCO PRÁCTICO

LOS DELITOS INFORMÁTICOS MÁS FRECUENTES EN LAS REDES SOCIALES EN EL MUNICIPIO DE LA PAZ

3.1 Análisis e Interpretación de los Resultados de las Encuestas

El presente trabajo de encuesta, se circunscribe al tema denominado "delitos informáticos que se dan con mayor frecuencia en las redes sociales en la ciudadanía del municipio de La Paz durante los últimos diez años (2012-2021); y su regulación jurisdiccional penal"; en este contexto, se realizaron 201 encuestas a los jóvenes del municipio de La Paz desde el 24 de febrero al 4 de marzo del 2023; asimismo, la muestra tiene un nivel de confianza del ± 97% y un error del ± 3%.

Como primera parte de la encuesta tenemos los datos de "edad y sexo" de los encuestados; en la Tabla 7 y la Figura 1 podemos observar que el 97% de los encuestados son jóvenes entre los 18 a 30 años; a mayor abundamiento, los adolescentes son los que más cerca están con las nuevas tecnologías y las TIC.

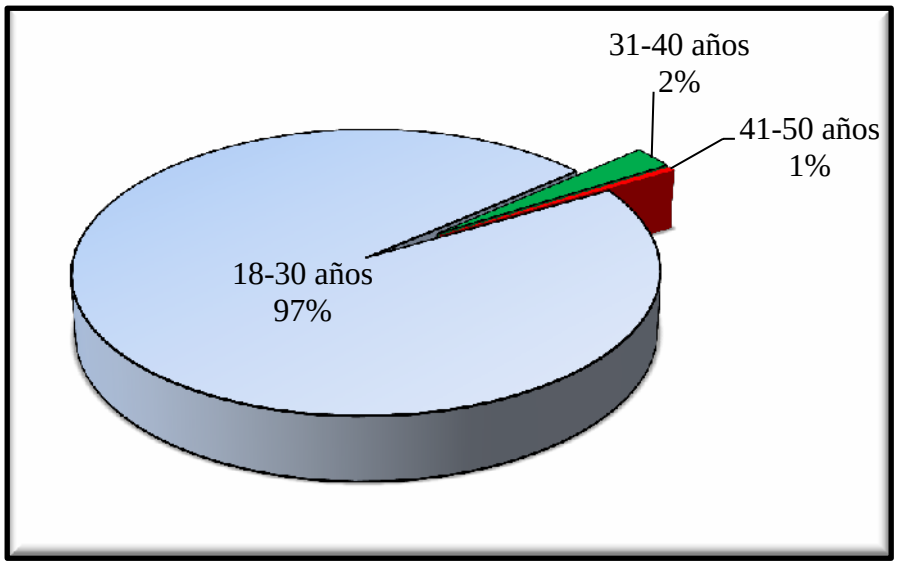
Tabla 7

¿Edad de los encuestados?

Categoría	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
18-30	195	**97,0**	97,0	97,0
31-40	5	**2,5**	2,5	99,5
41-50	1	**,5**	,5	100,0
Total	201	100,0	100,0	

Figura 1

¿Edad de los encuestados?



En la Tabla 8 y la Figura 2 podemos observar el "sexo" de los encuestados; en la Figura 2 podemos observar claramente que el 57% de los encuestados son mujeres, y el 33% son varones; adicionalmente un 10% no contesto, haciendo proveer que el 10% de los encuestados se considera de otro género que no estuvo contemplado en la encuesta.

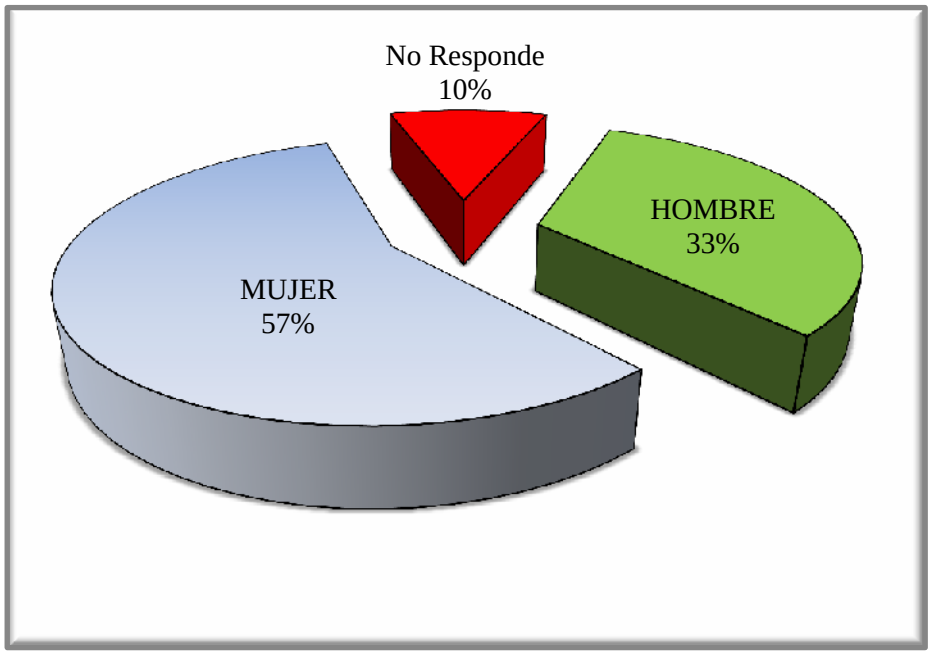
Tabla 8

¿Sexo de los encuestados?

Categoría	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
HOMBRE	66	**32,8**	36,7	36,7
MUJER	114	**56,7**	63,3	100,0
Total	180	89,6	100,0	
No responde	21	**10,4**		
Total	201	100,0		

Figura 2

¿Sexo de los encuestados?



En esta segunda parte de la encuesta, tenemos las siguientes preguntas para los encuestados:

Primera pregunta ¿Usted utiliza alguna red social en su vida cotidiana?, en la Tabla 9 y Figura 3 se puede observar claramente que el 100% de los encuestados respondió que si utiliza las redes sociales en su vida diaria.

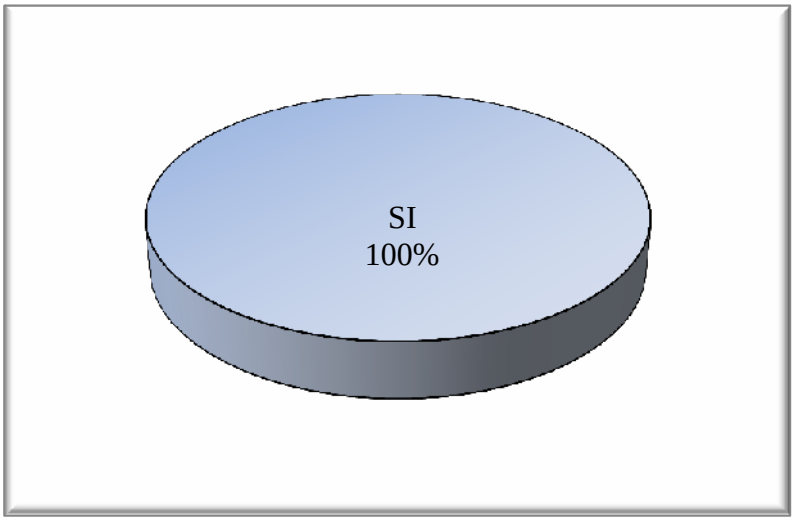
Tabla 9

¿Usted utiliza alguna red social en su vida cotidiana?

Categoría	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
SI	201	100,0	100,0	100,0

Figura 3

¿Usted utiliza alguna red social en su vida cotidiana?



Segunda pregunta ¿Cuál de las siguientes redes sociales es el que más utiliza?, en la Tabla 10 y Figura 4 se observar que los encuestados respondieron de la siguiente manera: 22% WhatsApp, 18% Facebook, 17% YouTobe, 16% TikTok, 11% Instagram,

9% Telegram, 1% Linkedln, y el 2% utiliza otras redes sociales más recientes. Por lo tanto, podemos concluir que los jóvenes del municipio de La Paz utilizan en su mayoría el WhatsApp, Facebook, YouTobe y TikTok como las redes sociales más populares.

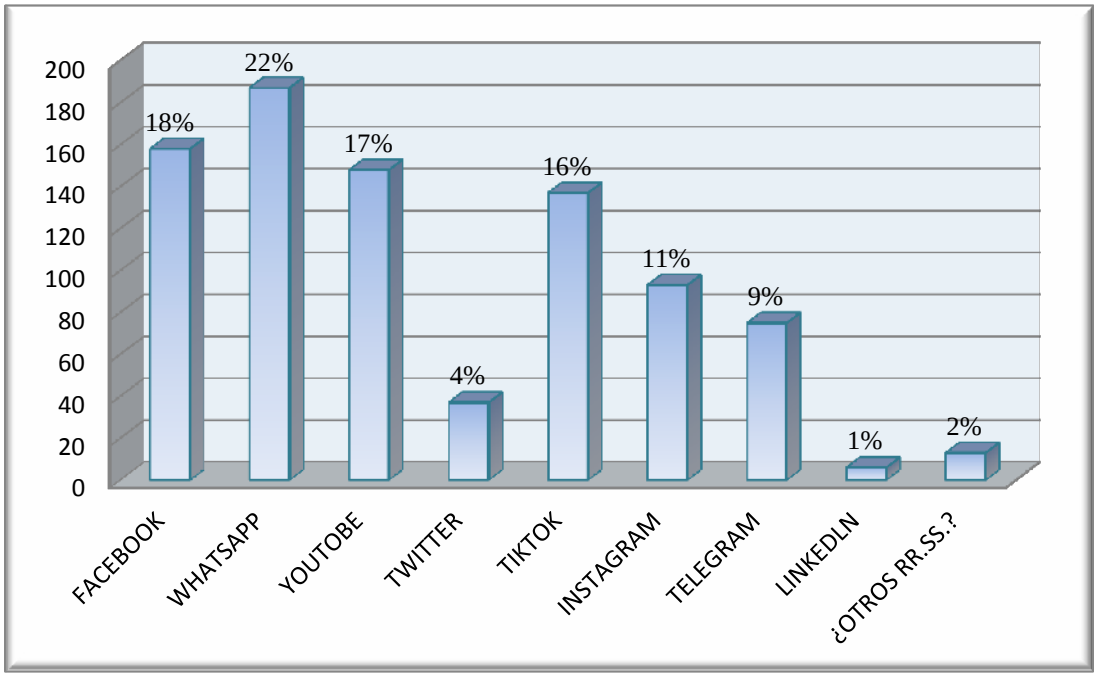
Tabla 10

¿Cuál de las siguientes redes sociales es el que más utiliza?

Categoría	Frecuencia	Porcentaje	Porcentaje de casos
Facebook	158	**18,5%**	78,6%
WhatsApp	187	**21,9%**	93,0%
YouTobe	148	**17,3%**	73,6%
Twitter	37	**4,3%**	18,4%
TikTok	137	**16,3%**	68,2%
Instagram	93	**10,9%**	46,3%
Telegram	75	**8,8%**	37,3%
Linkedln	6	**,7%**	3,0%
Otros	13	**1,5%**	6,5%
Total	854	100,0%	424,9%

Figura 4

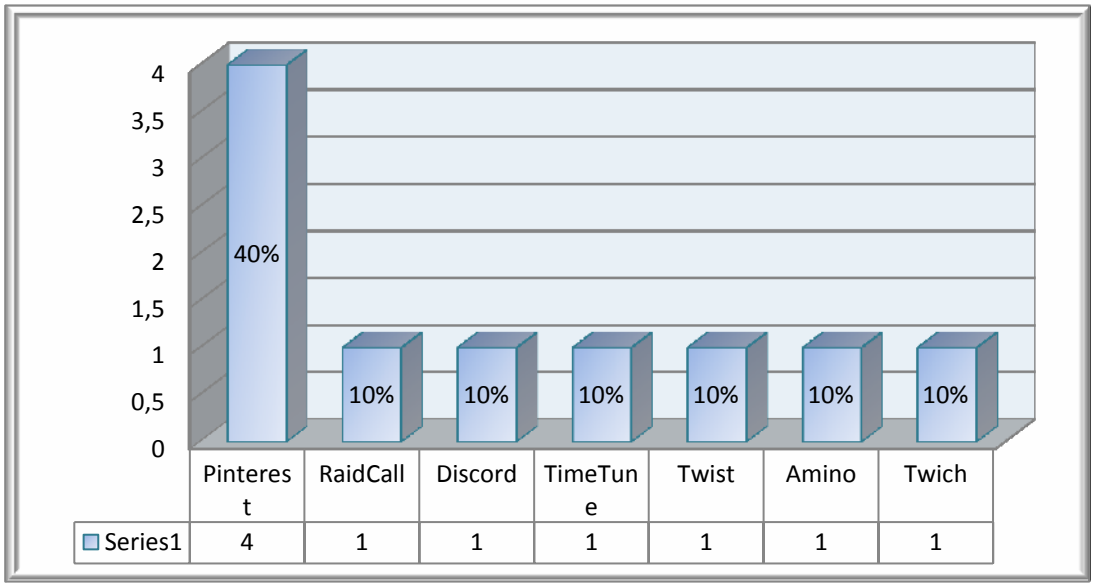
¿Cuál de las siguientes redes sociales es el que más utiliza?



En la Figura 4 se puede observar que el 2% de los encuestados respondió que utiliza “otras redes sociales” en su vida cotidiana; por la cual, en la Figura 5 podemos observar las otras redes sociales que utilizan los jóvenes: 40% Pinterest, 10% RaidCall, 10% Discord, 10% TimeTune, 10%Twist, 10% Amino, 10% Twich. Por lo tanto podemos inducir que las nuevas redes sociales que los jóvenes están empezando a utilizar son: RaidCall (sobre todo), seguido de: Discord, TimeTune, Twist, Amino y Twich como las nuevas redes sociales en crecimiento.

Figura 5

¿Otras redes sociales que utilizan?



Tercera pregunta, ¿Usted tiene conocimiento de alguno de los siguientes delitos informáticos en redes sociales en los últimos diez años?, en la Tabla 11 y Figura 6 los encuestados respondieron de la siguiente manera: estafa y fraude 15%, acoso cibernético 14%, suplantación de identidad 11,5%, trata y tráfico de personas 10,8%, sexting 9,8%, difamación, calumnia y amenazas 9,5%, pornografía infantil 8,4%, phishing 7,5%, grooming 7,0% y violación a la propiedad intelectual 5,3%. Por lo tanto, los tres delitos más comunes en redes sociales son: en primer lugar estafa y fraude, seguida de acoso cibernético y por último suplantación de identidad.

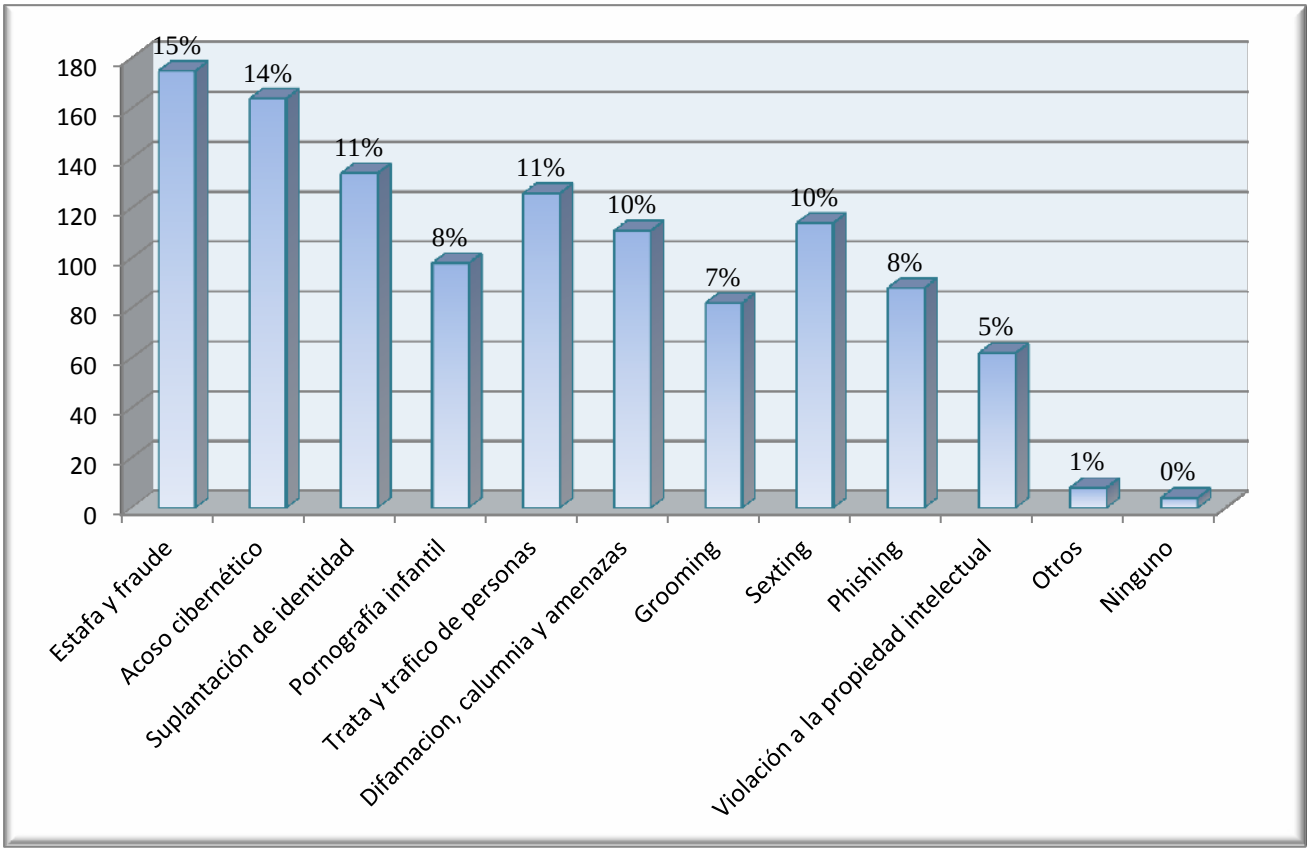
Tabla 11

¿Usted tiene conocimiento de alguno de los siguientes delitos informáticos en redes sociales en los últimos diez años?

Categoría	Frecuencia	Porcentaje	Porcentaje de casos
Estafa y Fraude	175	**15,0%**	87,1%
Acoso Cibernético	164	**14,1%**	81,6%
Suplantación de Identidad	134	**11,5%**	66,7%
Pornografía Infantil	98	**8,4%**	48,8%
Trata y Tráfico de Personas	126	**10,8%**	62,7%
Difamación, Calumnia y Amenazas	111	**9,5%**	55,2%
Grooming	82	**7,0%**	40,8%
Sexting	114	**9,8%**	56,7%
Phishing	88	**7,5%**	43,8%
Violación a la Propiedad Intelectual	62	**5,3%**	30,8%
Otros	8	**,7%**	4,0%
Ninguno	4	**,3%**	2,0%
Total	1166	100,0%	580,1%

Figura 6

¿Usted tiene conocimiento de alguno de los siguientes delitos informáticos en redes sociales en los últimos diez años?



Y por último, en la cuarta pregunta ¿Usted tiene conocimiento de algún delito informático en redes sociales llevado a cabo por la vía judicial?, en la Tabla 12 y figura 7 se observa que el 72 % de los encuestados respondió que no tiene conocimiento de delitos informáticos en redes sociales llevado a cobo por la vía judicial, y un 20% responde que si tiene conocimiento.

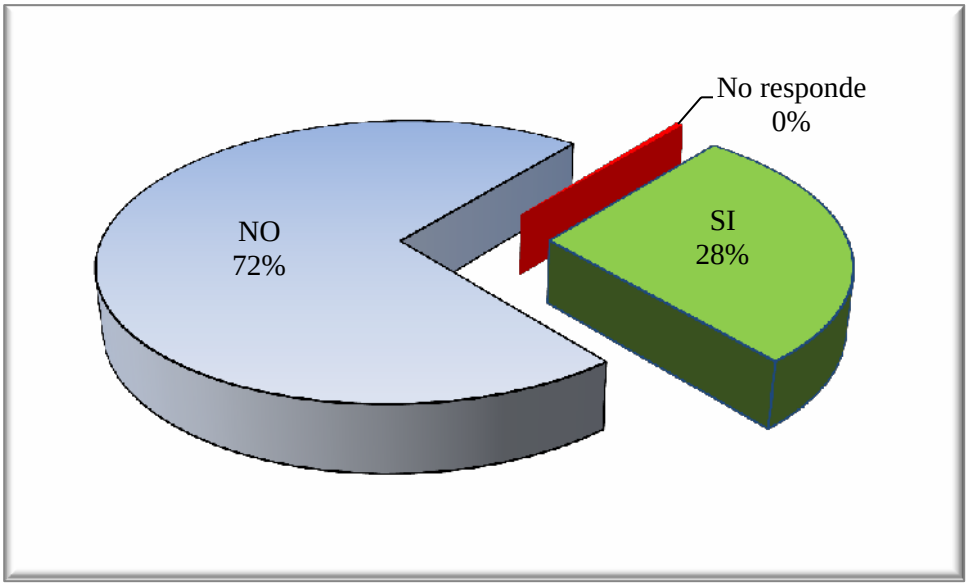
Tabla 12

¿Usted tiene conocimiento de alguno delito informático en redes sociales llevado a cabo por la vía judicial?

Categoría	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
SI	56	**27,9**	28,0	28,0
NO	144	**71,6**	72,0	100,0
Total	200	99,5	100,0	
No Responde	1	,5		
Total	201	100,0		

Figura 7

¿Usted tiene conocimiento de alguno delito informático en redes sociales llevado a cabo por la vía judicial?



Como resultado de las encuestas, concluimos que los delitos informáticos más frecuentes que se dan en las redes sociales entre los jóvenes del municipio de La Paz son: estafa y fraude (15%), acoso cibernético (14%), suplantación de identidad (11,5%), trata y tráfico de personas (10,8%), sexting (9,8%), difamación, calumnia y amenazas (9,5%), pornografía infantil (8,4%), phishing (7,5%), grooming (7,0%) y violación a la propiedad intelectual (5,3%); asimismo, dichos delitos son cometidos en las siguientes redes sociales más utilizadas: WhatsApp (22%), Facebook (18%), YouTobe (17%), TikTok (16%), Instagram (11%), Telegram (9%), y Linkedln (1%).

3.2 Análisis de las Entrevistas

Entrevista realizado al experto en Derecho Informático, Dr. Luis Fernando Zegarra Castro, (27 de marzo del año 2023).

En primer lugar, en el Código Penal Boliviano solo se tiene dos figuras penales sobre los delitos informáticos: "Manipulación informática (Art. 363 bis) y Alteración, acceso y uso indebido de datos Informáticos (Art. 363 ter)"; adicionalmente, para llevar a cabo un proceso judicial (acción penal) el Código de Procedimiento Penal en su Art. 384 (Contenido) exige la identificación del delincuente para proseguir con el proceso penal, la misma, en muchos casos no se los puede identificar a los delincuentes.

En ese contexto, los delitos informáticos en redes sociales más comunes que se cometen según el Observatorio de Delitos Informáticos[3] es: la "estafa" que se da sobre todo por Facebook y WhatsApp; en donde te ofrecen productos de alta calidad a mitad de precio; misma que motiva a las personas a querer adquirir dichos productos, realizando los depósitos a cuentas de los delincuentes; una vez realizado el depósito de dinero, los delincuentes desaparecen y las victimas no reciben ningún producto.

Por otro lado, tenemos la "difamación" a través de las redes sociales; si bien es un tipo penal que está contemplado en el código penal, no se puede llevar adelante el proceso penal, debido a que no se le puede identificar al delincuente, y el Código de Procedimiento Penal exige la identificación del delincuente para proseguir con el proceso.

Por lo tanto, muchos de los delitos informáticos en redes sociales ya estarían contemplados en el Código Penal Boliviano, con la única diferencia, de que dichos delitos

[3] El Observatorio de Delitos Informáticos, no es un observatorio formal, sino que es una iniciativa privada.

se cometen con la utilización de las tecnologías de información y comunicación (internet); de ahí que, varios autores llegan a afirmar que “son viejo delitos envasados en nuevas botellas”.

Consiguientemente, post pandemia COVID-19, los delitos informáticos se han incrementado exponencialmente en el municipio de La Paz, en la cual los delincuentes, con la utilización de la tecnologías se esconden detrás de una computadora, incluso fuera del territorio Boliviano. Después de la pandemia COVID-19, los delincuentes cometen sus crímenes con la utilización de la tecnología informática.

Por consiguiente, el Estado Boliviano crea la División de Cibercrimen a cargo de la FELCC, y que lo único que está realizando son patrullajes cibernéticos; asimismo, los delitos informáticos son en su mayoría “delitos privados”, en donde no interviene el Estado; y, al ser una afectación económica muy baja y el costo del proceso judicial altos, las víctima no tienden a denunciar.

Y por último, los delitos informáticos en redes sociales tienden a perfeccionarse con la Inteligencia Artificial. El fin de semana ha salido una alerta internacional sobre la recreación de voces con la Inteligencia Artificial, en la cual, se puedes simular la voz de cualquier persona; asimismo, lo que le ha pasado al propio Papa Francisco que a través de imágenes de inteligencia artificial se ha recreado una fotografía como si estuviera vistiendo un traje de diseñador,

Entrevista realizado al Sargento Primero Marco Saucedo Urquidi, investigador de la División de Cibercrimen de la ciudad de La Paz (2 de mayo del año 2023).

Los delitos informáticos más comunes que se dan en las redes sociales en el municipio de La Paz, y que vienen a la División de Cibercrimen de la FELCC La Paz a dejar su denuncia son entre ocho a diez personas por día; asimismo, los delitos más comunes que se reciben son: “estafa y difamación”, y los mismos, son realizados en su gran mayoría por las redes sociales de “WhatsApp y Facebook”.

Por una parte, la estafa se da por los diferentes perfiles falsos que utilizan los delincuentes para estafar; de igual forma, los delincuentes utilizan las cuentas de Tigo Money y Amazon, en la cual ofrecen productos de alta calidad a un precio muy bajo; una vez realizado el depósito de dinero por parte de las víctimas, los delincuentes desaparecen.

Por otra parte, tenemos la difamación, calumnia e injuria que son delitos de acción penal privada, pero que de alguna manera la División de Cibercrimen coadyuva, si bien no está inmerso en lo que es la policía y la fiscalía, nosotros sí coadyuvamos en la identificación de los perfiles de aquellas cuentas de las cuales están utilizando para difamar a las personas.

Adicionalmente, los delincuentes utilizan logos de las diferentes empresas en telecomunicación, mediante la cual, captan a sus víctimas para que realicen depósitos de dineros; y últimamente, se ha visto de que están utilizando imágenes de la policía boliviana, ya sea de la fuerza especial de lucha contra el crimen o del narcotráfico, indicando de que: estas personas han cometido algún tipo de delito y que si no van hacer el depósito de ciertas cantidades van a ser procesados o se les va seguir un juicio; les van

lavando en si el cerebro con diferentes acciones y videos amenazantes que mandan estas personas.

Por último, las sugerencias de prevención, serian que, si bien reciben estas personas algún tipo de mensaje o links, en primera instancia averigüen si evidentemente correspondería a la empresa de telecomunicación o alguna otra empresa y si es evidente y real, para que estas personas no lleguen a sufrir estos delitos, entonces es el consejo que siempre se les da a las personas, pese a eso, las personas utilizan los links, si bien sabemos que hoy en la actualidad, quien te puede regalar un celular o una suma de dinero, nadie no, entonces estas personas caen en estas dadivas que supuestamente van a recibir y llegado el momento no reciben nada, entonces sería que en primera instancia se comunique con la empresa que supuestamente le está auspiciando o que se ha ganado algo, para que de alguna manera desvirtué y no sea o sufra este tipo de delitos.

Entrevista realizado PhD. Karina Medinaceli Díaz, experta en Delitos Informáticos (24 de mayo del año 2023).

Primeramente hacer notar que, obtener datos o información sobre los delitos informáticos en las redes sociales es muy complicada o de difícil acceso (no tenemos una fuente verídica); incluso, el mismo órgano judicial no cuenta con datos. La única institución privada que recoge información, y asimismo coadyuva en la prevención y lucha contra el Cibercrimen (al mismo tiempo que denuncia), es el Observatorio de Delitos Informáticos en Bolivia (ODIB).

Por otra parte, el código penal boliviano solo cuenta con dos artículos sobre delitos informáticos: “Manipulación informática y Alteración, acceso y uso indebido de datos

Informáticos"; y que la misma, fueron introducidos en el Código Penal en el año de 1997, desde entonces, no ha tenido ninguna actualización hasta el día de hoy. Además, cuando un delito no está tipificado en el código penal, no es un delito; y por último, en derecho penal no existe la analogía.

En la estructura de la policía boliviana se crea la unidad de Cibercrimen en el año 2007 y 2009, llamado la "división de delitos informáticos", y se cierra por falta de denuncias; y, se reapertura en año 2018 - 2019 como la "División de Cibercrimen". Uno de los grandes problemas de la división de Cibercrimen es la movilidad constante del personal capacitado (siendo la principal causa por la que no se cuentan con registros).

En 2019 la Agencia de Gobierno Electrónico y Tecnología de Información y Comunicación (AGETIC) detecto los siguientes delitos informáticos en temas de "suplantación de identidad":

1. Personas que aparecían como acreedoras, con la simple fotocopia de su carnet de identidad.
2. Suplantación de padre e hijo (mismo nombre y apellido)
3. Suplantación de identidad en ventas de inmuebles.
4. Suplantación de madre e hija, para una operación del seguro.
5. Suplantación de dos hermanos con la licencia de conducir.

Por consiguiente, el delito de suplantación de identidad ha estado regulado por el código penal boliviano, pero, estaba vigente un par de meses y luego fue abrogado.

Y, según los artículos periodísticos que investigan los delitos informáticos en redes sociales, ponen a conocimiento uno de los delitos más comunes que se dan por

WhatsApp, con supuestos premios de Hipermaxi, Ketal, Boa, etc., que te llevan a un link, y lo único que hace es recoger datos para luego extorsionar.

BUDAPEST es la única institución internacional sobre los delitos informáticos, dicho convenio fue aprobado en el año 2001; y que varios países latinoamericanos forman parte del convenio y están compatibilizando sus normas con dicha institución; "en el caso de Bolivia, no está inscrita en el convenio de BUDAPEST", por la cual, no pude ser parte de la cooperación internacional sobre temas de delitos informáticos.

Por último, los delitos informáticos en redes sociales se amplifican con la "Inteligencia Artificial"; uno de estos casos es el programa Deepfake que usa la inteligencia artificial para editar videos con rostros de las personas, de igual forma copiar la voz de las personas para simular que dicen algo que nunca dijeron; misma que utilizan para estafar y difamar a las personas de su entorno, o incluso a la sociedad en su conjunto.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Con el crecimiento vertiginoso de las Tecnologías de la Información y la Comunicación (TIC) y actualmente con la Inteligencia Artificial, las redes sociales se han convertido en un nuevo contexto social de relacionamiento (proximidades virtuales), convirtiéndose en un componente indispensable para la humanidad. En ese contexto, los delitos informáticos en las redes sociales han evolucionado creando nuevas y sofisticadas formas de delinquir, dejando en la indefensión de las víctimas.

En cuanto a su regulación jurisdiccional, el código penal boliviano solo cuenta con dos artículos sobre delitos informáticos: “Manipulación informática y Alteración, acceso y uso indebido de datos Informáticos”; por lo cual, gran parte de los delitos cometidos en redes sociales no son regulados por la normativa; a su vez, para llevar una acción penal, el Código de Procedimiento Penal exige la identificación del sujeto activo, misma que no se lo puede identificar en muchos de los casos, por el anonimato de los delincuentes.

De manera que, los delitos informáticos en redes sociales más frecuentes que se dan en el municipio de La Paz son: estafa y fraude, acoso cibernético, suplantación de identidad, trata y tráfico de personas, sexting, difamación, calumnia y amenazas, pornografía infantil, phishing, grooming, y violación a la propiedad intelectual; dichos delitos son cometidos a través de las redes sociales más utilizadas como ser: WhatsApp, Facebook, YouTobe, TikTok, Instagram, Telegram y Linkedln.

Y por último, se estima que con la Inteligencia Artificial en desarrollo, los delitos informáticos en redes sociales se amplificarían exponencialmente, e incluso se estarían creando nuevas formas de cometer ilícitos por las redes sociales; mismas que debe ser analizado e investigado por los investigadores en el área del derecho informático y ramas anexas.

4.2 Recomendaciones

De todo el trabajo de investigación que se realizó, consideramos pertinente las siguientes recomendaciones:

En primer lugar, el Estado Bolivia debe formar parte del "Convenio de Budapest" para hacer frente a los delitos informáticos mediante la armonización de leyes entre naciones, así como cooperación, asistencia e investigación interna, como internacionalmente.

En segundo lugar, proponemos la actualización del código con la incorporación de un nuevo capítulo denominado "delitos informáticos y conexos"; en donde, se debe incorporar nuevas figuras delictivas; asimismo, la investigación debe ir a cargo de la fiscalía en todos los casos sobre delitos informáticos, y tener una coordinación más estrecha con las empresas que prestan los servicios de telefonía e internet.

En tercer lugar, prevenir a la ciudadanía, específicamente a niños, niñas y adolescentes, y en general a los sectores de la población más susceptibles de ser víctimas de los delitos informáticos en redes sociales, a través de programas educativos, así como

guías sobre buen uso de los servicios informáticos y redes sociales. Educación de los usuarios y consumidores de sistemas informáticos.

Y por último, a la Asamblea legislativa Plurinacional, considerar la propuesta de ley “Delitos Informáticos y Conexos”, para que pueda ser, analizado, discutido, sancionado y posterior promulgado como ley del Estado Boliviano.

PROPUESTA DE LEY

LEY GENERAL DE LOS DELITOS INFORMÁTICOS EN REDES SOCIALES

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- (Objeto). La presente ley tiene como objeto general la regulación de los delitos informáticos en redes sociales que se cometen a través de las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, como medio para la comisión de un delito o como fin u objeto del mismo.

Artículo 2.- (Partes). Las partes que componen el delito a efectos de la presente ley, son: Sujeto Activo, que será toda persona natural o jurídica que realiza el hecho delictivo; y un Sujeto Pasivo que será aquella persona natural o jurídica lesionada por el mismo.

Artículo 3.- (Marco normativo). La presente ley se rige por la Constitución Política del Estado, los tratados, convenios e instrumentos internacionales; de igual manera, la Ley Nº 1768 Código Penal, Ley Nº 1970 Código de Procedimiento Penal, y Ley Nº 164 de Telecomunicaciones, Tecnologías de Información y Comunicación.

Artículo 4.- (Finalidad). La presente ley tiene la finalidad de garantizar la prevención, investigación y sanción, de los delitos informáticos en redes sociales, que se cometen a través de las tecnologías de información y las comunicaciones (TIC), y la

inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop.

Artículo 5.- (Ámbito de aplicación). La presente ley se aplicará a los delitos cometidos en el territorio de Bolivia, y en los lugares sometidos a su jurisdicción; asimismo, se aplicara a quienes cometan los delitos dentro o fuera del territorio nacional.

CAPÍTULO II

DELITOS INFORMÁTICOS EN REDES SOCIALES

Artículo 6.- (Estafa y fraude). Los que con ánimo de lucro, utiliza el engaño a través de las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, induciendo al error por medio de artificios o engaños, sonsacara a otro dinero u otro beneficio o ventaja económica para sí o para un tercero, incurrirá en privación de libertad de dos (2) a seis (6) años.

Artículo 7.- (Acoso cibernético). El que por medio de las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, amenazare, maltratare, avergonzare, intimidare a una o varias personas mediante ataques personales, o divulgare información personal o falsa, será sancionado con privación de libertad de tres (3) a seis (6) años.

Artículo 8.- (Suplantación de identidad). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un

dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, suplante 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 de tres (3) a cinco (5) años.

Artículo 9.- (Trata y tráfico de personas). El que utilizando las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, reclutare, captare, trasladare, mediante amenazas o el uso de la fuerza u otras formas de coerción, será sancionado con prisión de cinco (5) a nueve (9) años.

Artículo 10.- (Sexting). El que sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales íntimos, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, será sancionado con privación de libertad de uno (1) a cuatro (4) años; si la víctima es menor de edad, la pena será de tres (3) a seis (6) años.

Artículo 11.- (Difamación, calumnia, injuria y amenaza). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, difame, calumnie, injurie o amenace, será sancionado con pena privativa de libertad:

I. Difamación. El que de manera, tendenciosa y repetida dañe la reputación de una persona con información falsa, será sancionado con privación de libertad de un año (1) a tres (3) años.

II. Calumnia. El que con la intención de causarle daño o perjuicio, acusare falsamente, será sancionado con uno (1) a tres (3) años.

III. Injuria. El que insultare a una persona con el fin de atentar contra su dignidad, honor, credibilidad, etc., será sancionado de uno (1) a tres (3) años.

IV. Amenaza. El que anunciare a alguien la intención de causarle un mal o provocarle un peligro, será sancionado de uno (1) a tres (3) años.

Artículo 12.- (Pornografía infantil). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, publicare, compartiere, enviare o distribuyere material pornográfico de un menor de edad, será sancionado con pena privativa de libertad de seis (6) a diez (10) años.

Artículo 13.- (Phishing). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, se gane la confianza por medio de engaños, haciéndose pasar por una persona o empresa, con el objetivo de obtener información personal confidencial, será sancionado con pena de reclusión de dos (2) a cuatro (4) años.

Artículo 14.- (Grooming). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, acosare o engañare a niños, adolescentes con fines sexuales, será sancionado con privación de libertad de dos (2) a cuatro (4) años; y si el hecho se llevara a cabo, será sancionado con tres (3) a ocho (8) años.

Artículo 15.- (Violación a la propiedad intelectual). El que, mediante las tecnologías de información y las comunicaciones (TIC) y la inteligencia artificial, con la utilización de un dispositivo informático como ser: computadora, celular inteligente, tablet, laptop, utilice o difunda obras de índole literal, imagen y audio, sin autorización del autor, será sancionado con privación de libertad de dos (2) a cuatro (4) años.

CAPITULO IV

COOPERACIÓN INTERNACIONAL

Artículo 16.- Principios Generales y Medidas de Cooperación. De conformidad con las disposiciones de la presente Ley y de los instrumentos internacionales y regionales pertinentes, las autoridades competentes promoverán la cooperación y asistencia multisectorial, intergubernamental e internacional con sustento en legislaciones uniformes o recíprocas y en la armonización de su derecho interno, con el fin de:

a) Prevenir y combatir los delitos informáticos en redes sociales.
b) Proteger y asistir a la persona naturales o jurídica que se ve afectada por la comisión de estos delitos;

c) Llevar a cabo investigaciones y actuaciones en relación con los delitos tipificados.

Artículo 17.- Acceso a la justicia. Para el cumplimiento de los fines de esta Ley, se adoptarán las medidas necesarias para que las víctimas de un delito tipificado conforme a las disposiciones de la presente y cometido en el territorio de otro país, puedan formular la denuncia ante las autoridades competentes de su lugar de residencia y tener asistencia adecuada.

Artículo 18.- Cooperación Mutua. Constituye un objetivo de la presente ley promover la cooperación público privado para la mejor concreción de la prevención, investigación y sanción de todo acto considerado delito informático en redes sociales, así como también para implementar programas de información y educación de usuarios y consumidores de servicios informáticos.

Artículo 19.- Acuerdos Bilaterales y Multilaterales. El Gobierno promoverá la celebración de convenios bilaterales y/o multilaterales sobre lo que es materia de la presente ley, con el fin de completar o reforzar las disposiciones de la misma y facilitar la aplicación de los principios que consagra.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 20.- Relación con otros Instrumentos Internacionales. Esta Ley no afectará a los derechos y obligaciones derivados de las disposiciones de otros instrumentos internacionales en los que el Estado nacional sea o llegue a ser parte, que contengan

disposiciones relativas a las materias reguladas por la presente y que garanticen una mayor protección y asistencia a las víctimas afectada por la comisión de los delitos informáticos en redes sociales.

BIBLIOGRAFÍA

LIBROS:

CLAVIJO CÁCERES, D., GUERRA MORENO, D. Y YÁÑEZ MEZA, D. (2014). *Método, Metodología y Técnicas de la Investigación Aplicada al Derecho.* Grupo Editorial Ibáñez, Bogotá Colombia.

CARBALLAR FALCÓN, J. A. (2011). *TWITTER Marketing personal y profesional*. Grupo RC. Service Point, Madrid España.

ESPINOZA VALENCIA, F. (2019). *Primer Diagnóstico sobre Ciberdelincuencia en Bolivia*. Fundación CONSTRUIR, La Paz Bolivia.

MORDUCHOWICZ, R., MARCON, A., SYVESTRE, V. Y BALLESTRINI, F. (2010). *Los adolescentes y las Redes Sociales*. Ministerio de Educación, Buenos Aires Argentina.

MACHICADO, J. (2010). *Concepto del Delito*. Apuntes Jurídicos, La Paz Bolivia.

NORIEGA SALAZAR, H. A. (2011). *Delitos Informáticos*. Instituto de la Defensa Pública Penal, Ciudad de Guatemala, Guatemala.

PRATO, L. B. Y VILLORIA, L. N. (2010). *Aplicaciones Web 2.0: Redes Sociales*. Universidad Nacional de Villa María, Ciudad de Villa María, Argentina.

RODRÍGUEZ, F. J. BARRIAS, I. Y FUENTES, M. T. (1994). *Introducción a la Metodología de las Investigaciones Sociales*. Ed. Política, La Habana Cuba.

SAMPIERI, R. H. (1998). *Metodología de la Investigación*. 2da. Ed. McGRAW-HILL Interamericana Editores, S. A. de C.V. Ciudad de México, México.

SAIN, G., MARTÍNEZ, M. S., TEMPERINI, M., RIQUERT, M. A., DUPUY, D., GRENNI, L., RÍOS, R.F., RESIO, M., ROIBÓN, M. M., ASPIS, A., DELBONO, P., BORZI CIRILLI, F. A., DARAHUGE, M. E. y ARELLANO GONZÁLES, L.

(2018). *Cibercrimen y Delitos Informáticos: Los Nuevos Tipos Penales en la Era de Internet*. Erreius, Buenos Aires, Argentina.

TÉLLEZ VALDÉS, J. (2008). *Derecho Informático*. 4ªed. Por McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V. Ciudad de México, México.

ZANONI, LEANDRO. (2008). *El Imperio Digital, el nuevo paradigma de la comunicación 2.0*. Ediciones B. Buenos Aires Argentina.

REVISTAS:

ALEMAÑY MARTÍNEZ, C. (2009). Redes Sociales: una nueva vía para el aprendizaje. *ECONPAPERS. Economics at your fingertips*, 1 (1). https://www.eumed. net/rev/ced/01/cam4.htm

BARRIUSO RUIZ, C. (2009) Las redes sociales y la protección de datos hoy. Universidad de Alcalá II, 301-338. https://core.ac.uk/download/pdf/58906859.pdf

HERNÁNDEZ DÍAZ, L. (2009). El Delito Informático. *Eguzkilore, Cuaderno del instituto Vasco de criminología*. Nº 23. P. 227-243. https://www.ehu.eus/documents/ 1736829/2176697/18-Hernandez.indd.pdf

IAB SPAIN. (2020). Estudio Anual de Redes Sociales 2020. #IABEstudioRRSS. https://iabspain.es/estudio/estudio-redes-sociales-2020/

LOREDO GONZÁLES, J.A. y RAMÍREZ GRANADOS, A. (2013). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celerinet. Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León, 44-51. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

PIFARRÉ, M.J., SALVADORI, I., LINARES, F. M. Y PICOTTI, L. (2013). Internet y Redes Sociales: un nuevo contexto para el delito. *IDP Revista de Internet, Derecho y Política*. Nº16, 40 – 49. https://www.redalyc.org/pdf/788/78828864004.pdf

RODRÍGUEZ JIMÉNEZ, A. y PÉREZ JACINTO, A. O. (2017). *Métodos científicos de indagación y de construcción del conocimiento.* Revista: esc.adm.neg. (EAN) No. 82, 179 – 200. http://www.scielo.org.co/pdf/ean/n82/0120-8160-ean-82-00179.pdf

TRIGO ARANDA, V. (2004). Historia y evolución de Internet. *Autores científico-técnicos y académicos, La revista de Acta*, Nº33. p. 22-11. https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf

TESIS:

BASTIDA RODRÍGUEZ, I. (2019) *El Derecho Penal y las Redes Sociales* [Tesis, Universidad de Valladolid de España]. https://core.ac.uk/download/pdf/250406305.pdf

CASTILLO RUGAMA, K.S. y ESPINOZA ALGABA, M.J. (2015) *Delitos Informáticos presentes en las Redes Sociales en Nicaragua y su correspondiente aplicación al sistema jurídico penal* [Trabajo Monográfico, Universidad Nacional Autónoma de Nicaragua]. http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/4191/1/230122.pdf

CHÁVEZ GALINDO, A. L. (2012) *Policía Cibernética: Vigilancia Preventiva, Permanente y Reactiva a los Ilícitos Informáticos* [Tesis, Universidad Rafael Landívar de Guatemala]. http://biblio3.url.edu.gt/Tesis/2012/07/01/Chavez-Ana.pdf

SANZ RODRÍGUEZ, P. (2014) *Redes Sociales y Derecho Penal* [Tesis, Universidad de Valladolib de España]. https://uvadoc.uva.es/bitstream/handle/10324/5518/TFG-N.22.pdf;jsessionid=A5760B5B283EE53B5467C605E67ACC84?sequence=1

VAL MORALES, L. M. (2019) *Los Delitos de Odio en las Redes Sociales* [Tesis, Universidad de Valladolid España]. https://uvadoc.uva.es/bitstream/handle/10324/37866/TFG-D_00826.pdf?sequence=1&isAllowed=y

ARCHIVOS PDF:

ACURIO DEL PINO, S. M. (2016). *Delitos Informáticos: Generalidades* [Archivo PDF]. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

BELLOCH, C. (2012). *Las tecnologías de la información y comunicación en el aprendizaje* [Archivo PDF]. https://www.uv.es/bellochc/pedagogia/EVA1.pdf

PONCE, I. (2012). *MONOGRÁFICO: Redes Sociales* [Archivo PDF]. http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales?format=pdf

RALLO LOMBARTE, A. y MARTÍNEZ MARTINEZ, R. (2010). Derecho y redes sociales. [Archivo PDF]. https://ebuah.uah.es/dspace/bitstream/handle/10017/8055/rallo_arenas_AFDUA_2010.pdf?sequence=1&isAllowed=y

ROS-MARTÍN, M. (2009). Evolución de los Servicios de Redes Sociales en Internet, *18* (5). https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/epi.2009.sep.10/21581

URUEÑA, A., FERRARI, A., BLANCO, D. Y VALDECASA, E. (2011). Las Redes Sociales en Internet. *ONTSI. Observatorio nacional de las telecomunicaciones y de la SI*. https://www.ontsi.es/sites/ontsi/files/redes_sociales-documento_0.pdf

LEYES Y DOCUMENTOS LEGALES:

CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL BOLIVIANO, 7 de febrero de 2009. La Paz Bolivia.

CÓDIGO PENAL BOLIVIANO, Ley Nº 1768 – 10 de marzo del 1997. La Paz Bolivia.

CONSEJO DE EUROPA, CONVENIO SOBRE LA CIBERDELINCUENCIA, BUDAPEST, 23.XI. 2001. Serie de Tratados Europeos- Nº185.

DICTAMEN 5/2009 sobre las redes sociales en línea. Grupo de trabajo sobre protección de datos del artículo 29. Dictamen 5/2009 sobre las redes sociales en línea, del Grupo de Trabajo sobre Protección de Datos del Artículo 29.

LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN, Ley Nº 164, de 8 de agosto de 2011. La Paz Bolivia.

POWER POINT:

JIMÉNEZ MARTÍN, J. (2015). *Delitos Informáticos* [Diapositiva PowerPoint]. Magistrado Subdirector Escuela Judicial Cartagena de Indias (Colombia). https://intercoonecta.aecid.es/Gestin%20del%20conocimiento/Jim%C3%A9nez%20Martin%20Jorge%20-%20Delitos%20inform%C3%A1ticos.pdf?ID=241

PÁGINA WEB:

EABOLIVIA.COM (…) *Historia del Internet en Bolivia*. https://www.eabolivia.com/blogs/17643-historia-de-internet-en-bolivia.html

WIKIPEDIA. La enciclopedia libre. https://es.wikipedia.org/wiki/Wikipedia:Portada

PERPLEXITY.AI. https://www.perplexity.ai/

ANEXO 1

https://unifranz.edu.bo/el-lado-mas-oscuro-de-la-inteligencia-artificial-la-ciberdelincuencia/

UNIFRANZ
Internacionalizate

EL LADO MÁS OSCURO DE LA INTELIGENCIA ARTIFICIAL: LA CIBERDELINCUENCIA

PUBLICADO POR PAULA BEATRIZ CAHUASA | 22 ABRIL, 2023

Extorsiones y otros delitos, a través de las redes sociales, se han vuelto frecuentes. Los adelantos tecnológicos y la Inteligencia Artificial (IA), que ofrecen grandes beneficios en diversos ámbitos, también están siendo aprovechados por redes delincuenciales no sólo en el país, sino en el mundo entero.

Datos de la Comisión Federal de Comercio de Estados Unidos dan cuenta que, sólo en 2022, más de 36 mil casos de extorsión telefónica fueron registrados en ese país con innumerables víctimas.

Marcelo Pacheco, director de la carrera de Ingeniería Comercial de la Universidad Franz Tamayo, Unifranz, asegura que, como ocurre con cualquier herramienta tecnológica, la IA puede ser utilizada para el bien o para el mal y que **los delincuentes pueden usarla para cometer** crímenes, como la **extorsión.**

"Sí, es posible utilizar la inteligencia artificial (IA) para realizar extorsiones, pero no es necesariamente fácil de hacerlo", indica.

Un ejemplo es el uso de los deepfakes (falsificaciones profundas), que son **videos manipulados mediante la IA** para hacer que una persona parezca decir o hacer algo que no ha hecho en realidad. Otro, es el uso de bots (robots) conversacionales (chatbots) para realizar estafas.

"Los bots pueden ser **programados para** hacer preguntas y **ofrecer información engañosa** o persuasiva para que las personas entreguen información personal o realicen pagos", puntualiza.

Bolivia no está al margen de los ciberdelincuentes

Al igual que otros países de la región, Bolivia no está al margen del accionar de los ciberdelincuentes. La extorsión y otro tipo de delitos cibernéticos pueden ser cometidos desde cualquier parte del mundo y los delincuentes pueden utilizar herramientas de IA para hacerlo.

"Algunas medidas de seguridad que pueden ser útiles incluyen mantener actualizados los programas de seguridad, **tener contraseñas seguras y únicas** para cada cuenta en línea, no compartir información personal con desconocidos en línea, y **ser cautelosos al hacer clic** en enlaces o descargar archivos de fuentes desconocidas", asegura el académico.

¿Una regulación de la IA evitaría su mal uso?

Debido a los posibles riesgos y desafíos que representa el uso de la IA para la sociedad, tanto actualmente como en el futuro, hay una imperiosa necesidad de una regulación ética y responsable.

Existen diferentes enfoques para regular la IA. Algunos países, por ejemplo, han establecido políticas y marcos regulatorios específicos para la IA, mientras que otros están considerando nuevas regulaciones o adaptando las ya existentes. En líneas generales, **la regulación** de la IA **se centra en la transparencia, la responsabilidad y la ética.**

William Llanos Torrico, docente de la materia de Derecho Informático en la Universidad Franz Tamayo, Unifranz, sostiene que **el delito informático implica actividades criminales** que los países han tratado de encuadrar en figuras típicas de carácter tradicional como robos, hurtos, fraudes, falsificaciones, estafas o sabotajes.

Sin embargo, la utilización de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las tecnologías, lo que demanda la necesidad de **mayor regulación por parte del Derecho.**

El impacto de las nuevas tecnologías está dando lugar a profundas transformaciones y el derecho debe responder ante estas nuevas relaciones.

Los bots activan conversaciones falsas con el objetivo de engañar a usuarios

Tips para evitar caer en redes extorsivas

- **Ser cautelosos** al interactuar con personas desconocidas en línea: Los delincuentes pueden utilizar bots conversacionales (chatbots) para realizar estafas o engañar a las personas para que entreguen información personal o realicen pagos.

- **Verificar la información** antes de compartirla: Las redes sociales y otras plataformas en línea pueden estar inundadas de información falsa o engañosa. Antes de compartir información en línea, es importante verificar la fuente y la veracidad de la información para evitar la propagación de noticias falsas o información engañosa.

- **Utilizar herramientas de seguridad**: Es importante mantener actualizados los programas de seguridad y utilizar herramientas como antivirus y firewalls para protegerse contra el malware y otros tipos de ataques cibernéticos.

- **Revisar** la configuración de **privacidad**: Las redes sociales y otras plataformas en línea suelen tener opciones de configuración de privacidad

que permiten controlar quién puede ver nuestra información personal y nuestras publicaciones.

- Estar informados sobre las últimas tendencias en IA y tecnología. Mantenerse informados sobre los últimos avances en tecnología y las tendencias en IA puede ayudarnos a **reconocer posibles riesgos y amenazas** y tomar medidas para protegernos contra ellas.

Inteligencia Artificial

Pacheco indica que la inteligencia artificial es un campo de la informática y la ingeniería que se centra en el desarrollo de sistemas informáticos capaces de realizar tareas que requieren inteligencia humana. Esto incluye el aprendizaje, la percepción, la toma de decisiones y el razonamiento.

Los sistemas de inteligencia artificial se basan en **algoritmos y modelos matemáticos** que les permiten analizar grandes cantidades de datos **para encontrar patrones** y hacer predicciones. Estos sistemas pueden ser entrenados con datos históricos y luego utilizados para tomar decisiones en tiempo real en situaciones nuevas.

Su aplicación es amplia y variada, desde la medicina hasta la fabricación y la logística. También está impulsando el desarrollo de tecnologías como los vehículos autónomos, los asistentes virtuales y los sistemas de recomendación personalizados.

ANEXO 2

https://unifranz.edu.bo/regulacion-de-las-tecnologias-imprescindible-para-prevenir-delitos-informaticos/

UNIFRANZ
Internacionalizate

REGULACIÓN DE LAS TECNOLOGÍAS, IMPRESCINDIBLE PARA PREVENIR DELITOS INFORMÁTICOS

PUBLICADO POR RICARDO ESPINOZA | 15 FEBRERO, 2023

La implementación de la tecnología, en casi todas las esferas de la sociedad, ha traído consigo múltiples beneficios y ha mejorado la calidad de vida de muchas personas, sin embargo, al ser infinitas las posibilidades que esta ofrece, su regulación y control son imprescindibles para garantizar la seguridad y el respeto a los derechos de los usuarios, una tarea en la que, desde hace varios años, se trabaja desde el Derecho a nivel global.

"La humanidad avanza a pasos agigantados con las nuevas tecnologías, los nuevos descubrimientos; la ciencia que progresa a diario nos obliga a adelantarnos, a adecuarnos y a superar su velocidad impresionante para trabajar en su regulación, las nuevas tecnologías deben ser reguladas", afirma Joaquín Vásquez, director de Derecho en UNIFRANZ El Alto.

Una de las herramientas más utilizadas a nivel global, el internet, reconocida por la Asamblea General de las Naciones Unidas, desde 2016, como un derecho humano, "por ser una herramienta que favorece el crecimiento y el progreso de la sociedad en su conjunto", no solo se constituye en un medio de comunicación masivo, donde uno puede conocer, en tiempo real, lo que sucede en cualquier latitud del mundo, sino también en un medio de almacenaje de impresionantes cantidades de datos e información, muchas veces relacionadas con la privacidad y dignidad de las personas.

Por ello, además de la libertad de expresión en Internet, la ONU también reivindica ciertos aspectos a tomar en cuenta por los Estados, como la protección de la libertad y la seguridad en Internet, la persecución de todas las violaciones de los derechos humanos y todos los abusos cometidos contra personas que ejercen sus derechos, el reconocimiento de la importancia de la privacidad online, entre otros.

"No podemos tener un solo aspecto humano que carezca de regulación, más aún cuando éste puede implicar un riesgo para la humanidad. Buscamos permanentemente la protección de los derechos, entenderlos, profundizar su alcance, lograr una mejora de vida, sin embargo, las nuevas TIC pueden poner en riesgo esto. Por ejemplo, el riesgo de no regular la Inteligencia Artificial (AI) puede suponer riesgos a la privacidad, a la seguridad", afirma el también abogado.

Para el profesional, si bien la transformación digital permite brindar calidad de vida y facilita a la humanidad lograr más cosas, de manera más rápida y eficiente, estas suponen una necesidad de regulación. No obstante, a decir del profesional, estas herramientas también deben ser aprovechadas para hacer más eficiente, más justo y proactivo el ejercicio del derecho.

El estado, como otras instancias públicas y privadas están frente al reto de ir a la par de la transformación digital y enfrentar el desafío de trabajar en la conformación de un nuevo Estado inteligente que garantice ciberseguridad a sus ciudadanos frente a las amenazas, no solo de hackers, sino de organizaciones criminales e inclusive Estados terroristas que impulsan el ciberdelito y el ciberterrorismo que nos pone en situaciones de indefensión a todo nivel. Estos y otros temas fueron el centro de reflexión de varios expertos en el área legal, durante el II Congreso Internacional de Derecho Informático y Derecho Empresarial: "Construyendo un nuevo orden", llevado a cabo por Unifranz en octubre de 2022.

DELITOS INFORMÁTICOS O CIBERCRÍMENES

El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos. En este sentido, se puede observar que, a través de la mayoría de tipos de delitos cibernéticos, los delincuentes tienden a utilizar estos métodos para robar información de tarjetas de crédito y obtener beneficios económicos. Asimismo, también se cometen delitos relacionados con derechos de propiedad intelectual, pornografía infantil y material de abuso.

IMPORTANCIA DE LA REGULACIÓN

Pese a las diferencias entre países, acorde a su nivel de desarrollo, la tecnología está presente en gran parte del globo terráqueo, incluyendo desde luego a Bolivia, en el que día a día se visibilizan múltiples avances en diversas áreas de la sociedad, mucho más desde la llegada de la pandemia, crisis que, pese a sus devastadoras consecuencias, sirvió de impulso para el salto tecnológico de las empresas, la digitalización de gran cantidad de servicios como la banca por internet, las compras en línea, entre otros.

Si bien fueron muchos los aspectos positivos, el boom digital también trajo consigo riesgos y amenazas a la seguridad de muchas personas y las organizaciones, a raíz del uso de las herramientas tecnológicas con fines ilícitos, para lo cual la Policía Boliviana cuenta con un área especializada, denominada Unidad de Cibercrimen.

"Vivimos en la era de las redes sociales, en la que tenemos la posibilidad de transmitir información en grandes cantidades, en cortos periodos de tiempo, lo cual hace necesaria una regulación nacional, que no solo considere el ámbito local sino mundial, universal, porque las transacciones, contratos, elementos de convicción no están en un solo lugar, no están en un lugar físico, sino que están en la nube, servidores de una empresa, en los teléfonos de ciertas personas entonces evidentemente necesitamos regular este aspecto", argumenta Vásquez.

Bolivia cuenta con la Ley N.º 164 de Telecomunicaciones, la cual regula la comunicación de datos, el comercio electrónico, la firma digital, entre otros. Asimismo, el Código Penal tipifica de manera específica los delitos de manipulación informática (Art. 363), acceso y uso indebido de datos informáticos (Art. 363), acoso cibernético (Código Niño, Niña y Adolescente). Sin embargo, se puede evidenciar que aún existen múltiples delitos cibernéticos que no se encuentran regulados o tipificados en la legislación.

Por otro lado, como sucede con otros tipos de hechos delictivos, muchos de ellos no llegan a ser denunciados y, por ende, no llegan a estrados judiciales. En otros casos, aquellos que podrían llegar a juicio son desestimados por no existir pruebas suficientes y la imposibilidad de dar con los autores, quienes se refugian en el anonimato.

Desde la formación de futuros profesionales en Derecho, el conocimiento y seguimiento a esta área del Derecho es fundamental, en pro de que las futuras autoridades y responsables de proyectar leyes caminen al paso de la tecnología, del conocimiento y aprovechamiento de sus ventajas, pero, fundamentalmente, de la preservación de los derechos de las personas.