



Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas Sociales y de la Justicia

**Delitos informáticos cometidos en las redes sociales en
Guatemala y el aporte del derecho comparado**
(Tesis de Licenciatura)

Claudia Marina Pec Vásquez

Guatemala, diciembre 2020

**Delitos informáticos cometidos en las redes sociales en
Guatemala y el aporte del derecho comparado**
(Tesis de Licenciatura)

Claudia Marina Pec Vásquez

Guatemala, diciembre 2020

Para los efectos legales y en cumplimiento a lo dispuesto en el artículo 1º, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Claudia Marina Pec Vásquez**, elaboró la presente tesis, titulada **Delitos informáticos cometidos en las redes sociales en Guatemala y el aporte del derecho comparado.**

AUTORIDADES DE LA UNIVERSIDAD PANAMERICANA

Rector M. Th. Mynor Augusto Herrera Lemus

Vicerrectora Académica Dra. Alba Aracely Rodríguez de González

Vicerrector Administrativo M. A. César Augusto Custodio Cóbar

Secretario General EMBA. Adolfo Noguera Bosque

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Decano Dr. Enrique Fernando Sánchez Usera

Vice Decana M. Sc. Andrea Torres Hidalgo

Director de Carrera M. A. Joaquín Rodrigo Flores Guzmán

Coordinador de Sedes M. Sc. Mario Jo Chang

Coordinador de Postgrados y

Programa de Equivalencias Integrales M.A. José Luis Samayoa Palacios

Coordinadora de Procesos académicos Licda. Gladys Jeaneth Javier Del Cid



UNIVERSIDAD
PANAMERICANA

"Sabiduría ante todo; adquiere sabiduría"

UNIVERSIDAD PANAMERICANA, FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA. Guatemala, treinta y uno de enero de dos mil veinte. -----

En virtud de que el proyecto de tesis titulado **DELITOS INFORMÁTICOS COMETIDOS EN LAS REDES SOCIALES EN GUATEMALA Y EL APORTE DEL DERECHO COMPARADO**, presentado por **CLAUDIA MARINA PEC VÁSQUEZ**, previo a otorgársele el grado académico de Licenciado(a) en Ciencias Jurídicas, Sociales y de la Justicia, así como los títulos de Abogado(a) y Notario(a), reúne los requisitos de esta casa de Estudios, es procedente **APROBAR** dicho punto de tesis y para el efecto se nombra como tutor al **DR. EDDY GIOVANNI MIRANDA MEDINA**, para que realice la tutoría del punto de tesis aprobado.



DR. ENRIQUE FERNANDO SÁNCHEZ USERA
Decano de la Facultad de Ciencias
Jurídicas y Justicia

 1779

 upana.edu.gt

 Diagonal 34, 31-43 Zona 16

Guatemala, 11 de mayo de 2,020

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como tutor del estudiante Claudia Marina Pec Vásquez, ID 000003920. Al respecto se manifiesta que:

- a) Brindé acompañamiento al estudiante en referencia durante el proceso de elaboración de la tesis denominada: Delitos informáticos cometidos en las redes sociales en Guatemala y el aporte del derecho comparado.
- b) Durante ese proceso le fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.
- c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE** para que se continúe con los trámites de rigor.

Atentamente,



Dr. Eddy Giovanni Miranda Medina

LIC. EDDY GIOVANNI MIRANDA MEDINA
ABOGADO Y NOTARIO



UNIVERSIDAD
PANAMERICANA

"Sabiduría ante todo; adquiere sabiduría"

UNIVERSIDAD PANAMERICANA, FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA. Guatemala, dieciocho de mayo de dos mil veinte. -----

En virtud de que el proyecto de tesis titulado **DELITOS INFORMÁTICOS COMETIDOS EN LAS REDES SOCIALES EN GUATEMALA Y EL APOORTE DEL DERECHO COMPARADO**, presentado por **CLAUDIA MARINA PEC VÁSQUEZ**, previo a otorgársele el grado académico de Licenciado(a) en Ciencias Jurídicas, Sociales y de la Justicia, así como los títulos de Abogado(a) y Notario(a), ha cumplido con los dictámenes correspondientes del tutor nombrado, se designa como revisor metodológico a la **LCDA. GLADYS JEANETH JAVIER DEL CID**, para que realice una revisión del trabajo presentado y emita su dictamen en forma pertinente.

DR. ENRIQUE FERNANDO SÁNCHEZ USERA
Decano de la Facultad de Ciencias
Jurídicas y Justicia

☎ 1779

🌐 upana.edu.gt

📍 Diagonal 34, 31-43 Zona 16



LCDA. GLADYS JEANETH JAVIER DEL CID
Abogada y Notaria

Guatemala, 21 de octubre de 2020

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como **revisora tesis** de la estudiante **Claudia Marina Pec Vásquez ID 000003920**, titulada: **Delitos informáticos cometidos en las redes sociales en Guatemala y el aporte del derecho comparado**. Al respecto se manifiesta que:

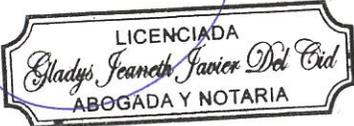
La versión final de la investigación fue objeto de revisión de forma y de fondo, estableciendo que la misma constituye un estudio serio, que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE**, para que se continúe con los trámites de rigor.

Atentamente,



Lcda. Gladys Jeaneth Javier Del Cid
Abogada y Notaria



LICENCIADA
Gladys Jeaneth Javier Del Cid
ABOGADA Y NOTARIA



UNIVERSIDAD
PANAMERICANA

"Sapientia ante todo; adquiere sapientia"

ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: CLAUDIA MARINA PEC VÁSQUEZ

Título de la tesis: DELITOS INFORMÁTICOS COMETIDOS EN LAS REDES SOCIALES EN GUATEMALA Y EL APORTE DEL DERECHO COMPARADO

El Decano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciado(a) en Ciencias Jurídicas, Sociales y de la Justicia, así como los títulos de Abogado(a) y Notario(a), el (la) estudiante: ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.

Segundo: Que tengo a la vista los dictámenes del Tutor y Revisor, en donde consta que el (la) estudiante en mención ha completado satisfactoriamente los requisitos académicos y administrativos vigentes para el desarrollo de la Tesis de Licenciatura.

Tercero: Que tengo a la vista el documento, *declaración jurada del estudiante*, donde consta que el (la) estudiante autor de la presente tesis manifiesta, bajo juramento, que ha respetado los derechos de autor de las fuentes consultadas y ha reconocido los créditos correspondientes; así como la aceptación de su responsabilidad como autor del contenido de su Tesis de Licenciatura.

Por tanto,

Se autoriza la impresión del documento relacionado en el formato y características que están establecidas para este nivel académico.

Guatemala, 27 de noviembre de 2020.

"Sapientia ante todo, adquiere sapientia"


Dr. Enrique Fernando Sánchez Usera
Decano de la Facultad de Ciencias
Jurídicas y Justicia



☎ 1779

🌐 upana.edu.gt

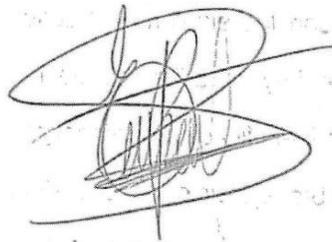
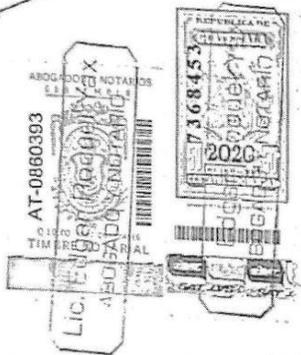
📍 Diagonal 34, 31-43 Zona 16

En la ciudad de Guatemala, el día treinta de octubre del año dos mil veinte, siendo las catorce horas en punto, yo, EDGAR ROQUEL YAX, Notario me encuentro constituido en la sede central de la Universidad Panamericana, ubicada en la Diagonal treinta y cuatro, treinta y uno guión cuarenta y tres zona dieciséis, de esta ciudad, en donde soy requerido por CLAUDIA MARINA PEC VASQUEZ, de cuarenta y tres años de edad, soltera, guatemalteca, auxiliar judicial, de este domicilio, quien se identifica con Documento Personal de Identificación (DPI) con Código Único de Identificación (CUI) dos mil cuatrocientos cincuenta y dos, cuarenta mil ciento sesenta, cero ciento uno, extendido por el Registro Nacional de las Personas (RENAP) de la República de Guatemala. El objeto del requerimiento, es hacer constar su **DECLARACIÓN JURADA** de conformidad con las siguientes cláusulas: **PRIMERA:** Manifiesta, bajo solemne juramento de Ley y advertido de la pena relativa al delito de perjurio, ser de los datos de identificación personal consignados en la presente y que se encuentra en el libre ejercicio de sus derechos civiles. **SEGUNDA:** Continúa manifestando bajo juramento el requirente: i) ser autor del trabajo de tesis titulado: "Delitos informáticos cometidos en las redes sociales en Guatemala y el aporte del derecho comparado"; ii) haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; iii) aceptar la responsabilidad como autor del contenido de la presente tesis de licenciatura. No habiendo nada más que hacer constar, finalizo el presente instrumento en el mismo lugar y fecha de inicio, treinta minutos después, la cual consta en una hoja de papel bond, impresa en ambos lados, que numero, sello y firmo, a la cual le adhiero los timbres para cubrir los impuestos correspondientes que determinan las leyes respectivas: un timbre notarial del valor de diez quetzales con serie y número AT- cero ochocientos sesenta mil trescientos noventa y tres (AT-0860393) y un timbre fiscal del valor

de cincuenta centavos de quetzal con número siete millones trescientos sesenta y ocho mil cuatrocientos cincuenta y tres (7368453) . Leo lo escrito al requirente, quien enterado de su contenido, objeto, validez y demás efectos legales, la acepta, ratifica y firma con el Notario que autoriza. DOY FE DE TODO LO EXPUESTO.

f-) 

ANTE MÍ:



A handwritten signature, likely of the notary, written in black ink.

Lic. Edgar Roquel Yax
ABOGADO Y NOTARIO

Nota: Para efectos legales, únicamente el sustentante es responsable del contenido del presente trabajo.

Dedicatoria

A Dios

El eterno Padre, Creador de la Saboduría, es el que me provee todo lo que necesitamos, y si hoy he llegado hasta donde estoy es por su Misericordia, y tomada de la mano de Dios puedo estar segura que él es la fuerza para lograr mis metas.

A mis padres

Rodolfo Antonio Pec Arenas y Myriam Amparo Vasquez Medina, a los que les debo la vida, son mis pilares y sin ellos jamás hubiera llegado a cumplir esta meta y ser una profesional del Derecho.

A mis hijos

Jeraldinne María Jimenez Pec y Pablo Rodolfo Jimenez Pec, son la bendición más grande que Dios me ha dado, mi motor, han sido parte fundamental para alcanzar esta meta.

A mi familia

Por apoyarme en todo momento, y no dudo que se alegran por haber alcanzado ésta meta.

A mi novio Jaime Escobar por su apoyo y amor incondicional, siempre te estaré agradecida por impulsarme siempre a triunfar.

A mis Compañeros Quienes siempre me han apoyado con su amistad, apoyo incondicional.

A la UPANA Por darme la enseñanza y el conocimiento.

Índice

Resumen	i
Palabras clave	ii
Introducción	iii
Delitos informáticos	1
Redes sociales	26
Análisis jurídico de los delitos informáticos cometidos en las redes sociales en Guatemala	44
Delitos en las redes sociales	49
Aporte del derecho comparado sobre los delitos informáticos en redes sociales	54
Conclusiones	65
Referencias	67

Resumen

Es justo decir, que el uso de las nuevas tecnologías ha sido una experiencia positiva para el mundo, porque a través de estas tecnologías se puede conocer en tiempo real lo que pasa en cualquier parte del mundo, sin embargo, se debe reconocer que no sólo trajo experiencias positivas, hay que mencionar que para muchos países las nuevas tecnologías se han convertido en una herramienta más para los delincuentes, lo que llevó a la necesidad de que esa conducta fuera tipificada en un nuevo tipo penal, este es conocido como delitos informáticos, no obstante ello, esta es sólo una modalidad, ya que, de allí se desprenden otros delitos, los más conocidos son: el robo de identidad (pishing), el ciberacoso (cyberbulling), la sexualidad, seducción y abuso virtual (sexting, grooming), chantaje sexual (sextortion), programa malicioso (*malware*). En varios países esta conducta ya se encuentra regulada, no así en Guatemala, ya que, no se cuenta con una ley especial que norme este tipo de conductas.

En este sentido, se hizo necesario ir a consultar la legislación comparada en los países de España, Argentina, México y Costa Rica pudiendo comprobar que en efecto y a diferencia de Guatemala, en otros países sí cuentan con una normativa específica de los delitos informáticos cometidos en las redes sociales.

Palabras clave

Delitos. Informático. Redes. Tecnología. Derechos.

Introducción

Es importante señalar, que las acciones delictivas pueden cometerse en forma directa y personal, pero a la vez se pueden cometer haciendo uso de las redes sociales a través del uso de un computador o teléfono celular lo cual se conoce doctrinariamente como delitos informáticos, para lo cual el Estado debe garantizar a sus habitantes el bien común, creando políticas que vayan enfocadas en minimizar los actos delictivos, toda vez que resulta importante señalar que efectivamente el uso de las redes sociales y su indebida aplicación ha generado en diversas partes en el mundo y Guatemala no es la excepción de cometer hechos delictivos.

Dentro de las razones que justifican la elaboración de la presente tesis, es que, en Guatemala exista una normativa específica en materia de delitos informáticos, los cuales se han visto marcos dentro de la sociedad guatemalteca, y que, lastimosamente hasta la presente fecha no se han podido resolver por no contar con el procedimiento adecuado.

Si en Guatemala se contará con una normativa específica en materia de delitos informáticos, se estaría dando cumplimiento a uno de los fines del Estado, que es el mantenimiento de la paz social para lo cual debe crear las condiciones necesarias para que los habitantes puedan vivir y comunicarse en armonía, en ese sentido también el Estado en uso de su

poder de imperio (*ius puniendi*), es decir, la potestad que tiene de legislar y determinar sanciones a los responsables de una norma de conducta toda vez que se hallen responsables ante un órgano jurisdiccional competente.

Es por ello que el objeto de la presente investigación es conocer los delitos informáticos cometidos en las redes sociales en Guatemala y el aporte del derecho comparado y los objetivos específicos, a) establecer las nuevas técnicas por las cuales se cometen ilícitos a través de las redes sociales; b) determinar la necesidad de legislar para sancionar a los autores y cómplices que participen en la comisión de delitos informáticos en redes sociales.

Para la elaboración del presente estudio se utilizará el método analítico el cuál orientará a la investigadora para realizar un análisis profundo de la generalidad del tema central, así como determinar la literatura existente, cuáles serán las partes fundamentales que deben incorporarse y sobre todo lo esencial que será incluido en el informe final. El enfoque del presente trabajo de investigación es dar a conocer en el primer capítulo los delitos informáticos, conocer sus aspectos generales, la definición, los sujetos que intervienen en la perpetración del ilícito y las técnicas por las cuales se cometen ilícitos a través de las redes sociales y la necesidad de legislar una ley penal especial que prevenga y sancione este tipo de ilícitos cometidos a través de las redes sociales, no reformar las existentes, ya que,

este tipo de delitos tienen sus propias características y las sanciones deben ser acordes al daño moral ocasionado. En el tercer y último capítulo se tratará lo referente a los servicios que prestan las redes sociales, la protección a la información personal, el aporte del Derecho Comparado (Argentina, México y Costa Rica) sobre los delitos informáticos en redes sociales y se hablará de la necesidad de legislar una ley penal que prevenga y sancione ese tipo de ilícitos cometidos a través del uso de internet en especial las redes sociales.

Delitos informáticos

Aspectos generales

La convivencia que se genera en forma cotidiana entre los seres humanos ha sido fundamental para el desarrollo de la sociedad, no obstante, hay que considerar que algunas conductas resultan inapropiadas en la relación social, es por ello que es imprescindible establecer una serie de normas jurídicas que permitan la regulación de todo lo que pueda ser perjudicial, cabe resaltar que el orden jurídico es considerado en la doctrina como uno de los elementos constitutivos de todo Estado. Ahora bien, las normas jurídicas son parte del campo de estudio de la ciencia del derecho, la cual se ha dividido en una serie de disciplinas para una mejor comprensión, siendo una de ellas el Derecho Penal.

Los autores de Mata Vela & de León Velasco, manifiestan al respecto:

De las distintas ramas del conocimiento humano, el derecho es sin duda una de las más antiguas, cuya misión ha sido regular la conducta de los hombres a través del complicado devenir histórico de la sociedad, tratando de alcanzar la justicia, la equidad y el bien común como los valores fundamentales más altos a los que aspira (...) y de las ciencias eminentemente jurídicas (...) el Derecho Penal, la disciplina más vieja, cuya misión siempre ha sido (...) proteger valores fundamentales del hombre, tales como: su patrimonio, su dignidad, su honra, su seguridad, su libertad, y su vida como presupuesto indispensable para gozar y disfrutar de todos los demás. (2016, pág. 3)

Entre lo expuesto por los autores, resulta ineludible la idea acerca del complicado devenir histórico de la sociedad, puesto que cada período de tiempo ha sido marcado por diferentes circunstancias, entre otras, de naturaleza económica, política, geográfica, étnica, cultural, ética, moral, aspectos que deben considerarse esenciales para poder establecer precisamente una serie de normas de conducta que permitan la convivencia en armonía, es oportuno señalar que el Estado de Guatemala de acuerdo a lo establecido en el artículo 1º. de la Constitución Política de la República tiene como fin supremo la realización del bien común, partiendo de una especial protección a la integridad de la persona y la familia a través de una serie de deberes que el mismo texto constitucional impone para el Estado, además de una serie de derechos fundamentales que recopila, los cuales deben ser garantizados por medio de una tutela efectiva, misión que en efecto se procura por medio de la disciplina del derecho penal.

Zambrano Pasquel, señala que el Derecho Penal “puede ser concebido desde un punto de vista objetivo, es decir como un sistema normativo, y desde un punto de vista subjetivo en el que debe ser apreciado como potestad del Estado”. (2019, pág. 1).

El autor permite obtener una perspectiva sobre ésta disciplina, sin embargo, es preciso resaltar que no trata cualquier sistema normativo, éste resulta de naturaleza especial, ya que a través de su contenido se establecen la conductas que serían consideradas constitutivas de delito o falta, se fija la pena que se podrá imponer y en algunos casos medidas de seguridad, por otra parte, la facultad que se le reconoce al Estado es la de perseguir y castigar todas aquellas acciones delictivas que puedan acaecer.

Según Gómez de la Torre, y otros:

“El Derecho Penal es el instrumento jurídico más enérgico del que dispone el Estado para evitar las conductas que resultan más indeseadas e insoportables socialmente (...) tiene su razón de ser en constituir un medio imprescindible para posibilitar la vida en comunidad”
(2016, págs. 1-3)

Conforme a lo anterior, se puede inferir que la finalidad de la disciplina jurídica del Derecho Penal, es mantener el orden y la paz en la sociedad, tarea que en definitiva ha sido objeto de un proceso largo de construcción y por supuesto de evolución, puesto que se debe configurar en atención a la realidad de cada contexto.

Hoy en día es imprescindible que se consideren factores como la globalización; la conectividad a través de internet; la transformación de los medios de comunicación; el uso y desarrollo de las Tecnologías de la Información y Comunicación; la implementación de herramientas

digitales en la prestación de servicios públicos y privados; el procesamiento y almacenamiento de datos personales; el comercio electrónico; la banca electrónica; aspectos que de alguna manera han contribuido con el desarrollo de la sociedad, pero, también han permitido el surgimiento de nuevas formas de delinquir, por lo que cada Estado debe preocuparse por garantizar la seguridad de sus habitantes ante cualquier amenaza.

Al respecto Flores Salgado, manifiesta:

(...) el avance tecnológico informático ha tenido un gran impacto en casi todas las áreas de la vida social, sin embargo, derivado del uso de la computadora vemos que ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos (...) (2014, pág. 131)

En la actualidad hay que considerar que ya no es sólo el uso de la computadora, es tan común que las personas cuenten con dispositivos móviles como los *smarthphones*; *smarthwatch*; tabletas, ordenadores portátiles, todos conectados a *internet*, a los cuales se les suman, consolas de videojuegos, televisores, cada uno de ellos a merced de los llamados delitos informáticos, debido al acceso que pueden tener criminales por medio de las denominadas redes telemáticas.

A decir de Santos González:

(...) una red telemática (o red de datos) se podría definir como la infraestructura que posibilita que varios dispositivos intercambien datos entre sí, conectados para ello a algún medio físico que permita la transmisión (...) Los dispositivos que forman parte de la red también reciben el nombre de nodos. En cuanto a los medios físicos a través de los cuales viajan los datos, estos pueden ser medios guiados (como el clásico cable de cobre o la fibra óptica, o se pueden utilizar ondas electromagnéticas transmitidas a través del aire. (2015, pág. 16)

En esencia, a través de las redes telemáticas es posible una interconexión de dispositivos que permite el acceso en forma sencilla, práctica y a distancia de una serie de recursos y datos que se encuentren en unidades de almacenamiento. Actualmente el uso de la red más grande conocida como internet es generalizado, circunstancia que favorece la aparición de nuevas formas de delinquir, las cuales aún no se tipifican en muchas de las legislaciones a nivel mundial, aunque ya existen algunos referentes, los cuales se tratarán en el desarrollo de la investigación.

Barrio Andrés, indica:

Internet es, sin duda, la clave de bóveda en la Sociedad de la Información (...) La popularización de la Red a escala global ha permitido la creación del ciberespacio virtual, al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, sobre todo en la última década del siglo XX, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales. Incluso ha surgido una nueva disciplina jurídica, el Ciberderecho (...) para dar respuesta a las situaciones jurídicamente disruptivas. (2018, pág. 17)

No resulta extraño que los avances tecnológicos hayan dado lugar a nuevos conceptos, en la cita se hace referencia al término ciberespacio virtual, un espacio distinto al que nuestros sentidos están acostumbrados a

percibir en forma física, es decir, un entorno diferente, reconocido también como espacio digital, escenario que en la actualidad tiene relevancia jurídica por acciones perjudiciales que se han ejecutado en los últimos años por personas maliciosas, en palabras del autor, situaciones jurídicamente disruptivas, que básicamente representan una ruptura a la paz y orden social, por lo que el derecho penal tradicional de alguna manera debe transformarse, ya que con anterioridad para tipificar delitos sólo se han considerado acciones u omisiones que tienen lugar en el mundo físico, que permite su ubicación en tiempo, modo y lugar. En cuanto a la idea del surgimiento del ciberderecho o derecho informático como disciplina jurídica, no tardará en ser reconocido en la ciencia del derecho, puesto que la tecnología seguirá avanzando y no importando las condiciones, el bien común como fin supremo debe prevalecer en todo momento, quedando obligado cada Estado a implementar las medidas pertinentes, en especial, el tratamiento de los delitos informáticos.

El uso de una amplia gama de dispositivos digitales, la trascendencia que ellos representan en los sistemas de almacenamiento y procesamiento de información, la realización de actividades cotidianas, así como en los diferentes instrumentos de trabajo y la importancia y sensibilidad que pueden tener los datos acumulados, hace aconsejable e impostergable la protección penal de diversos bienes y valores de cualquier amenaza, idea que comparten los autores Marco Galindo, Marco Simó, Prieto Blázquez,

& Segret Sala, al afirmar que, “los sistemas informáticos constituyen, hoy día, un pilar fundamental en el que se sustentan organizaciones de todo tipo para dar apoyo a sus actividades” (2010, pág. 47).

Es incuestionable que los dispositivos digitales se encuentran presentes en casi todos los rincones del mundo, así como la idea de que ha representado ventajas para el hombre en los diferentes ámbitos en los que se utiliza, no obstante, como ya se hizo mención, conlleva nuevos riesgos.

Galán Muñoz, asevera:

Las posibilidades de abusos mediante sistemas informáticos no solo existen, sino que, como ha demostrado la realidad, son múltiples y variados. Ello ha llevado a que se haya dejado atrás, hace ya mucho tiempo, la utópica idea de que el entorno digital podía autorregularse, sin que fuese necesario que los Estados interviniesen y controlasen las actividades de los ciudadanos. (2019, pág. 14)

Con respecto a ello, es claro que el uso de la tecnología debe regularse y sobretodo protegerse, para lo cual es imprescindible la intervención del Estado.

Definición

Es importante considerar que en la doctrina además del concepto delito informático, para referirse al mismo fenómeno, también se utilizan los siguientes: delito telemático, ciberdelito, delito electrónico.

Barrios Osorio, citando a Davara define delito informático como:

(...) la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea *hardware o software*. (2010, pág. 135)

Entre los aspectos que sobresalen de la definición se encuentran: a) la conducta debe caracterizarse por ser típica, antijurídica, culpable, imputable y punible, elementos que la doctrina ha determinado para que la acción u omisión se califique como delito, en este aspecto es fundamental la labor legislativa, puesto que es el Organismo de Estado a quien se le ha delegado el proceso de creación de la ley, la única fuente para crear tipos penales; b) el instrumento para la comisión del hecho delictivo debe ser un dispositivo digital conectado a cualquier red telemática, circunstancia que merece especial atención y cooperación a nivel internacional, ya que debido a la alta conectividad que existe a nivel mundial, un ataque podría ejecutarse desde cualquier parte del mundo; c) la actividad delictiva puede tener como objeto la destrucción de componentes físicos de un dispositivo, ocasionar daños al sistema operativo que permite su funcionamiento o aprovecharse de datos que se encuentran compartidos en un sistema informático.

Los autores Raya Cabrera, Raya González, & S. Zurdo, indican que cada uno de los sistemas informáticos incorpora tres elementos de la siguiente manera:

Un componente físico (*hardware*): incluye las placas, circuitos integrados, conectores, cables y sistema de comunicaciones.

Un componente lógico (*software*): permite disponer de un lenguaje lógico para comunicarse con el hardware y controlarlo. Hay dos tipos de software:

Software de base: es el conjunto de programas necesarios para que el hardware tenga capacidad de trabajar. Recibe también el nombre de sistema operativo.

Software de aplicación: son los programas que maneja el usuario (tratamiento de textos, bases de datos, hojas de calculo...).

Un componente humano: está constituido por las personas que participan en la dirección, diseño, desarrollo, implantación y explotación de un sistema informático. (2014, pág. 18)

En palabras sencillas, *hardware* es todo componente físico que forma parte de la estructura de cualquier dispositivo digital; *software* en cambio, se integra por elementos intangibles que a partir de códigos especiales permiten el funcionamiento de los aparatos; finalmente, resulta interesante que los autores incluyan al elemento humano como parte del sistema informático, puesto que, precisamente todas las creaciones y avances tecnológicos están al servicio del hombre, los beneficios en la vida cotidiana han sido muchos, lamentablemente algunos los utilizan en perjuicio de otros.

Noriega Salazar, establece otra definición sobre delito informático, considerando que es:

(...) toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático, o a producir un resultado de daño en ésta o de los sistemas que la misma hace operar. (2011, pág. 23)

A criterio de la investigadora, la definición anterior resulta más completa al incluir la tipicidad y antijuricidad entre los elementos de la definición; en cuanto el medio a utilizar para la comisión del delito, se comparte la misma idea, una computadora, al igual que el fin que persiguen los delitos informáticos, siendo éste causar daños a un sistema informático o bien aprovecharse de archivos que se encuentren compartidos o almacenados, ya sea por personas particulares, instituciones públicas o privadas, inclusive por Organismos de Estado.

Analizadas cada una de las ideas, se define el delito informático, como toda acción de carácter ilícita y antijurídica que ejecuta cualquier persona empleando para ello, un dispositivo digital conectado a una red telemática, que tiene por objeto causar daño material o inmaterial a bienes jurídicos que merecen una tutela de índole penal.

En ese sentido, Noriega Salazar, expone que:

(...) en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro. Por un lado las acciones que van dirigidas al sabotaje, el daño, la destrucción o pérdida de equipos de computación afectan (...) el patrimonio, por otro lado

(...) pueden afectar (...) la indemnidad sexual, la privacidad (...) la propiedad intelectual
(...) (2011, pág. 24)

El imparable avance que tiene la tecnología a nivel mundial, sin lugar a dudas expone cada vez más a la sociedad a todo tipo de delito informático, no hay sector alguno que pueda quedar fuera del alcance de la criminalidad; es más, considerando que existen grupos más vulnerables como la niñez, la adolescencia y las mujeres, debe agilizarse la actualización del marco legal de cada país, de tal manera que sean tipificados y por ende castigados de conformidad de la ley.

Siendo un tema de actualidad e interés para los operadores de justicia, la doctrina ha empezado a ahondar en aspectos relacionados a los delitos informáticos, su definición, elementos, clasificación, regulación legal nacional e internacional, los cuales deben ser considerados en la adopción de un mecanismo que le permita al Estado castigar ese tipo de conductas antisociales, en Guatemala más allá de incluir su tipificación en el Código Penal, sería pertinente crear una ley especial considerando para el efecto aplicar una pena principal y otra accesoria, además de fortalecer la institucionalidad del sistema de justicia, de tal modo que se tengan los medios necesarios para contrarrestar el mal que ocasionan estos ilícitos.

Actualmente, determinar la comisión de un delito informático en Guatemala, no es tan fácil, esto debido a que el Ministerio Público, no cuenta con el personal altamente calificado, ya que resulta un tanto complicado establecer en qué momento se causó el mismo; otra de las desventajas que existen en el país, en cuanto a la comisión de este tipo de delitos, es la facilidad de su ejecución, ya que el instrumento utilizado puede ser manipulado desde cualquier lugar; finalmente, aún no existen tipos penales en los que se pueda encuadrar la conducta delictiva, ya que no se cuenta con una normativa específica.

Significa que, en el caso de Guatemala, el delito informático, no es conocido como tal, aunque algunas conductas de esta naturaleza pueden relacionarse con delitos establecidos de manera expresa en el Código Penal vigente, es necesario considerar la emisión de una normativa especial que permita establecer cuáles son los aspectos o características que diferencian a este tipo de delitos de los demás.

Para una mejor ilustración, dentro de los aspectos que contribuyen a determinar con exactitud la configuración de los delitos informáticos, se pueden mencionar entre otros, los siguientes:

- Son conductas criminales de personas especializadas en la materia.
- Solo un cierto número de personas con conocimientos técnicos puede llegar a cometerlos.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de las funciones y organizaciones del sistema tecnológico y

económico.

- Son acciones que en muchas ocasiones se realizan cuando el sujeto trabaja.
- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo, espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Ofrecen facilidades para su comisión, a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. (Landa, 2007, p.237)

Bien jurídico tutelado

Se debe tener presente que el bien jurídico no es creado por el derecho, sino más bien este los reconoce, debido a que los intereses son vitales y fundamentales en una sociedad, es por ello que la misma Constitución Política de la República de Guatemala, también los reconoce, debido a ello existe normativa que debe velar por el buen cumplimiento de lo establecido en la misma, para el efecto, se debe tener claro que dentro de estos bienes jurídicos tutelados se encuentra la vida, la familia, la salud, la seguridad entre otros establecidos en la carta magna.

Para el efecto, se debe considerar de conformidad con González, lo siguiente:

Bien jurídico es el interés jurídicamente protegido. Todos los bienes jurídicos son intereses vitales, intereses del individuo o de la comunidad: los intereses no los crea el ordenamiento sino la vida; pero la protección jurídica eleva el interés vital a bien jurídico. El bien jurídico

protegido es el fundamento de la norma. La prohibición de una conducta y la imposición de una sanción, sólo se justifican en cuanto sirvan para proteger un bien jurídico. Así por ejemplo, la prohibición de la conducta de matar se justifica en la protección al bien jurídico vida o la interdicción de hurtar en la defensa del bien jurídico propiedad. (2019, p.18)

Se considera de interés, hacer referencia a que el bien jurídico tutelado, como ya se hizo mención incluye a los delitos que se puedan cometer en contra de las personas, en especial cuando esta sufre algún tipo de agravio físico, asimismo, se encuentran los delitos contra el honor, lo cual incluye la dignidad, el decoro, la moral; aunado a estos, la propiedad, la seguridad, son otros de los derechos que se deben proteger, aunque los mismos encuentran protección en los delitos regulados en el Código Penal vigente en Guatemala, deben fortalecerse atendiendo los nuevos riesgos de la tecnología.

En cuanto al bien jurídico tutelado en los delitos informáticos, se debe considerar los contenidos en el Código Penal, dentro de los cuales se regulan en su orden, en el artículo 274 “A” la destrucción de registros informáticos con pena de prisión y multa. Además, el artículo 274 “B” la alteración de programas con similar pena con la antes indicada. El artículo 274 “C” regula la reproducción de instrucciones o programas de capacitación sancionado con pena de prisión y multa. Asimismo, el artículo 274 “D” regula los registros prohibidos y sanciona a quien crea bancos de datos cuando los mismos puedan afectar la intimidad de las personas; lamentablemente es una práctica que no resulta ajena en el país.

Asimismo, el artículo 274 “E” regula la manipulación sancionada con prisión y multa y que se refiera a programas de computación para alterar información. Además, el artículo 274 “F” regula el uso de información también sancionado con prisión y multa para la persona que obtenga datos obtenidos en registros informáticos para lo cual el artículo 274 “G” regula programas restrictivos también sancionado con prisión y multa a quien pusiere en circulación programas que causen perjuicio a los registros o equipo de computación y finalmente el Artículo 274 “H” regula la alteración maliciosa de numero de origen es decir cuando en un equipo de cómputo exista un operador extranjero de telefonía utilizado exclusivamente para tráfico, lo que representa la alteración de la identificación del usuario.

Ante todo, se debe tomar en cuenta que el Código Penal fue reformado en el año de 1996 es decir, ya existe una diferencia de veinticuatro años, razón por la cual la normativa en mención requiere de una reforma, por medio de la cual se pueda actualizar lo relativo a los delitos informáticos, tomando en consideración que en esa época se tendía a confundir el tema objeto de análisis.

En la actualidad son más evidentes las nuevas formas de delinquir que tienen lugar en el vertiginoso avance de la informática; aunque podría decirse que la comisión de éstos, se reduce a la obtención de un beneficio económico y por intereses políticos o ideológicos.

Regulación legal

Guatemala no es la excepción en la implementación de los medios tecnológicos que se han descubierto y aplicado en materia de sistemas operativos, los cuales han transformado las reglas y actividades como la contratación; las nuevas modalidades de comercio, comunicación, banca, entre otros, ya que es un país, que de forma común se adapta a los diferentes cambios que se promueven desde las sociedades desarrolladas; por lo que es imprescindible priorizar el abordaje de los llamados delitos informáticos, para beneficio de la población en general, no sólo a través de las normas de tipo sustantivo; ya que también es pertinente robustecer aspectos procesales para una efectiva persecución penal de dichas conductas antijurídicas, es oportuno señalar que el país no sería el único que tendrá la difícil tarea de fortalecer su ordenamiento jurídico.

De hecho, a criterio de Flores Salgado:

El derecho penal de los estados interesados en combatir esta nueva delincuencia, contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y métodos disponibles en el derecho penal. (2014, pág. 134)

En el país, algunos de los aspectos que podrían obstaculizar la lucha contra los delitos informáticos están: la poca inversión en la adquisición de tecnología de punta que permita a quienes intervienen como operadores de justicia efectuar la persecución de aquellas personas que comentan delitos de este tipo; la escasa actualización; que es un fenómeno que se encuentra aún en formación.

En relación a la normativa legal vigente en materia penal, puede calificarse hasta cierto punto como obsoleta, ya que la amplia gama de delitos informáticos que pueden ser cometidos, no se contemplan del todo en el Código Penal, Decreto Número 17-73 del Congreso de la República de Guatemala. Dicha circunstancia, lamentablemente favorece que determinados actos delictivos queden en la impunidad, ya que conforme al principio de legalidad establecido en el artículo 17 de la Constitución Política de la República y el artículo 1 del Código Penal, ninguna persona puede ser penada por hechos que no se encuentren establecidos de forma expresa como delito o falta.

De alguna manera, podría manifestarse que el Estado de Guatemala no brinda la seguridad y certeza jurídica que tiene como deber conforme al artículo 2°. de la Constitución Política de la República, en ese sentido, debe aumentar su interés y los esfuerzos para evitar que personas sin escrúpulos sigan aprovechando el ciberespacio para cometer fechorías,

beneficiándose del vacío legal que existe a la presente fecha. Lo cual seguirá siendo perjudicial para personas particulares, empresas, instituciones públicas, organizaciones no gubernamentales, en fin, cualquiera que utilice dispositivos digitales.

Sujetos del delito informático

De conformidad con los aspectos doctrinarios del Derecho Penal, cuando se comete un hecho ilícito, existen dos sujetos, siendo estos el activo y el otro pasivo, dentro de los cuales pueden existir una o dos personas o en algunos casos más, para el efecto, a continuación, se hace referencia a cada uno de ellos, ya que, de esta manera se podrá comprender de una mejor manera.

Sujeto activo

Para cometer un delito informático, se debe considerar que, este no lo puede realizar cualquier persona, ya que, quien lo haga debe tener los conocimientos suficientes en dicha materia, así como contar con el equipo tecnológico necesario para su realización, también es esencial que el sujeto se encuentre en lugares estratégicos y por lo general que en los mismos se maneje información de carácter sensible.

En lo que respecta al sujeto activo, se debe comprender lo siguiente: “Son las personas que cometen el delito, en este caso, de índole informático. Generalmente son personas con especiales habilidades para el manejo de los sistemas informáticos y en muchos casos trabajan en lugares en los que se maneja información.” (Rivera, 2009, p. 9)

Resulta que en algunas ocasiones los delincuentes informáticos solo reaccionan ante un reto tecnológico, es decir, quizá no se tenga la intención de realizar un hecho punible, pero si el conocimiento suficiente para hacerlo, no obstante, aunque se ejecute bajo esas circunstancias, deberá asumir la responsabilidad que se le pueda deducir.

Sujeto pasivo

En cuanto a este sujeto, se debe tener presente que es la persona titular del bien jurídico, el cual como ya se hizo mención se trata de proteger a través de lo regulado en las leyes respectivas, para el caso de Guatemala, el Código Penal, en pocas palabras se está haciendo referencia a la víctima del delito sobre quien recae la conducta de acción u omisión, para lo cual estos pueden ser personas, instituciones crediticias, el gobierno, entre otros, sin embargo, se debe comprender que lo esencial del sujeto pasivo, es que éste denuncie los mismos.

Es la víctima del delito, que puede ser una persona tanto física como jurídica que utilice sistemas automatizados de información, normalmente a través de *internet*. En la mayoría de casos, no denuncia los delitos informáticos, por lo que su persecución se hace más que complicada. (Rivera, 2009, p. 9)

Para establecer la magnitud de los delitos informáticos, es esencial que el sujeto pasivo de los mismos dé a conocer la magnitud del daño ocasionado que en la mayoría de ocasiones no es así, esto debido a que los mismos o no son descubiertos o en su caso no son del conocimiento de las autoridades competentes, peor aun cuando el Estado no cuenta con las leyes específicas en la materia.

Técnicas por las cuales se cometen ilícitos a través de las redes sociales

Como se expuso anteriormente, el sujeto activo que comete los delitos informáticos, es una persona que cuenta con los conocimientos necesarios en cuanto a la informática, lo cual les permite entrar a las redes sociales, así como a los ordenadores, sin la autorización correspondiente, lo cual expone a los dueños de las redes sociales. Lo que se busca con la realización de ilícitos a través de las redes sociales, es causar un daño a las personas, en especial, porque en la actualidad, la mayoría de personas se encuentran conectados a una red social, peor aún, dan a conocer casi toda su vida, lo cual es información que toma el sujeto activo, para determinar la forma en que viven y que facilita la comisión de los ilícitos.

A criterio de la investigadora las técnicas que puede utilizar el sujeto activo de los delitos informáticos, son variadas, dentro de las cuales se encuentran el enviar imágenes o mensajes de texto con contenido sexual, mejor conocido en las redes sociales como *sexting*, el cual puede afectar en gran manera a las personas, asimismo, es importante tomar en consideración que en muchas ocasiones el propietario de la cuenta no se da cuenta de dicha acción.

Hay sujetos activos, que utilizan la técnica de la injuria y calumnias que van dirigidas hacia una persona determinada o en su caso hacia una entidad, con el simple gusto de realizar un daño, pero como hasta la presente fecha no se pueden detener las mismas, se continúa realizando daño a través de las redes sociales.

Delitos informáticos reconocidos por la Organización de Naciones Unidas

Hasta la presente fecha existen varios delitos informáticos los cuales como ya se hizo mención se diferencia por la naturaleza de los mismos, sin embargo, cada país ha legislado a su manera lo relativo a esta clase de delitos, es por ello que se hace referencia a las modalidades que se consideran:

- a) Ataques contra sistemas y datos informáticos
- b) Usurpación de la identidad
- c) Distribución de imágenes de agresiones sexuales contra menores
- d) Estafas a través de *Internet*
- e) Intrusión en servicios financieros en línea
- f) Difusión de virus
- g) *Botnets* (redes de equipos infectados controlados por usuarios remotos)
- h) *Phishing* (adquisición fraudulenta de información personal confidencial). (Loredo y Ramírez, 2013, P.45)

Para la comisión de los delitos mencionados en el inciso c) es necesario tener acceso a material ya sea violento o pornográfico, mismo que es utilizado por pederastas para así contactar a niños que se encuentren conectados a redes sociales, pues esto lo utilizan para distraer a los usuarios, causando de esta manera problemas de socialización, en especial para el sujeto pasivo, sin embargo, el sujeto activo aprovecha para realizar robos de identidad, provocando a la víctima la pérdida de intimidad, ya que, por medio de estos se busca acosar a través de las redes sociales.

La Organización de las Naciones Unidas, en el décimo Congreso sobre Prevención del Delito y Justicia, con la finalidad de minimizar la lucha contra la delincuencia en el *internet*, establece la existencia de ocho delitos

informáticos, dentro de los cuales se encuentran:

- Espionaje industrial: Los piratas pueden realizar tareas de espionaje avanzado para las empresas o para su propio provecho copiando secretos comerciales que abarcan desde información sobre técnicas o productos hasta la información sobre estrategias de comercialización:
- Sabotaje de sistemas: los ataques como el bombardeo electrónico, consisten en el envío de mensajes repetidos a una dirección o a un sitio electrónico, impidiendo así que los usuarios legítimos tengan acceso a ellos.
- Sabotaje y vandalismo de datos: Los intrusos pueden acceder a sitios electrónicos o bases de datos y borrarlos o cambiarlos, corrompiendo los datos mismos y causando perjuicios aún mayores si se usan datos incorrectos posteriormente para otros fines.
- Pesa u olfateo de claves secretas: Los delincuentes suelen engañar a los usuarios nuevos e incautos del *internet* para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio.
- Estratagemas: Los estafadores utilizan diversas técnicas para ocultar computados que se parecen electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.
- Pornografía infantil: La distribución de pornografía infantil por todo el mundo a través de la *internet*.
- Juegos de azar: Se ha incrementado a medida que el comercio brinda facilidad de crédito y transferencia de fondos en la red.
- Fraude: Ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores.
- Blanqueo de dinero: Comercio de mercancías o dinero para lavar las ganancias que deja el delito. (2013, p.3)

Se debe considerar con respecto a los fraudes cometidos mediante la manipulación de computadoras, que, dentro de estas se pueden incluir la manipulación de los datos de entrada y salida, así como de los programas, este tipo de delito se aprovecha en las transacciones financieras, en las cuales transfieren ya sea fondos de una cuenta o crean otra.

Las falsificaciones informáticas, son acciones delictivas que tienen por objeto la alteración de datos de los documentos que se encuentran almacenados de forma digital, sean estos personales o institucionales, dentro de los instrumentos empleados se encuentran las computadoras, así como las fotocopiadoras computarizadas, por medio de las cuales se pueden crear documentos falsos, los cuales no pueden ser distinguidos a no ser que sea un experto, pues la calidad de estos es casi exacta. Este tipo de acciones representan mayor riesgo para los registros público y los asuntos relacionados a seguridad del Estado.

Cabe hacer mención que dentro de los delitos reconocidos por la Organización de las Naciones Unidas se encuentran el causar daños o modificaciones de programas o datos computarizados, dentro de los cuales se encuentran el sabotaje informático, el cual se puede efectuar a través de virus, gusanos y la bomba lógica o cronológica, es por ello, que en la investigación se ha hecho mención que la persona que cometa esta clase de infracciones debe tener el suficiente conocimiento en materia informática.

Al respecto Miró Llinares, señala:

Uno de los principales riesgos que, para particulares y, muy especialmente, para empresas, conlleva el acceso al ciberespacio por medio de sistemas informáticos, es el de sufrir lo que se ha venido denominando sabotaje informático, incluyendo a su vez en él tanto los comportamientos ya conocidos y asumidos como comunes en el entorno virtual, consistentes

en el envío a través de redes telemáticas de virus informáticos que aprovechan la inmensidad de la red para multiplicarse y acceder a miles de terminales, como cualesquiera otras formas de destrucción de archivos o datos de terminales concretos y determinados, con fines industriales o de daño individual. (2012, pág. 57)

Contar con un amplio conocimiento en materia informática, conlleva una enorme responsabilidad, considerando que se puede obtener el acceso no autorizado a servicios y sistemas informáticos, circunstancia que puede afectar significativamente la vida de personas e instituciones, acciones perjudiciales que realizan los piratas informáticos o mejor conocidos como *hackers*. Asimismo, se puede realizar una reproducción automatizada de programas informáticos, derivado de lo anterior, se han dado a conocer una serie de problemas no solo nacionales sino también transnacionales.

En la actualidad ya se han acuñado una variedad de términos para tratar de identificar todas aquellas que se pueden considerar como delitos en el ciberespacio, conforme a ello, son tantos los tipos de delitos informáticos, los que se pueden cometer contra los sistemas informáticos, tales como el acceso no autorizado, así como la destrucción de datos, la infracción al copiar las bases de datos, la interceptación de correo electrónico, las estafas electrónicas, así como las transferencias dañando de esta manera al sujeto pasivo.

De manera general podría decirse que el sujeto activo que se beneficia de la comisión de los delitos informáticos son el espionaje, pues no se limita a ningún sistema, porque se ha llegado al punto de dañar a las entidades gubernamentales; el terrorismo, utiliza estos medios para dar a conocer sus proyectos delictivos; el narcotráfico, considerando que cada delincuente utiliza tales medios a su conveniencia.

A nivel internacional se han dado a conocer una variedad de instrumentos, los cuales, permite dar una idea a los países, para que estos consideren la importancia de contar con una normativa específica en materia de delitos informáticos, sin embargo, en Guatemala a pesar de tener conocimiento de los mismos, no se cuenta con la misma, lo que conlleva a que se continúe con la misma normativa, la cual no cuenta con ninguna actualización.

Redes sociales

Los seres humanos, siempre han sido seres sociales, es decir que, necesitan relacionarse con los demás, que necesitan la participación de otros para el emprendimiento de acciones, para cubrir sus necesidades, para comunicarse e interactuar, pues cada uno de estos aspectos es necesario para la construcción de la identidad de cada una de las personas, ya que desde tiempos muy antiguos estos se han agrupado para apoyarse, para

cambiar información y para cuidarse mutuamente, todo ello lo han realizado de manera personal, sin embargo:

A la llegada del siglo xxi, sin embargo, las formas de comunicación e interacción entre individuos cambiaron de manera importante. En ciertos contextos socioeconómicos y socioculturales, ya no sólo se mantiene contacto con las personas de manera directa –física, interpersonal, cara a cara–, sino también de manera virtual, con la mediación de tecnologías digitales como la telefonía móvil y la *Internet*. (Cortés Campos, Zapata González, Menéndez Domínguez, & Canto Herrera, (2015) p. 101.

Las tecnologías de información vinieron a generar grandes cambios en la sociedad, pues esto permitió que las personas se relacionaran con otras que se encontraban en distintas partes del mundo y en la medida que estas avanzan van generando bases para el surgimiento de un entorno completamente nuevo y diferente a lo que los seres humanos estaban acostumbrados, es por ello que se debe tener mayor precaución, misma que las personas no tienen y por considerar que la información que manejan se encuentra segura, se despreocupan de la existencia de sujetos que pueden indagar la misma, para causarles un daño.

Es conveniente definir en primera instancia qué significa en forma común el término redes sociales, en ese sentido, para Lozares citado por Crovi Drueta, López Cruz, & López González, indica que son “un conjunto bien definido de actores, individuos, grupos, organizaciones, comunidades, sociedades globales (...) que están vinculados unos a otros a través de una o un conjunto de relaciones sociales” (2009, pág. 41)

Básicamente redes sociales, conceptualiza la interrelación que existe entre los seres humanos en los diferentes ámbitos de la vida cotidiana. Ahora bien, al incursionar este tipo de relaciones a través del uso de la tecnología se tiene que:

Los autores Agustino y Guilaín & Monclús Ruiz, definen las redes sociales como: “aquella plataforma tecnológica que permite a sus usuarios, a través de sus correspondientes perfiles, vincularse entre sí, creando sistemas cruzados e interactivos de generación y difusión de información”. (2019|, pág. 22)

Cada una de estas tecnologías de información y comunicación hacen innecesaria pero no menos importante la presencia física de las personas al momento de la ejecución o toma de decisiones de dichos procesos, puesto que, los individuos emplean este tipo de herramientas tecnológicas, para compartir y brindar información de todo tipo, así como prestar ayuda en caso de emergencia, ofrecer asistencia legal, socializar con sus contactos, discutir sobre asuntos de interés, entre otros aspectos, que suscitan en este tipo de tecnología.

Desde la llegada de las tecnologías de información y comunicación, en la actualidad, los seres humanos viven rodeados de ella, pues el avance que esta ha tenido en el mundo es inmenso y, uno de los inventos que trajo

consigo son las redes sociales, por ello, la sociedad se encuentra inmersa en un mundo donde se entremezcla información a cada segundo de forma desordenada ya sea de consumo, trivial y nociva, sin embargo, ha sido necesario que entre tanta información que circula, poner un orden a esos elementos y convertirlos en elementos útiles para la sociedad y el mundo entero. En especial porque las nuevas generaciones se exponen a muchos riesgos a edades cada vez más tempranas.

La revolución tecnológica tiene sus orígenes:

En 1969, con la creación de *internet* por parte del Departamento de Defensa de Estados Unidos, que ha promovido el desarrollo y la masificación de nuevos aparatos tecnológicos, como computadores personales, teléfonos inteligentes y tablets, generando un intercambio global y expedito que plantea una modificación de los paradigmas de la comunicación. (Arab y Díaz, 2015, p.8)

Es evidente que luego de la creación de las herramientas tecnológicas, el uso de ellas se incrementó en la sociedad y, más aún en la información y comunicación entre los seres humanos, puesto que las personas empezaron a buscar la forma de cómo interactuar con otras que se encontraban alejadas, utilizando la tecnología y, es allí donde surgen las diferentes redes sociales, con la finalidad de que aun no estando cerca, se pueda relacionar o comunicarse a través de mensajes o por video.

Cuando las redes sociales empezaron a surgir y las personas empezaron a utilizarlas, estas fueron llamadas nativos digitales pues nacieron del marco de la sociedad, estos le llevaban una gran ventaja a los predecesores, pues estos últimos tuvieron que aprender a usarlas conforme se iban desarrollando. Para los individuos esto no tendría tanto impacto, sin embargo, en la actualidad es la forma en cómo las personas interactúan entre sí de forma rápida, creando relaciones entre individuos o empresas sin jerarquía o límites físicos, ya sea por intereses o valores comunes.

Las redes sociales poseen ciertas características que es importante hacer mención, una de ellas es que es de carácter dinámico, es decir, que su flujo continuo de intercambios combina elementos emocionales de los seres humanos, así como información de soporte social, que es de alimentos, consejos, apoyo efectivo, entre otros factores, que contienen elementos instrumentales o materiales quienes enriquecen la naturaleza dinámica de las redes sociales.

Otra de las características que se deben tomar en consideración en cuanto a las redes sociales, es que son cuantitativas, es decir:

La cantidad de miembros que la integran (tamaño), la frecuencia con que establecen contactos, el grado de simetría existente en el contacto de los miembros, el tamaño de la red, las características relacionadas con variables como el sexo, la edad, la raza, etc.. Igualmente, se distinguen características cualitativas como la amistad, el nivel de intimidad, entre otras. (Ávila, 2012, p.25)

Por esta razón, es que hoy en día las redes sociales despiertan interés personal y profesional en la sociedad, puesto que el fácil acceso a esta y la forma rápida de interacción, hacen que la comunicación en las personas sea más accesible, sin embargo, el estudio de las redes sociales no se enfoca tanto en el individuo, sino más bien en los tipos de relaciones que se mantienen entre las personas y los lazos que los unen, puesto que como se observó en el subtítulo anterior existen diferentes tipos de delitos informáticos que ponen en peligro la vida e integridad de los seres humanos, en especial a la niñez y la adolescencia que ha crecido utilizando dispositivos digitales para realizar diferentes tareas.

Por lo que, se ha considerado de interés dar a conocer aspectos de importancia sobre las redes sociales, pues es allí donde más información maneja el ser humano y, donde más se relaciona con personas de su mismo país o de otras nacionalidades, ya sea por amistad, parentesco, de trabajo, entre otros aspectos, que influyen en su vida.

Definición

Es importante comprender que significan en sí las redes sociales y, para ello, la Real Academia Española (2019), indica lo siguiente: “Plataforma digital de comunicación global que pone en contacto a gran número de usuarios.” Este contacto, al cual se hace mención es a través de

invitaciones que envían a otros individuos ya sean amigos, familiares o personas desconocidas, quienes crean su perfil, con información personal, es decir, gustos, intereses en el deporte, música, entre otros aspectos.

Claramente se puede observar que, las redes sociales guardan gran cantidad de información personal de los individuos, entre ellas se encuentran fotos, pensamientos propios y los intereses antes mencionados, pues esta es muy parecida a la relación natural que existe en los seres humanos, es decir, de forma física, con la diferencia que esta es de manera virtual, a través de las herramientas tecnológicas.

Aparte de guardar gran cantidad de información personal de los seres humanos, estas nuevas herramientas tecnológicas que han surgido en la actualidad, han venido a ofrecer una gran variedad de servicios a los individuos, entre ellos, la posibilidad de ver videos, compartir fotografías, audios, documentos, reencontrarse con familiares que habían perdido comunicación de hace décadas, facilitar la manera de comunicación entre las personas que se encuentren en diferentes lugares, pues estas han sido capaz de derribar las paredes físicas para fomentar la construcción de comunidad global.

En este mismo sentido, se define a las redes sociales como: “Una categoría de aplicaciones y servicios que facilitan la acción colectiva y la interacción social en línea con un rico intercambio de información multimedia que genera evolución del conocimiento de manera global.” (Cabero Almenara y Otros, 2016, p.4)

La definición antes citada, indica que las redes sociales también se refieren a aplicaciones que las personas utilizan para interactuar, pues es a través de estas la forma en como compartir información, videos, mensajes, música, entre otros aspectos; por lo que se deduce con base a las dos definiciones antes citadas que las redes sociales, funcionan para la interacción social, el intercambio de información entre personas, grupos e instituciones con los mismos intereses personales.

Clasificación de las redes sociales

El mundo de las redes sociales es inmenso pues existe una infinidad de aplicaciones que son dirigidas para distintas temáticas, por lo que, es necesario conocer su clasificación, para conocer más a fondo cual es la actividad de cada una de ellas, para el efecto, a continuación, se hará énfasis de forma resumida al significado de estas y de esta manera comprender el tema objeto de investigación.

Redes sociales horizontales: con respecto a este tipo de red social, se indica 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. Su función principal es la de relacionar personas a través de las herramientas que ofrecen, y todas comparten las mismas características: crear un perfil, compartir contenidos y generar listas de contactos. (Observatorio Tecnológico, 2012)

Las redes sociales horizontales, como son para cualquier tipo de usuario y tienen libre acceso y participación del individuo que desee utilizarlas, en ellas se incluye las redes sociales como *Facebook*, que fue creada para estudiantes de la Universidad de Harvard, sin embargo, en la actualidad, esta red puede ser utilizada por toda persona que tenga una cuenta de correo electrónico o incluso un número telefónico, pues también incluye *Facebook Messenger*, es decir, que se pueden enviar mensajes, fotos, videos, personalmente a través de esta aplicación, constituyen las redes sociales más utilizadas a nivel mundial.

Dentro de esta clasificación de red, también se encuentra *WhatsApp Messenger* o simplemente *WhatsApp*, que es una aplicación para teléfonos inteligentes, en donde se envían y reciben mensajes mediante *internet*, asimismo, se pueden crear grupos de personas como de la familia, compañeros de trabajo, de clase, entre otro tipo, también se pueden realizar llamadas o video llamadas, enviar fotos, videos y compartir

documentos en *pdf*, *Word*, presentaciones, entre otros, pues esto permite que sea más fácil el envío.

Otra de las redes sociales horizontales, es *Instagram*, la cual:

Es una aplicación destinada a compartir fotos y videos. Actúa como una red social y sus usuarios también pueden aplicar gran diversidad de filtros, efectos fotográficos, marcos, similitudes térmicas, colores retro, vintage, así como videos de corta duración y en directo, que posteriormente podrás compartir en diversas redes sociales como Facebook, Twitter, Tumblr o Flickr. ¿Recuperado de e-forma.kzgunea.es/mod/book/view.php?id=7767, fecha de consulta, 20 de febrero de 2020.

Esta es otra de las redes sociales, que busca interactuar con los usuarios de forma distinta, aunque también se envíen mensajes, es una aplicación en donde solo se comparten videos y fotos, con la única diferencia que el seguimiento no tiene que ser recíproco para interactuar y, como es una red social horizontal, es utilizada, por personas individuales, empresas y gobiernos, ya que no fue específica para un público en sí.

Otro tipo de redes sociales horizontales que utiliza la sociedad es *Twitter*, la cual se refiere a una aplicación que permite difundir mensajes cortos a otros usuarios, así como leer los de otras personas; *MySpace*, que incluye blogs, espacios de entretenimiento social, escuchar música y ver vídeos; *Google+*, es otra de las redes sociales horizontales que está dirigida a toda la población y al igual que las demás, en esta también se debe contar con una cuenta de correo electrónico de *Gmail*.

Redes sociales verticales: en cuanto a este tipo de redes sociales, Agustino y Guilayn & Monclús Ruiz, exponen:

En contraposición a las redes sociales horizontales se encuentran las de carácter vertical, las cuales están dirigidas a un perfil de usuario específicamente predefinido (configurándose dichas redes a fin de adaptarse a dicho perfil y sus potenciales necesidades de publicación y distribución de contenidos).

Dentro de esta categoría, podrían distinguirse los siguientes subtipos:

- i. Redes profesionales: A través de este tipo de red social los usuarios generan y comparten en su perfil información relacionada con su carrera o actividades profesionales (...)
- ii. Redes de ocio: Esta clase de red vertical pretende promover determinada manifestación de ocio (...)
- iii. Redes de difusión de conocimiento: Este tipo de red tiene por objeto permitir a sus usuarios intercambiar de forma alturista información sobre diversos temas (...) (2009, págs. 23-24)

En ese sentido, puede indicarse que, a diferencia de las horizontales estas sí están dirigidas a un grupo en específico, puesto se dividen por temáticas, por actividad y por contenido compartido, ya que de esta forma clasifican los gustos e intereses de las personas o usuarios que buscan intercambiar algo en común, como actividades, contenidos o temas en concreto, de alguna manera resultan un tanto cerrados.

Queda claro que las redes sociales verticales se clasifican por temática, se dividen en profesionales, las cuales van dirigidas como su nombre lo indica a empresarios, negocios y actividades comerciales, ya que a través de ellas se permite compartir experiencias, relacionar grupos de empresas o usuarios que estén interesados en el ámbito laboral, dentro de estas se encuentran *LinkedIn*, *Viadeo*, *ResearchGate*, entre otras.

También se encuentran las de identidad cultural, las cuales van dirigidas a aquellas personas que quieren mantener su origen; asimismo están las de aficiones, que se refieren a:

Redes sociales que están dirigidas a los amantes de alguna actividad de ocio y tiempo libre. Encontramos redes tan dispares como los pasatiempos que recogen, por ejemplo: *Bloosee*, sobre actividades y deportes en los océanos; *Ravelry*, para aficionados al punto y el ganchillo; *Athlinks*, centrada en natación y atletismo; *Dogster*, para apasionados de los perros; o *Moterus*, relacionada con las actividades y el estilo de vida de motoristas y moteros. (Observatorio Tecnológico, 2012)

Las redes sociales verticales que se clasifican por actividad, se encuentran las de juego, que como su nombre lo indica son aplicaciones en donde los usuarios se conectan de forma on-line para jugar y relacionarse con otras personas a la vez, mediante los servicios que ofrece; asimismo se encuentra las de geolocalización, que su finalidad es mostrar la posición ya sea de la persona o la localización de un objeto, por ejemplo, *maps* o *waze*.

Este tipo de red social, también se clasifica por contenido, es decir, fotos, que su finalidad, es buscar, almacenar, ordenar y compartir fotografías con los usuarios, dentro de estas se encuentra *Pinterest*, *Fotolog*, *Flickr*, entre otros; asimismo se agrupan por música, las cuales son especializadas para escuchar, clasificar y compartir música, por ejemplo, *Spotify*, *Deezer*, entre otras; por videos, en donde los sitios *web* almacenan y popularizan este contenido a través de sus usuarios, la más conocida es *YouTube*.

También se clasifican por documentos, en los cuales se puede encontrar, publicar y compartir todo tipo de archivos de manera fácil y accesible para las personas, por ejemplo, *Scribd*; asimismo, por presentaciones, lo cual significa, que son aplicaciones que les permiten a los usuarios compartir sus presentaciones profesionales, personales o académicas, entre ellas se encuentra, *Prezi*, *SlideShare*.

Como se puede observar, existe una gran cantidad de redes sociales para que las personas interactúen entre sí a través de distintas actividades, temáticas o contenido, pues cada una de estas ofrece distintos tipos de ocupaciones, para que los individuos conversen ya sea de forma instantánea o en tiempo diferido, además, que se retroalimentan por medio de las contribuciones de otros usuarios, asimismo, se debe considerar que cada día se están creando nuevas redes, las cuales de igual forma están siendo utilizadas por las personas.

Aspecto positivo de las redes sociales

Es evidente que hoy en día, las redes sociales están presentes en la vida de los seres humanos en cualquier actividad que estos realizan, pues como se observó anteriormente existe una gran cantidad de ellas, que están dirigidas a cualquier tipo de usuario, desde el aspecto individual hasta lo profesional, por lo que el impacto de las redes sociales, ha generado ciertos

aspectos positivos a la misma, por ello, se ha considerado de importancia darlos a conocer.

Para lo cual, se indica lo siguiente:

El uso controlado y supervisado de redes sociales muestra beneficios en pacientes con trauma cerebral que reciben rehabilitación, quienes desarrollan mejores estrategias compensatorias en comparación a aquellos pacientes que son rehabilitados tradicionalmente. Se ha mostrado que *internet* estimula un mayor número de regiones cerebrales, aumenta la memoria de trabajo, produce una mayor capacidad de aprendizaje perceptual y permite hacer frente a varios estímulos de manera simultánea. Los nativos digitales tienen mejor habilidad para tomar decisiones rápidas. También se ha asociado a un mayor desarrollo del polo frontal, de la región temporal anterior, del cíngulo anterior y posterior y del hipocampo. (Arab y Díaz, 2015, p.11)

De acuerdo a la cita anterior, las redes sociales han generado grandes beneficios de rehabilitación para las personas, así como a superar la timidez y a establecer lazos de amistad a través del intercambio de información que realizan, siempre y cuando se le dé el uso apropiado a este tipo de actividad tecnológica, pues como se hizo mención anteriormente, estos aspectos positivos son generados cuando su uso es controlado y supervisado, caso contrario, como ya se ha relacionado a través del contenido, los riesgos son diversos.

Es importante que todas las personas tengan conocimiento sobre el uso de las redes sociales, pues es la forma de como hoy en día se comunica la sociedad, además de ello, también funciona para generar elementos educativos, pues ya no es suficiente que los estudiantes sean buenos

utilizando libros, sino que, el buen uso de las nuevas tecnologías ha servido para optar a un apoyo en logros académicos, así como a un mejor puesto de trabajo, a generar cierta competencia técnica, tanto en los alumnos como en los docentes.

Además de ello, las redes sociales también funcionan de canales de información ya que, es el medio por el cual, las personas se enteran de las noticias del día, ya que como se hizo mención anteriormente, es de fácil acceso para la sociedad, hoy en día es más sencillo enterarse de los grandes titulares por las redes sociales que por los medios de comunicación.

Muchas personas, también utilizan las redes sociales, para cualquier tipo de negocio, ya que a través de ellas ofrecen sus productos, a través de una cuenta empresarial, en donde colocan imágenes de sus productos y al hacer clic aparece el precio, pues es como una tienda solo que *online* y, puede acceder a ella las veinticuatro horas del día, lo que facilita tanto al consumidor como al negociante, la venta del producto o servicio.

Cuando las personas utilizan de forma adecuada las redes sociales, estas son de gran apoyo para el desarrollo, aprendizaje ya que por increíble que pueda ser, pues estas también han sido de gran beneficio para la rehabilitación de niños con parálisis cerebral, distrofias musculares y trastornos de aprendizaje, ya que los distrae del dolor, de su situación actual, generando así una mejor autoestima en ellos mismos.

Aspecto negativo de las redes sociales

A pesar de que existen varios aspectos positivos del uso de las redes sociales en la sociedad, el mal uso de estas, también trae consigo elementos negativos, que es de gran importancia hacer mención, pues:

El abuso de redes sociales ha mostrado una asociación con depresión, síndrome de déficit atencional con hiperactividad, insomnio, disminución de horas total de sueño, disminución del rendimiento académico, repetición y abandono escolar. También ha sido asociado con un amplio rango de problemas psicosociales. Estudios han revelado falla en la toma de decisiones en los adictos a juegos online. Los adolescentes que juegan de forma excesiva tienen menos capacidad de procesar el feedback frente a las decisiones, no considerándolo a la hora de tomarlas. Se ha visto, además, fallas en los procesos de aprendizaje en relación al desarrollo de personalidad, se ha registrado que, a mayor gravedad de la personalidad, mayor es el riesgo de adicción. El Trastorno de Personalidad Borderline aumenta el riesgo de ciberadicción. (Arab y Díaz, 2015, p.10)

Claramente, se puede observar que el mal uso que le den las personas a las redes sociales, puede causar grandes daños a su personalidad, así como a su grupo familiar, esto debido a que se inicia por dañar la autoestima, relaciones personales físicas, a su privacidad, pérdida de tiempo, entre otros aspectos, que hacen que en varias ocasiones los individuos no se sientan a gusto con el ideal de vida que desearon y con las personas que les rodea, puesto que ha afectado en gran manera en su identidad.

Otro de los aspectos negativos de las redes sociales, es la violencia que existe, en *internet*, los videojuegos y en las distintas aplicaciones que existen, pues esto aumenta la agresividad tanto en los niños como en los

jóvenes, generando tendencia a la delincuencia, así como diferentes temperamentos en los niños; además de ello, se encuentra un alto grado de exposición deseada y no deseada de pornografía, en la que en varias ocasiones los niños y adolescentes tienen fácil acceso, sino tienen un control por parte de los padres, aspecto que en algunas ocasiones es casi imposible.

Anteriormente se hizo mención, que en las redes sociales las personas creaban cuentas con información personal, gustos e intereses, pues son datos necesarios para acceder a ellas y que a la vez los usuarios tengan información de sus contactos, sin embargo, esto también es un aspecto negativo para que personas mal intencionadas tengan conductas inadecuadas, ya que como no existe una presencia física entre los usuarios existe el anonimato, lo cual le permite a los individuos crear cuentas con identidades falsas, para engañarlas, para criticar, menospreciar y humillar, lo cual afecta el autoestima de la víctima, lamentablemente es común en la red encontrar cuentas con datos falsos.

Las redes sociales también pueden llegar a aislar a las persona, pues aunque esté interactuando con otra que se encuentra a una distancia muy lejana, se aísla de las personas que la rodean porque le presta más atención a los contactos que tiene en sus redes sociales, que a los que tiene físicamente, por lo que se considera necesario, que las personas utilicen

estas herramientas tecnológicas cuando no estén interactuando con los individuos que tiene a su lado, aspecto que no se ha logrado controlar, pues se ha visto que las personas cada vez más utilizan las redes sociales no importando si tienen amigos alrededor.

Es importante que las personas manejen de forma adecuada las redes sociales, porque como se pudo observar, existe gran peligro en el mal uso de estas, pues es necesario que genere estrategias para que estas favorezcan y no dificulten la construcción de su identidad, de sus actividades y de las relaciones físicas que puedan tener con otras personas que le rodean, ya que es preciso que también tengan comunicación de manera personal, además de resguardar su privacidad para que no sean víctimas de acoso, de *bullying*, de engaño y de exhibicionismo.

Tal como lo indican Pérez Vallejo & Pérez Ferrer:

(...) en los últimos años, la violencia protagonizada en la sociedad por menores y adolescentes en la escuela es motivo de creciente preocupación; y en ese sentido, los medios de comunicación se hacen eco a diario de noticias relacionadas con el fenómeno conocido en la extendida terminología anglosajona como *bullying*. (2015, pág. 13)

Fenómeno que lamentablemente se ha trasladado al ciberespacio, muchos hechos de acoso y violencia entre menores de edad han sido noticia a nivel mundial, el alcance que tienen las redes sociales es tan poderoso que incluso algunos niños y adolescentes han optado por quitarse la vida, debido a la intimidación, maltrato o exclusión de la que son objeto por parte de compañeros, incluso por parte de algunos educadores.

Como se pudo observar en el presente capítulo, las redes sociales son de gran importancia para las diferentes actividades que realizan los seres humanos en su vida cotidiana, pues hoy en día no existen gestiones en donde los individuos no tengan que utilizar las redes sociales, por esta razón el uso adecuado de estas, es fundamental para que no existan delitos informáticos que puedan afectar la integridad física, emocional, económica de las personas, así mismo, que puedan evitar todo tipo de pérdida en dispositivos digitales.

Análisis jurídico de los delitos informáticos cometidos en las redes sociales en Guatemala

En la investigación, se ha dado a conocer que en Guatemala desde hace varios años no se cuenta con una actualización en cuanto a los delitos informáticos, a pesar que los mismos no han sido la excepción en el país, tal y como se ha hecho mención anteriormente, en la mayoría de los casos el sujeto pasivo no denuncia los mismos, esto debido a que se desconoce de la existencia de los mismos.

En el Código Penal guatemalteco, se establecen los delitos informáticos, sin embargo, no existe un capítulo específico como tales, además de ello, se debe considerar que existen otros delitos que se encuentran en la diversidad de contenido de la normativa, dentro de estos se encuentran la

violación a los derechos de autor, violación a los derechos de propiedad industrial, el pánico financiero, el ingreso a espectáculos y distribución, producción comercialización o difusión de pornografía a menores de edad, comercialización de datos personales y alteración fraudulenta.

Es por ello que se considera esencial realizar un análisis de la normativa jurídica vigente en Guatemala, determinar la importancia de que se regule una ley específica en materia de delitos informáticos, para así brindar una mayor seguridad a los guatemaltecos, tomando en cuenta que el uso de las nuevas tecnologías son de interés para adquirir conocimientos, así como de tener comunicación no solo a nivel nacional sino también internacional.

Protección a la información personal como un derecho

La Constitución Política de la República de Guatemala, en el artículo 24 determina que la correspondencia, libros y documentos de toda persona son considerados inviolables para lo cual solo podrá revisarse en virtud de resolución judicial firme, es decir, únicamente con autorización de juez competente siempre y cuando se realice por escrito, así como debe indicarse el motivo por el cual se hará la revisión correspondiente. Asimismo, es importante señalar que se garantiza el secreto de la correspondencia así como las comunicaciones telefónicas y todo lo que se relaciona con la tecnología moderna y en ese sentido se deberá tener orden

judicial, y es importante señalar que toda información obtenida con violación con las disposiciones antes mencionadas, no producen fe ni hacen prueba en juicio lo cual pone de manifiesto que constituye una violación a los derechos individuales que el Estado de Guatemala reconoce a todo habitante.

En Guatemala, la normativa fundamental es la Constitución Política de la República y es en ella en donde se establecen los derechos de la población, mismos que deben ser cumplidos y respetados a cabalidad por las entidades tanto estatales como del sector privado, se presenta el derecho a la privacidad de información personal, en la cual se incluye los documentos y su contenido, además, debe tenerse presente que la misma tiene aproximadamente treinta y cinco años de vigencia, y en ella se contempla lo relativo a las nuevas tecnologías.

El legislador, consideró los avances que iban a existir en cuanto a la tecnología y fue por ello que se estableció como derecho la inviolabilidad de la información de las personas, sin embargo, este es un aspecto que hasta la presente fecha aún no se ha contemplado a profundidad, pues a pesar de la existencia de delitos informáticos, se tiene muy poco conocimiento de la gravedad de los mismos. Es por ello esencial determinar que la intimidad de las personas es un derecho que debe cumplirse y respetarse, tal y como establece la normativa constitucional,

nadie puede ser objeto de interferencias en su vida privada, su familia, su domicilio o en su correspondencia no importando si esta es física o digital.

Dentro del marco jurídico constitucional, específicamente en el artículo 35 se hace referencia a la libertad de emisión del pensamiento de la manera siguiente:

Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por ley o disposición gubernamental alguna. Quien en uso de esta libertad faltare al respeto de la vida privada o a la moral, será responsable conforme a la ley. Quienes se creyeren ofendidos tienen derecho a la publicación de sus defensas, aclaraciones y rectificaciones.

En respeto a los derechos humanos de las personas, se debe tomar en cuenta que la privacidad de los seres humanos ha sido afectada, especialmente en la era digital, por la enorme circulación y almacenamiento de datos personales que existe en las diferentes plataformas, la cual ha conllevado a problemas en los cuales también se afecta a la familia, el domicilio y la correspondencia, se vulnera la honra y reputación a través de las redes sociales.

En Guatemala, hasta la presente fecha no se ha puesto la atención debida a cuestiones tales como la promoción y protección del derecho a la privacidad en la era digital, así como el establecimiento de garantías procesales, la supervisión y los recursos nacionales defectivos, para que estos puedan vigilar la privacidad como derecho humano de los

guatemaltecos, tampoco se han examinado los principios de no arbitrariedad y legalidad.

En Guatemala a pesar que el Código Penal regula algunos delitos informáticos, no los contempla todos, dentro de ellos los relativos a las redes sociales, aspecto que conlleva a que el Estado vulnera el derecho a la privacidad establecido en el artículo 12 que se encuentra contenido en la Declaración Universal de los Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

Los últimos gobiernos de turno, no han realizado un estudio efectivo, en la forma en que se está dañando a la población guatemalteca, y es efectivamente, en la vulneración a su derecho a la privacidad, pues a través de las redes sociales, los delincuentes han optado por amenazar, extorsionar, robar, causar daños a la moral entre otros aspectos, de los cuales en la actualidad no se tiene un procedimiento por medio del cual se establezca el respeto a la privacidad.

El derecho a la privacidad de la información personal, debe basarse en las garantías establecidas en la Constitución Política de la República, así como en las leyes específicas y en las normas de carácter internacional; la inexistencia de estas o el irrespeto abre el camino a indiscreciones indebidas en los derechos humanos de las personas, a través de la

normativa se debe contribuir al libre desarrollo de la personalidad y que a la vez el uso de las nuevas tecnologías no afecte el disfrute de los derechos de los individuos.

Delitos en las redes sociales

Como se ha observado a lo largo de la investigación realizada, las redes sociales en la actualidad han constituido el nuevo ámbito de desarrollo personal de los seres humanos, pues es en este espacio virtual, en donde los individuos pasan varias horas del día en comunicación con otros, creando nuevas relaciones personales o manteniendo las ya existentes.

Sin embargo, no todo lo que se realiza en las redes sociales es positivo, puesto que existen personas mal intencionadas que utilizan este medio tecnológico, para atacar el patrimonio, el honor, la libertad, la indemnidad sexual, la intimidad y la dignidad de los seres humanos, por lo que se ha considerado de interés dar a conocer algunos delitos que se cometen en las redes sociales y en qué consisten, pues en varias ocasiones los individuos no se dan cuenta de que son víctimas de delitos informáticos, en ese sentido, se hace referencia a los siguientes:

Grooming

Este tipo de delito en las redes sociales, se define como:

El acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor, incluyéndose en este desde el contacto físico hasta las relaciones virtuales y la obtención de pornografía infantil. (Instituto Nacional de Tecnologías de la Comunicación, p.5)

El sujeto pasivo de este tipo de delitos, son básicamente los niños, niñas y adolescentes, pues como se indicó anteriormente, su fin primordial es tener el control sobre la víctima para abusar de ella sexualmente. La forma más común que se ha utilizado en los últimos tiempos, es que el delincuente se hace pasar por otro niño, niña o adolescente, para ganarse su confianza y, de esta manera obtener los datos que necesita, por ejemplo, en donde vive, que hacen sus padres, en donde estudia, a qué hora sale, que realiza en sus tiempos libres, incluso si tiene novio o novia, para poder llevar a cabo el delito, en fin, el delincuente analiza y sigue los pasos de su víctima durante un período prolongado de tiempo, hasta lograr su objetivo.

Luego que ya tenga estos datos, el agresor empieza a engañar a la víctima, a través del enamoramiento, pues empieza a enamorarla y a decirle que está enamorado de él o de ella, cuando la persona cae en su juego, el delincuente consigue que esto generalmente a través de la *webcam* se desnude y, que realice actos sexuales.

Cuando ya ha sucedido todo ello, entonces comienza el chantaje, el cual consiste en que el abusador manipula a la víctima con que hará público todos los videos que esta le envió, por lo que ocasiona que esta se deprima, que su autoestima esté baja, que exista temor y desconfianza todo el tiempo y a la vez, provoca cambios de humor repentinos en las personas, pues su estado de ánimo está mal y, en varias ocasiones los influye al suicidio.

Sexting

En cuanto al *sexting*, es otro delito que ha empezado a utilizar por los delincuentes, debido a que se ha convertido en un atractivo, tanto para personas adultas como para niños, ello debido a que no existe un control legislativo, para el efecto, se hace referencia a lo siguiente:

Una práctica que consiste en compartir imágenes de tipo sexual, personal o de otros, por medio de teléfonos o *internet*. El riesgo, es que las imágenes sean publicadas y viralizadas sin permiso. Con ello la intimidad queda expuesta a la mirada pública, con todas las consecuencias a corto y largo plazo de este hecho. (Arab, 2015, p.10)

De acuerdo a lo antes citado, el *sexting* es casi parecido al *grooming*, con la única diferencia que, en este, se envían fotos y videos a personas con las cuales ya tienen confianza, pero estas son publicadas en las diferentes redes sociales con el consentimiento del protagonista y, aunque no se vea como un delito en sí, porque tiene el permiso del individuo, se está violando su privacidad.

Este tipo de delito, al igual que el *grooming*, más que todo afecta a los niños, niñas y adolescentes, es decir que es un grupo demasiado vulnerable ante los criminales cibernéticos, quienes a través de las redes sociales y los aparatos tecnológicos llevan a cabo este tipo de acciones, no midiendo el peligro que puede ocasionar en la vida de seres inocentes, hay que considerar que el daño no queda solo en ellos, también afecta a todos los miembros de las familias de las víctimas.

Cyberbullying

El *cyberbullying*, como delito en las redes sociales, consiste en:

Una agresión repetitiva de uno o más individuos en contra de una persona, utilizando dispositivos o servicios de tecnología. Hay elementos que diferencian al *cyberbullying* del *bullying* tradicional o “cara a cara”, la principal es el uso de la tecnología, lo cual cambia el impacto de esta conducta sobre la víctima. Hay medidas tecnológicas y políticas para los servicios en *Internet*, pero la forma más efectiva para contrarrestar el *cyberbullying* es evitando que ocurra, a través de la concientización y la educación en el tema, particularmente entre niños y adolescentes. (Aquino Luna, 2014, p.3)

Como se puede observar en la cita anterior, este tipo de delito informático es violencia que se causa a la integridad y honor de la persona, afectando así su estado emocional a través, de comentarios, publicaciones, videos, datos privados o cualquier tipo de información que las personas utilizan para avergonzar a otra, pues aunque no se haga de forma física o personal, se le está dañando el autoestima a los individuos, haciendo que este entre en pánico, desesperación, inestabilidad e incluso, influyendo al suicidio.

Robo de identidad

El robo de identidad en las redes sociales se define de la siguiente manera: “El término se referirá a todos los datos personales de alguien, cuando se utilizan por otra persona, y esto le permite actuar como la víctima con el fin de cometer delitos.” (Rua, 2015, p.19). Entonces de acuerdo a lo antes citado, el robo de identidad, es cuando los individuos utilizan los datos personales de otra sin su consentimiento para hacerse pasar por él o ella, y así cometer delitos y fraudes a través de las redes sociales.

Para llevar a cabo este delito, los delincuentes generalmente realizan tres procesos, el primero es la etapa de obtención de la información personal, el segundo es la posesión o transferencia de información y el tercero es la utilización de los datos ya obtenidos para cometer los delitos o fraudes, pero, ¿Cómo es que obtienen los datos personales?, esta información la consiguen a través de engaños, en donde hacen que la persona revele su contraseña, accediendo de esta forma a sus redes sociales.

Asimismo, se hacen pasar por encuestadores de empresas o negocios, ofreciendo todo tipo de ofertas, ya sea por medio de llamadas telefónicas o envían mensajes de correos electrónicos, pidiendo información ya sea de su tarjeta de débito o crédito, así como su nombre, dirección y fecha de nacimiento, adquiriendo así toda la información que necesitan, para llevar a cabo su objetivo.

Existen diferentes formas de robo de identidad, por lo que es necesario que en Guatemala exista una ley que penalice este tipo de delitos cibernéticos, pues al igual que los demás, causan serios daños a la integridad y honor de la persona, dejándola en un mal estado emocional y económico.

Aporte del derecho comparado sobre los delitos informáticos en redes sociales

A nivel internacional, son varios los países que ya han puesto la atención debida a la delincuencia que se realiza a través de las redes sociales, debido a ello han creado leyes por medio de las cuales buscan proteger a la población en especial cuando se vulnera el derecho a la privacidad, aspecto, que como ya se hizo mención se encuentra regulado en diversos instrumentos internacionales.

Barrio Andrés, expone:

(...) las diversas manifestaciones de conductas delictivas vinculadas a las tecnologías cibernéticas, cuyo rasgo definitorio y difirenciador es el de realizarse en otro espacio distinto a aquél en el que siempre se habían ejecutado las infracciones penales, han planteado retos y desafíos jurídicos, frente a los cuales ya se han promulgado respuestas normativas, de ámbito estatal, comunitario e internacional. (2017, págs. 15-16)

En efecto, como lo indica el autor, existen ya algunos referentes en cuanto a la regulación de los delitos informáticos, claro, la construcción de las normas jurídicas no ha sido tarea sencilla, debido a la especialidad que requiere su tratamiento, además de aspectos como la complejidad para

establecer el lugar en que se comete el delito debido a la transnacionalidad de las redes telemáticas, a continuación, se hará reseña de algunas de los cuerpos normativos que se han creado en el derecho comparado.

Los delitos informáticos en España

El Código Penal de España, referente a Delitos Informáticos, contenidos en la Ley-Orgánica, 10/1995, tiene varios artículos en los cuales se hace referencia a estos delitos, para el efecto, en el artículo 197 se hace referencia a la protección de los secretos o vulnerar la intimidad de otro o en su caso a quien se apodere, utilice o modifique en perjuicio de otra persona datos de carácter personal que se encuentren registrados en ficheros o soportes informáticos.

En el artículo 264 de la ley española, se establece pena y multa a quien “destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.” Y así existen otros artículos en los cuales se busca la protección de los datos personales de las personas.

Según la información contenida en la página web alojada en la dirección electrónica https://delitosinformaticos.info/delitos_informaticos/legislación.html

En España a pesar de no existir una normativa específica, en materia de delitos informáticos, se cuenta con una Ley orgánica de Protección de Datos de Carácter personal, así como con una Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de Carácter Personal, una Ley de Telecomunicaciones, Ley de Propiedad Intelectual y una Ley de Firma Electrónica.

Recuperado de: https://www.delitosinformaticos.info/delitos_informaticos/legislacion.html, fecha de consulta 16 de marzo de 2020.

Los delitos informáticos en Argentina

El Código Penal de la Nación Argentina, se encuentra contenido en la Ley número 11.179 del Senado de la Nación, ha tenido algunas reformas dentro de su contenido, dentro de las cuales se encuentra lo relativo a los delitos informáticos, mismo que se realizó a través de la Ley 388, la cual como se indicó no es una ley especial, sino más bien es un cuerpo normativo en el cual se establecieron figuras específicas con el objeto de regular las nuevas tecnologías como los medios de comisión de delitos, dentro de los cuales se incluye la distribución y tenencia con fines de distribución de pornografía infantil, la violación de correos electrónicos, el acceso ilegítimo a sistemas informáticos, el daño informático y distribución de códigos maliciosos así como la interrupción de comunicaciones.

Asimismo, se incluyó otra reforma a través de la Ley 26.904 relativa al *Grooming*, la normativa en mención impone una pena de prisión de seis meses a cuatro años a quien “por medio de comunicaciones electrónicas,

telecomunicaciones o cualquier otra tecnología de transmisión de datos contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.” Es decir, al Código Penal de Argentina, se han agregado hasta la presente fecha catorce delitos en materia informática, con la finalidad de brindar una mayor protección a su población.

En Argentina, también se cuenta con una ley específica en materia de protección de datos personales, misma que se caracteriza por definir cuáles son los principios en materia de protección de datos, los cuales abarcan desde, los derechos de los titulares, así como los responsables de archivos, registros y bancos de datos, también se hace mención a la existencia de un control, sanciones, la acción de protección que tiene el Estado en cuanto a los datos personales e inclusive el *spam* están vinculados a la ley en mención.

Los delitos informáticos en México

Se debe tomar en consideración que México es un país, que cuenta con varios Estados, es por ello que se hará mención de forma general a las normativas existentes en cuanto a las leyes que contiene lo relativo a los delitos informáticos como lo establece el Código Penal de México.

- Comercio electrónico
 - Firma electrónica
 - Protección de datos personales
 - Derecho a la información
 - Gobierno digital
 - Ataques a las vías de comunicación y violación de correspondencia
 - Revelación de secretos
 - Acceso ilícito a sistemas y equipos de informática
 - Acceso a las carpetas digitales
 - Utilización de medios electrónicos
 - Derechos de autor
 - Propiedad Industrial
 - Mercado de valores
 - Telecomunicaciones
 - Valor probatorio de documentos electrónicos en legislación diversa.
- Recuperado de: www.informatica-juridica.com/legislacion/mexico/
fecha de consulta: 25 de marzo de 2020.

Conforme al texto anterior, se puede inferir que existe suficiente regulación para prevenir lo relativo a los delitos informáticos en el país vecino y en el Código Penal de cada Estado, además de lo anterior, también se han tipificado delitos tales como la producción, impresión, enajenación, distribución de documentos de crédito; así como falsificación

de documentos, falsificación de medios electrónicos o magnéticos, revelación de secretos, acceso ilícito a equipos y sistemas informáticos y los derechos contra los derechos de autor, también se encuentra la alteración de medios de identificación electrónica, la sustracción, uso y revelación de información electrónica confidencial, la defraudación, así como el descifrar una señal de satélite cifrada, en tal virtud, México ha logrado avances significativos en el tratamiento de los delitos informáticos.

Los delitos informáticos en Costa Rica

Para el caso de Centroamérica, Costa Rica, es uno de los países que ha considerado la regulación de los delitos informáticos, sin embargo, esto no se hizo por medio de una ley específica, pues el Código Penal, Ley Número 4573, ha sido reformado, particularmente la sección VIII llamada Delitos Informáticos, a través del Decreto Legislativo, Ley Número 9048, para lo cual se incluyeron entre la tipificación de delitos, tales como corrupción, el cual se refiere a la exhibición erótica, pornográfica de los menores de edad, utilizando las redes sociales o cualquier otro medio informático o telemático.

Asimismo, se incluyeron delitos como, violación de correspondencia o comunicaciones, que se refiere al daño de la intimidad o privacidad de otras personas; violación de datos personales, el cual significa apoderarse, modificar, interferir, acceder, copiar, transmitir, publicar, difundir y utilizar datos personales en beneficio propio, a través de redes informáticas o telemáticas, sin autorización del titular.

Otro de los delitos que se regularon, fue la extorsión, la estafa informática y daño informático, los cuales se refieren a dañar, utilizar, modificar, manipular, datos del titular, para beneficio propio o de terceros utilizando la información contenida en sistemas y redes informáticas o telemáticas, así como aparatos electrónicos; asimismo la ley en mención incluyó el delito al daño agravado y sabotaje informático, que establecen aspectos relacionados con las bases de datos de las redes, sistemas y equipos informáticos, telemáticos y electrónicos, en donde alteran, obstaculizan y modifican el funcionamiento de las partes o componentes de estos.

El derecho comparado es de gran importancia, ya que, por medio de este, se puede comprobar que son varios los países que ya cuentan con una normativa específica en materia de protección a la información personal, a excepción de Costa Rica, que como se pudo constatar, este incluyó tal protección en el Código Penal a través de una reforma.

Asimismo, en los distintos Códigos Penales citados, se han realizado reformas en cuanto a las redes sociales, cuestión que no ha sucedido en Guatemala, pues la única reforma que se tuvo en la normativa penal guatemalteca en materia de delitos informáticos fue hace veinticuatro años aproximadamente, y solamente fue con respecto a unas ampliaciones a los mismos artículos, en ningún momento se han considerado otros delitos.

La necesidad de legislar una ley penal que prevenga y sancione este tipo de ilícitos cometidos a través del uso de *internet* en especial las redes sociales

En Guatemala hasta la presente fecha se carece de una normativa específica en materia de protección de datos, sin embargo, se debe tomar en cuenta que en el año 2009 se presentó la iniciativa número 4090 ante el Congreso de la República de Guatemala, la cual contenía la Ley de Protección de Datos Personales, misma que solamente posee dictamen favorable emitido por la comisión de Economía y Comercio Exterior, pero aún tiene pendiente el tercer debate y la aprobación por el pleno del Congreso, acción que lleva detenida ya casi diez años.

La iniciativa de ley en mención, hace referencia varios factores, uno de ellos es en el artículo 1, objeto y fin:

La presente Ley tiene como objetivo garantizar a cualquier persona física o jurídica, sean cuales fueren su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la persona; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondiente a su persona o bienes. En ningún caso se podrá afectar el secreto de las fuentes de información periodística y el secreto profesional que determinen las leyes correspondientes.

La ley en mención también hace referencia a que, en el ámbito de aplicación de la misma, se deben incluir los archivos automatizados, así como los archivos mantenidos por personas físicas, los archivos de información tecnológica o comercial, los que se encuentren en informática jurídica.

En la iniciativa de Ley de la Protección de Datos Personales, también se incluye en el artículo 11 lo relativo a los derechos y garantías de las personas, para el efecto, se regula que debe haber una demora razonable cuando alguien solicite datos propios; la misma debe ser suministrada de forma clara así como ser amplia y versar sobre la totalidad del registro que pertenece al titular, dicha información puede ser proporcionada en forma escrita o en su caso por medios electrónicos, también se podrán actualizar los datos o en su caso eliminar los mismos.

En la iniciativa de ley se hace mención a las transferencias de datos personales, así como a la creación de una dirección para la protección de datos personales, para lo cual se establece la conformación de la misma,

así como lo relativo a la estructura interna, se regula a la vez los procedimientos a seguir al momento de existir intervención en archivos y bases de datos, el régimen disciplinario aplicable a los archivos y bases de datos, se dan a conocer las consecuencias, al momento de cometer faltas leves, graves y gravísimas, así como los pasos que se deben seguir de forma interna.

La iniciativa de ley se encuentra completa, sin embargo, se considera esencial, que al ya existir una ley en la misma se debería realizar una unificación de delitos, considerando que dentro del contenido de dicha iniciativa no existe lo relativo a los delitos informáticos, de los cuales no solamente se deberían agregar los regulados en el Código Penal sino también agregar los que se puedan cometer en las redes sociales.

En otros países, la existencia de una normativa jurídica específica ha sido esencial, en especial porque se da la protección debida a los datos de las personas, esto debido a que se han realizado los estudios necesarios para determinar que las redes sociales, no solo son de ayuda para el ser humano, pero esto dependerá del uso que se les quiera dar.

El legislador guatemalteco, debe realizar un análisis sobre la clase de delitos que se cometen en contra de la población guatemalteca y dentro de ellos incluir las redes sociales, las cuales también deben ser objeto de

protección, pues estas se encuentran abiertas a todas aquellas personas que las puedan utilizar ya sea para bien o para causar un daño, derivado de ello es que los delincuentes desde hace ya algún tiempo utilizan estos para manipular, así como afectar los derechos de los usuarios y debido al desconocimiento existente, en cuanto a la inexistencia de una ley específica, no se ha logrado proteger a la población de este tipo de violación.

Conclusiones

En Guatemala a los delitos informáticos, no se les ha dado la atención debida como lo han hecho otros países, puesto que aún no se cuenta con una ley especial que encuadre la conducta delictiva de aquellas personas que abusando de las herramientas tecnológicas, buscan como invadir la privacidad y seguridad de las personas y esto se da en cualquiera de los ámbitos, puede ser a nivel empresarial, académico, laboral, inclusive las personas menores de edad que son uno de los grupos más vulnerables.

Las redes sociales son esenciales para las diferentes actividades que realizan los seres humanos, utilizando desde un computador hasta un celular inteligente, por lo que el uso y el abuso que se le dé a este tipo de tecnología de información y comunicación, generará impactos positivos y negativos en el desarrollo cognitivo, afectivo, social y de identidad de las personas, por ello, es importante que los individuos se eduquen, modulen y controlen el acceso de estas herramientas para generar un impacto positivo tanto en su vida personal como en la sociedad.

El Estado de Guatemala a diferencia de otros países, no se tiene protegida a la población en el sentido de delitos informáticos, en especial aquellos que se realizan a través de las redes sociales, esto debido a que el Congreso de la República hasta la presente fecha no ha aprobado la Ley de

Protección de Datos Personales, la cual sería indispensable para ello, pues en la misma se podrían unificar otros derechos de conformidad con lo establecidos por la Organización de las Naciones Unidas.

Referencias

Agustino y Guilayn, A., & Monclús Ruiz, J. (2019). *Aspectos legales de las Redes Sociales*. España: Wolters Kluwer España, S.A.

Aquino, R. (2014). *Cyberbullying: acoso utilizando medios electrónicos*. Revista digital universitaria.

Arab, E. y Díaz A. (2015). *Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos*. Revista Médica Clínica Las Condes.

Ávila, J. H. (2012) *Redes Sociales y análisis de redes. Aplicaciones en el contexto comunitario y virtual*. Barranquilla, Colombia: Corporación Universitaria Reformada.

Barrio Andrés, M. (2017). *Ciberdelitos Amenazas criminales del ciberespacio*. Madrid: Editorial Reus, S.A.

Barrio Andrés, M. (2018). *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos*. España: Wolters Kluwer España, S.A.

Barrios, Osorio, O.R. (2006). *Derecho e informática*. Guatemala: Editorial Mayte.

Barrios Osorio, O. R. (2010). *Introducción de las Nuevas Tecnologías en el Derecho*. Guatemala: Instituto de la Defensa Pública Penal.

Cabero J., Barroso, J., Llorente, M. del C., y Cabrera, C. Y. (2016). *Redes sociales y Tecnologías de la Información y la Comunicación en Educación: aprendizaje colaborativo, diferencias de género, edad y preferencias*. *Revista de Educación a Distancia*.

Cortés Campos, R. L., Zapata González, A., Menéndez Domínguez, V. H., & Canto Herrera, P. J. (2015). *El estudio de los hábitos de conexión en redes sociales virtuales, por medio de la minería de datos*. México: Instituto Politécnico Nacional.

Crovi Drueta, D. M., López Cruz, M., & López González, R. (2009). *Redes Sociales, Análisis y aplicaciones*. México: Plaza y Valdés, S.A. de C.V.

de Mata Vela, J. F., & de León Velasco, H. A. (2016). *Derecho Penal Guatemalteco* (Vigésima sexta ed.). Guatemala: Magna Terra Editores.

Flores Salgado, L. (2014). *Derecho Informático*. México: Grupo Editorial Patria.

Galán Muñoz, A. (2019). *Los Ciberdelitos en el ordenamiento Español*.
Barcelona: Editorial UOC.

González, E. (2009). *Apuntes de derecho penal guatemalteco*. Guatemala:
Fundación Mirna Mack.

Gómez de la Torre, I. B., Arroyo Zapatero, L., Ferré Olivé, J., García
Rivas, N., Terradillos Basoco, J., Acale Sánchez, M., . . . Serrano
Piedecasas, J. R. (2016). *Curso de Derecho Penal, Parte General*.
Barcelona: Ediciones Experiencia, S.L.

Hernández, L. (2009). *El delito informático*. España: Editorial Eguzkilore.

Instituto Nacional de Tecnologías de la Comunicación. (2013). *Guía S.O.S
contra el Grooming. Padres y educadores*. España: Instituto Nacional
de Tecnologías de la Comunicación.

Landa Durán, G. (2007). *Los delitos informáticos en el derecho penal de
México y España*. España: Universidad de Castilla- La Mancha.

Loredo González, J. y A. Ramírez Granados. (2013). *Delitos
informáticos: su clasificación y una visión general de las medidas de
acción para combatirlo*. México: Universidad Autónoma de Nuevo
León.

Marco Galindo, M. J., Marco Simó, J. M., Prieto Blázquez, J., & Segret Sala, R. (2010). *Escaneando la Informática*. Barcelona: Editorial UOC.

Miró Llinares, F. (2012). *El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, S.A.

Noriega Salazar, H. A. (2011). *Delitos Informáticos*. Guatemala: Instituto de la Defensa Pública Penal.

Organización de las Naciones Unidas. (2010). *Xº. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia penal*. Salvador: Departamento de Información Pública de las Naciones Unidas.

Pérez Vallejo, A. M., & Pérez Ferrer, F. (2015). *Bullying, Cyberbullying y acoso con elementos sexuales: desde la prevención a la reparación del daño*. Madrid: DIKINSON, S.L.

Rivera Panizo, S. *Los delitos informáticos*. (2009). España: Universidad de Santiago de Compostela.

Raya Cabrera, J. L., Raya González, L., & S. Zurdo, J. (2014). *Sistemas Informáticos*. Madrid: RA-MA Editorial.

Rua, E. (2015). *Guía de buenas prácticas – Internet – Robo de Identidad*. Portugal: APAV.

Santos González, M. (2015). *Diseño de Redes Telemáticas*. Madrid: RA-MA, S.A. Editorial y Publicaciones.

Suarez. R. (2009). *Los delitos informáticos*. España: Universidad de Santiago de Compostela.

Zambrano Pasquel, A. (2019). *Derecho Penal, Parte General* (Vol. Tomo I). Quito: Corporación de Estudios y Publicaciones.

Materiales Legales

Asamblea Nacional Constituyente. (1985). *Constitución Política de la República de Guatemala*. 31 de mayo de 1985. Guatemala.

Congreso de la República de Guatemala. (1973). *Decreto Número 17-73. Código Penal*. 15 de septiembre de 1973. Guatemala.

Decreto Legislativo, Ley Número 9048. Asamblea Legislativa de la República de Costa Rica, 2012.

Código Penal de España, referente a Delitos Informáticos, contenidos en la Ley-Orgánica, (10/1995).

Código Penal de la Nación Argentina, se encuentra contenido en la Ley número 11.179 del Senado de la Nación.

Artículos obtenidos de internet

Clasificación de redes sociales. (2020, 01 de febrero). *Observatorio tecnológico. Gobierno de España.* Recuperado de <http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redes-sociales?start=3>.

Instagram. (2020, 07 de febrero). *Departamento de Desarrollo Económico y Competitivo. Gobierno de Vasco. Eusko Jaurlaritza.* Recuperado de http://e-forma.kzgunea.eus/pluginfile.php/13051/block_html/content/INSTAGRAM.pdf

Red Social. (2020, 01 de febrero). *Real Academia Española*. Recuperado de <https://dle.rae.es/?w=red>

https://www.delitosinformaticos.info/delitos_informaticos/legislacion.html, fecha de consulta 16 de marzo de 2020.

www.informatica-juridica.com/legislacion/mexico/ fecha de consulta: 25 de marzo de 2020.