UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

REDES SOCIALES Y PLATAFORMAS DIGITALES COMO MEDIOS PARA LA COMISIÓN DE DELITOS Y SU FALTA DE TIPICIDAD EN EL SISTEMA JURÍDICO PENAL EN GUATEMALA

JORGE CARLOS ENRIQUEZ SOFIANOS

GUATEMALA, JUNIO DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

REDES SOCIALES Y PLATAFORMAS DIGITALES COMO MEDIOS PARA LA COMISIÓN DE DELITOS Y SU FALTA DE TIPICIDAD EN EL SISTEMA JURÍDICO PENAL EN GUATEMALA

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

JORGE CARLOS ENRIQUEZ SOFIANOS

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, junio de 2019

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic.	Gustavo Bonilla
VOCAL I:	Lic.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Henry Manuel Arriaga Contreras
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Denis Ernesto Velàsquez Gonzales
VOCAL V:	Br.	Abidán Carías Palencia
SECRETARIO:	Lic.	Fernando Antonio Chacón Urízar

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic.	José Miguel Cermeño Castillo
Vocal:	Licda.	María Lesbia Leal Chávez
Secretaria:	Licda.	Gloria Isabel Lima

Segunda Fase:

Presidente:	Lic.	Eddy Augusto Aguilar Muñoz
Vocal:	Lic.	Freddy Amílcar Díaz Ovalle
Secretaria:	Licda.	Cristina Elizabeth Gómez Medrano de Arenas

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis". (Artículo 43 del Normativo para Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C. A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 19 de julio de 2018.

Atentamente pase al (a) Profesional, **JOSE EDUARDO MORFIN CRUZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **JORGE CARLOS ENRIQUEZ SOFIANOS**, con carné **200817627**, intitulado **REDES SOCIALES Y PLATAFORMAS DIGITALES COMO MEDIOS PARA LA COMISIÓN DE DELITOS Y SU FALTA DE TIPICIDAD EN EL SISTEMA JURÍDICO PENAL EN GUATEMALA.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

LIC. ROBERTO FREDY ORELLANA MARTÍNEZ
Jefe(a) de la Unidad de Asesoría de Tesis

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

Fecha de recepción 31 / 7 / 2018.

Asesor(a)
Jose Eduardo Morfin Cruz
ABOGADO Y NOTARIO

LEGALIS, S.A.
Corporación de Abogados

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

Guatemala, 03 de agosto de 2018

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
17 AGO. 2018
UNIDAD DE ASESORIA DE TESIS
Hora: 15:14
Firma:

Lic. Roberto Fredy Orellana Martínez
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su despacho

Estimado Licenciado Orellana Martínez:

Tengo el agrado de dirigirme a usted con el objeto de manifestarle que en el cumplimiento a la resolución de la unidad de Asesoría de Tesis, asesoré el trabajo de tesis presentado por el bachiller, **JORGE CARLOS ENRÍQUEZ SOFIANOS**, quien elaboró el trabajo de tesis intitulado: **REDES SOCIALES Y PLATAFORMAS DIGITALES COMO MEDIOS PARA LA COMISIÓN DE DELITOS Y SU FALTA DE TIPICIDAD EN EL SISTEMA JURÍDICO PENAL EN GUATEMALA** y quien se identifica con el carné estudiantil 200817627, habiendo asesorado el trabajo encomendado, me complace hacer de su conocimiento que:

1. Contiene un amplio contenido jurídico del derecho penal, donde se comprueba la necesidad de la creación de una ley penal específica en materia de delitos informáticos cometidos a través de las redes sociales.

2. El procedimiento para la elaboración de la investigación incluyó los siguientes métodos de investigación: el análisis, la inducción, la deducción, y la síntesis ya que estableció los fundamentos legales por los cuales se demuestra el conocimiento en derecho penal y la teoría formal del delito.

3. La relación empleada en el desarrollo de la tesis cumple con los requisitos necesarios, además de que la misma contribuye científicamente al estudio del derecho penal en Guatemala, recolectando información actualizada y suficiente, relacionado con el tema investigado.

4. La bibliografía utilizada es la adecuada, siendo la conclusión discursiva de manera acertada con el contenido de los capítulos de la tesis, en el desarrollo del trabajo de investigación le indique al bachiller Jorge Carlos Enríquez Sofianos diversas modificaciones a la introducción, índice, capítulos y citas bibliográficas acorde al tema, al considerar que eran necesarias y el sustentante estuvo conforme en su realización.

4° avenida A 21-43 5to nivel zona 14
Guatemala, Guatemala
Teléfonos: 23665565-22589681

5. El informe final de tesis es de gran contribución científica para la sociedad y para la legislación guatemalteca. Material que puede servir como de consulta para futuras investigaciones.

6. Personalmente me encargue de orientar al bachiller Jorge Carlos Enríquez Sofianos durante las etapas correspondientes al proceso de investigación científico, doctrinario, haciendo uso de la metodología correcta la cual comprueba la hipótesis relacionada.

La tesis cumple con todos los requisitos legales del Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, haciendo saber al bachiller Jorge Carlos Enríquez Sofianos, que no formamos parentesco dentro de los grados de ley, motivo por el cual emito **DICTAMEN FAVORABLE**, para que pueda continuar con el trámite respectivo para evaluarse posteriormente por el tribunal examinador en el examen público de tesis; previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Atentamente,

Jose Eduardo Morfin Cruz
ABOGADO Y NOTARIO

Lic. José Eduardo Morfín Cruz
Abogado y Notario
Asesor de Tesis
Colegiado No. 2602

Guatemala, CA.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Universidad de San Carlos de Guatemala
Unidad de Asesoría de Tesis
Lic. Roberto Fredy Orellana Martínez
JEFE
Facultad de Ciencias Jurídicas y Sociales

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 15 de marzo de 2019.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JORGE CARLOS ENRIQUEZ SOFIANOS, titulado REDES SOCIALES Y PLATAFORMAS DIGITALES COMO MEDIOS PARA LA COMISIÓN DE DELITOS Y SU FALTA DE TIPICIDAD EN EL SISTEMA JURÍDICO PENAL EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIO
GUATEMALA, C. A.

RFOM/JP.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
GUATEMALA, C. A.

DEDICATORIA

A DIOS: Por darme vida y porque de Él son todas las cosas, las cuales nosotros administramos.

A MI MADRE: Marta Lidia Sofianos Cruz, por el apoyo incondicional que me ha brindado y por ayudarme a seguir adelante y por ser mi admiradora número uno en esta vida.

A MIS HERMANOS: Francisco, Alejandro y Oscar Alfredo por brindarme cariño y apoyo en estos momentos.

A MI ABUELA: Por todos sus sabios consejos y por su ayuda desinteresada que desde la distancia me ha brindado.

A MIS AMIGOS: Exhortarlos a que siempre busquen sus sueños y no permitan que nadie les diga que no son posibles.

A: La Facultad de Ciencias Jurídicas y Sociales, por la formación académica y por ser la fuente de mi conocimiento.

PRESENTACIÓN

En la actualidad, la legislación guatemalteca no regula los delitos que se cometen en las redes sociales ni en los sistemas informáticos, mediante una ley específica, solo se hace un compilado de tipos penales relacionados con la informática a través del Decreto 33-96 del Congreso de la República de Guatemala que agregó los Artículos 274 A al 274 G al Código Penal. Por lo que la investigación contiene un análisis de los tipos penales y los bienes jurídicos violentados en las redes sociales y demás plataformas digitales, considerando su falta de estudio por parte de los legisladores guatemaltecos.

El trabajo de tesis pertenece a la materia de derecho penal, ya que trata lo referente a los delitos cometidos en redes sociales y por ende, a los bienes jurídicos protegidos que se violentan; además, es una investigación de tipo cualitativa, puesto que se realizó desde los temas más generales hasta llegar a los temas más específicos tomando en cuenta que se escudriñó detalladamente los tipos penales informáticos.

El objeto de estudio, por lo antes mencionado, son las redes sociales y las plataformas digitales; y el sujeto son los usuarios de estas, al encontrarse propensos a sufrir algún tipo de delito informático al no contar con una protección jurídica. Y debido a que en Guatemala, son inexistentes las investigaciones relacionadas con este tipo de delitos, esta tesis representa una fuente de información en la doctrina penal y para una ulterior ley que tienda a proteger a las personas en las redes sociales y demás plataformas digitales. La investigación se realizó tomando como base el año en el cual surgen las redes sociales, es decir desde 1996 hasta el año 2017.

HIPÓTESIS

Las redes sociales y las plataformas digitales como herramientas para la comisión de delitos aún no tipificados en la legislación guatemalteca, afecta bienes jurídicos como el patrimonio y crea un marco de inseguridad jurídica-informática, que tiene como efecto inmediato la falta de inversión extranjera y nacional en la industria de las tecnologías y telecomunicaciones que en otros países generan una fuente de inversión, pudiendo comparársele con lo que generan otras industrias históricas. Haciendo imperiosa la creación de una ley que plantea una innovación en el andamiaje jurídico de Guatemala y propulse la modernización del Estado de derecho.

COMPROBACIÓN DE LA HIPÓTESIS

Del análisis realizado en la investigación, se demostró los beneficios que conllevaría para la población guatemalteca la creación de una ley que tipifique las conductas delictivas en las redes sociales y en las demás plataformas digitales; además se comprobó la importancia de proteger ciertos bienes jurídicos que se violentan a las personas, aunque no sean usuarios de estas redes.

De esta manera se validó la hipótesis de la trascendencia de la creación de una ley sobre delitos informáticos y que los legisladores erróneamente han dejado por un lado la importancia de las redes sociales y por ende se ha descuidado la protección de bienes jurídicos de mucha relevancia para la sociedad guatemalteca. La investigación se realizó haciendo uso del método deductivo.

ÍNDICE

Pág.

CAPÍTULO IV

INTRODUCCIÓN

En la actualidad, en la legislación guatemalteca no se ha legislado sobre una ley que regule lo referente a los delitos que se cometen en las redes sociales ni en las demás plataformas digitales. Para protección de los ciudadanos únicamente se cuenta con el Decreto 33-96 del Congreso de la República de Guatemala que entró en vigencia el 3 de julio de 1996 y que reformó el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, concretamente adicionando los Artículos 274 A al 274 G.

Es por este motivo que se realiza la investigación, para comprobar la importancia que tiene para la sociedad guatemalteca la entrada en vigencia de una ley que regule las conductas en redes sociales y que tipifique los delitos que en estas se cometen y por ende, se contribuya a la modernización del ámbito jurídico en Guatemala.

Con lo establecido en el párrafo anterior, es que el objetivo general se alcanzó al establecer los motivos por los cuales es de suma preeminencia para el Estado y para la sociedad en general, que el Congreso de la República de Guatemala apruebe una ley que tipifique las conductas delictivas que se cometen en el ámbito de redes sociales y en las demás plataformas digitales. De este modo es que, el trabajo de tesis comprueba la evolución que representaría para todo el sistema de justicia que se apruebe y entre en vigencia una ley especial que norme todo lo relacionado a materia cibernética y en consecuencia, de lo provechoso que esto sería para los usuarios y para las demás personas, puesto que cualquiera puede ser sujeto de un delito cibernético aun sin ser usuario de redes sociales.

La hipótesis planteada en el trabajo de tesis se comprobó, puesto que, se demuestra que las consecuencias de la creación de una ley que tipifique los delitos informáticos tiene una multiplicidad de beneficios para la sociedad y para el gobierno de turno, dado que dicha ley promovería la inversión extranjera y nacional al contar con un respaldo que provea seguridad informática y conllevaría, además, la creación de una diversidad de

empleos no solo en el ámbito informático sino creando empleos de forma indirecta para los ciudadanos.

Esta tesis se desarrolló en cuatro capítulos: en el primero se trató sobre los delitos informáticos debido a que de estos se derivan los delitos que actualmente se cometen en las redes sociales y en una pluralidad de entornos digitales; en el dos se expuso todo lo referente a las redes sociales, como consecuencia que estas son el espacio en donde se cometen los delitos de que trata la tesis; en el tercero se hizo un estudio de los bienes jurídicos que protege el derecho penal, no solamente mencionando los relacionados con los delitos informáticos sino también, los que se violentan en todos los ámbitos del ciberespacio; y en el cuarto se desglosaron los efectos que los delitos informáticos realizan en Guatemala y de los beneficios que conllevaría la tipificación de dichos delitos.

Durante el desarrollo de la investigación, se hizo uso del método deductivo, ya que se efectuó un estudio de los temas más generales hasta llegar a los más específicos, desde sus raíces, pasando por todo su desarrollo hasta su actualidad, para relacionarlos en el tema final. De la misma forma, se utilizó el método sintético, puesto que, con el análisis de las diferentes instituciones y teorías que se desarrollan en esta investigación, se comprende de una manera más amplia todo lo que envuelve a uno de los temas de más actualidad, como lo son los delitos cometidos en las redes sociales y demás plataformas digitales. Además, se usaron las técnicas bibliográficas y documentales, con el propósito de obtener información de la legislación nacional e internacional y así entender la historia, contenido, principios, teorías y fines del tema principal.

Por medio de la información establecida en este trabajo de investigación se da a conocer los beneficios sociales que implica para la sociedad guatemalteca la creación y necesidad de contar con una ley que tipifique las conductas delictivas en el mundo cibernético y las consecuencias de sumo impacto que en la actualidad se originan de los delitos informáticos. Así pues, la tesis demuestra la relevancia de una ley penal informática en Guatemala.

CAPÍTULO I

1. Los delitos informáticos

En la actualidad las computadoras se usan no solo como instrumentos auxiliares de apoyo en una multiplicidad de actividades humanas, sino como medio para obtener información, lo que las sitúa también como un nuevo medio de comunicación fundado en la informática cuya tecnología se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Las computadoras ponen a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance de millones de interesados y de usuarios, sin limitaciones, con lo cual, entrega con facilidad, un conjunto de datos que hasta hace unos años solo podían ubicarse luego de extensas búsquedas. Ese caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos.

El desarrollo de las tecnologías de la informática ha representado un cambio radical, puesto que se han creado diversas formas de comunicarse como la mensajería instantánea, nuevas redes sociales y videollamadas con los cuales resulta más fácil comunicarse de una forma que hace solo unos años se hubiera considerado inimaginable. Tomando en consideración que el internet es una herramienta con una multiplicidad de beneficios, que se ha vuelto indispensable, convirtiendo a las personas

dependientes de los medios electrónicos ya que los utilizan para realizar una variedad de actividades como comprar en línea, hacer pagos de los servicios domésticos, hacer trámites, comunicarse e incluso publicitarse.

Con lo antes explicado se ha dado paso a que los medios informáticos se usen indebidamente transformando muchas actividades licitas en ilícitas. "Se suben datos personales a la red de empresas, del gobierno y en las redes sociales; esto se ha convertido en un problema ya que existen personas que crackean o hackean esas redes para consultar, obtener o destruir información, generando un delito informático."[1]

El progreso de la informática no solo tiene un lado provechoso para la sociedad, sino que plantea también problemas de significativa relevancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración y la defensa de diferentes programas. Como consecuencia de este desarrollo, surge el aumento del nivel de los delitos relacionados con los sistemas informáticos a nivel mundial, lo que representa una amenaza para la economía de los países y también para los ciudadanos comunes.

La importancia de la informática se realza en la organización tanto de empresas privadas como de entidades públicas en lo referente a investigaciones científicas o incluso como medio de entretenimiento, el uso de la informática es en ocasiones imprescindible. Puesto que la informática está hoy presente en casi todos los campos de la vida moderna, con

[1] Campos, Pamela. Delitos informáticos en México y sus formas de prevención. Pág. 30.

mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos se realizaban únicamente de forma manual. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas circunstancias negativas, como por ejemplo, lo que ya se conoce como criminalidad informática.

Con el pasar de los años se ha demostrado la evolución de los medios tecnológicos y del uso de la informática relacionados con los aportes que estos contribuyen a la sociedad en la actualidad. Por lo que es indiscutible que el progreso moderno no se presentaría si no intervinieran de manera directa los elementos electrónicos que existen hoy en día. No obstante, la utilización de dichos medios informáticos, al ser destinados al servicio de la comunidad, requieren de una imperiosa regulación jurídica con respecto a su utilización.

Los efectos de la revolución digital se hacen sentir en los múltiples sectores de la sociedad a nivel mundial como lo es en la política, economía, educación y en el entretenimiento. Con lo cual, la sociedad ha encontrado nuevas formas de relacionarse y este fenómeno ha traído cambios profundos, por lo que es imprescindible la existencia de cuerpos legales para normar las actividades digitales, con el fin de que no se produzcan efectos negativos ni que se produzcan hechos delictivos.

Por lo antes mencionado, el desarrollo de las tecnologías ha provocado la existencia de nuevos tipos penales, por lo que es importante mencionar que los antecedentes de los delitos informáticos van a la par del progreso de las tecnologías de la información. Con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y

desarrollo en muchas áreas. Por lo que por un lado representa una mejora para la sociedad, por otro, los delincuentes se han beneficiado al tener nuevos medios para cometer delitos.

Como se ha mencionado, los beneficios que ha traído la revolución tecnológica son de gran relevancia para la humanidad, pero como proceso también conlleva consecuencias negativas, como lo es que el ciberespacio ha sido concebido como un ámbito propicio para la realización de conductas antijurídicas. "A partir de la existencia de nuevas formas de operar con la tecnología, aparecen delitos que no son nuevos, sino que existían desde mucho antes de la aparición de la informática, pero que presentan importantes particularidades que han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver."[2]

El avance de la tecnología ha causado que los delincuentes cuenten con nuevas herramientas delincuenciales; y se tenga la posibilidad de cometer delitos desde cualquier parte del mundo con una gran cantidad de víctimas potenciales bajo un total anonimato.

1.1 Definición de delito informático

La revolución tecnológica de los últimos años ha traído consigo las nuevas tecnologías de la información y de la comunicación que han producido un cambio necesario en la

[2] Quintero, René. Delitos informáticos. Pág.1

sociedad dando lugar a esta nueva sociedad digital, donde el hombre busca el desarrollo de su conocimiento y un mayor acceso a la información, lo que lleva a modificar y a producir cambios en el pensamiento humano. Toda esta nueva tecnología que promueve la vida cotidiana se desarrolla en conjunto con la aparición de un nuevo entorno digital, es decir, representa un medio en el que cada persona recibe, transmite y obtiene permanentemente información a través de las redes sociales en las que el espacio físico y el tiempo son modificados por redes de comunicación cibernética que permiten procesar información y transmitirla en tiempo real desde cualquier lugar del mundo generando grandes recursos de información en forma de imágenes, textos, gráficos y sonidos.

Lo antes mencionado, tiene consecuencias en múltiples ámbitos ya que las redes sociales se han convertido en un espacio social, y una alternativa al mundo real donde se desarrollan actividades comerciales, informativas, de ocio, y también ilícitas. Con lo que el perfeccionamiento y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como el análisis de la suficiencia del sistema jurídico vigente para regular las nuevas posiciones, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo moderno.

Es por esta razón, que de la mano de la evolución de la tecnología informática y su influencia en una multiplicidad de áreas de la vida social, han surgido una serie de comportamientos delincuenciales y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad en la mayoría de legislaciones. "La doctrina ha denominado a este grupo de

comportamientos, de manera genérica, delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática."[3]

Para poder entender y describir, cuáles de la gran variedad y clases de hechos y actos que se presentan hoy día en las redes sociales se pueden encuadrar en los delitos informáticos, es necesario saber primero que significa una red social y posteriormente definir el concepto de delito informático, con el propósito de caracterizar cuáles de las actividades presentes y que desarrollan las personas que hacen parte de estas redes podrían legalmente sancionarse por hechos que lesionan algún bien jurídico tutelado. Y así posteriormente encaminar la normatividad hacia el control legal de estas redes para brindarles a todos los usuarios las herramientas legales específicas para defenderse, prevenir y sancionar este creciente ambiente digital.

Redes sociales son las plataformas informáticas a través de las cuales las personas interactúan a distancia y mediante las cuales se transfieren una innumerable cantidad de datos. Se puede decir, además, que redes sociales son "aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción".[4] Lo anterior tiene especial relevancia si se toma en cuenta los principios formadores del derecho penal, que se deben tener a la vista en todo momento. En efecto, no basta en este caso únicamente la intuición en cuanto a que se estima que una

[3] Del Pino, Santiago. Delitos informáticos: generalidades. Pág. 4.
[4] Sanz Rodríguez, Patricia. Redes sociales y derecho penal. Pág. 6.

determinada conducta podría ser punible, el derecho penal exige una subsunción exacta de la conducta en la norma penal para que se esté en presencia de un hecho que revestido de carácter ilícito.

Ya definido el concepto de redes sociales, es preciso entender diferentes conceptos que se han venido presentando con el surgimiento, impacto y el desarrollo de las tecnologías de información pues estas han generado la necesidad de ajustar las formas de operación de las organizaciones, tanto de sus procedimientos estándares hasta la aplicación de otras tecnologías. Por lo que es de suma relevancia encontrar una aproximación que permita relacionar la normatividad jurídica con la realidad y con las tendencias de la tecnología en conjunto con los delitos informáticos.

El delito informático se puede definir desde un punto de vista típico y atípico y se puede decir que es una "actitud contraria a los intereses de las personas en que se tiene a los computadores como instrumento o fin; o las conductas típicas, antijurídica o culpables en las que se tienen los computadores como instrumento o fin."[5]

El delito informático está vinculado no solo a la realización y una conducta delictiva a través de miembros o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información como bien jurídico tutelado, diferenciándolo de los intereses jurídicos tradicionales dentro de las distintas legislaciones.

[5] Ojeda, Jorge. Delitos informáticos y entorno jurídico vigente en Colombia. Pág. 49.

Es importante resaltar que el delito informático no se realiza necesariamente para obtener un determinado beneficio. Este delito es también: "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas."[6]

La definición de delito informático varía según cada legislación. En algunos países es diferente, puesto que se sanciona a los delitos cometidos contra el software y en otros no se tipifican dichos hechos. No obstante se debe tomar en cuenta que un equipo informático está compuesto de software y hardware, y un ataque informático puede afectar a ambos. Esto significa que la especialidad de los delitos informáticos se basa en realizar ataques informáticos en contra del software o hardware de un medio electrónico, con el objeto de obtener información, alterar o causar daños en el funcionamiento del sistema y otras conductas ilícitas. Asimismo, ya no solo existen delitos informáticos que atentan contra el patrimonio, sino que ahora dañan a la persona físicamente atentando contra su dignidad personal, su libertad sexual y su vida.

Después de haber mencionado algunas definiciones de delito informático se debe destacar algunas consideraciones importantes sobre las mismas. Cabe destacar sin establecer una regla genérica, que un delito de este tipo se puede cometer, no solo utilizando una computadora sino cualquier dispositivo electrónico. Lo cual, se convierte

[6] Hernández, Leyre. El delito informático. Pág. 227.

en el primer supuesto de este tipo de conductas antijurídicas. Y ello resulta un poco confuso para el legislador puesto que no se puede prever la innumerable cantidad de medios a través de los cuales es posible afectar un determinado bien jurídico penalmente protegido.

1.2 Sujetos del delito informático

En la doctrina penal, la ejecución de la conducta punible supone la existencia de dos sujetos, un sujeto activo y otro pasivo. A su vez, estos pueden ser una o varias personas naturales o jurídicas.

En este orden de ideas, el bien jurídico protegido es en definitiva el elemento localizador de los sujetos y de su posición frente al delito. De esta manera, el titular del bien jurídico lesionado es el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. Por lo que, quien lesione el bien que protege la legislación, a través de la realización del tipo penal, es el ofensor o sujeto activo.

Los sujetos que participan en un delito informático son: el sujeto activo. Se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal; y el sujeto pasivo que es la persona titular del bien jurídico que la ley protege y sobre la cual recae la actividad típica del sujeto activo del delito.

En el derecho penal, específicamente en el delito en tratamiento, se suele llamar sujeto activo a la persona que provoca un daño y que posee habilidades para el manejo de

sistemas informáticos y que tiene un nivel y coeficiente académico superior a la media de las personas. Por su parte el sujeto pasivo comprende a las víctimas de los delitos informáticos, es decir, es el afectado de la acción que realiza el sujeto activo. El sujeto pasivo puede ser una institución gubernamental, bancaria, militar o cualquier tipo de empresas públicas y privadas, respecto a este sujeto se debe hacer mención que la mayoría de víctimas no denuncia derivado de la falta de un cuerpo legal que sancione este tipo de delitos; las instituciones o empresas no denuncian debido al desprestigio que ocasionaría hacia ellas y la posterior desconfianza en la sociedad.

El sujeto activo en el delito informático, es una persona que ostenta características que no tienen los delincuentes comunes, debido a que son sujetos que poseen habilidades para el manejo de los sistemas informáticos y generalmente se encuentran en lugares adecuados donde se maneja información sensible.

Con el progreso del delito informático se ha podido corroborar que los autores de estos delitos son muy diversos y que, lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que ingresa en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

De la mano del estudio del delito en mención, surge la controversia sobre las aptitudes del delincuente informático, puesto que para algunos autores el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas inteligentes, decididas, motivadas y dispuestas a

aceptar un desafío tecnológico, características que se pueden encontrar en un empleado del sector de procesamiento de datos.

Tomando en consideración las características mencionadas de los sujetos de este tipo de delitos, estudiosos en la materia han nombrado a los delitos informáticos como delitos de cuello blanco, el cual se atribuye que fue el criminólogo Edwin Sutherland en el año de 1943 el primero en usarlo. El cual utilizaba este término ya que, el sujeto activo del delito informático es una persona de cierto status económico, su comisión no puede explicarse por motivos de pobreza ni por mala habitación, ni tampoco por carencia de recreación, ni por baja educación, ni mucho menos por poca inteligencia.

A lo anterior es importante agregarle que los delitos informáticos no poseen todas las características de los delitos de cuello blanco, en cierta medida coinciden en un número importante de ellas, por ello mismo, la cualificación del sujeto activo no es un elemento determinante en la delincuencia informática. Solo algunos delitos, como los cometidos por los hackers propiamente dichos, pueden considerarse como realizados por un sujeto altamente calificado. Los demás, no requieren, en cuanto al sujeto, calificación, toda vez que pueden cometerse por personas que recién se inician en la informática o por niños que están aprendiendo individualmente en sus hogares.

El sujeto pasivo del delito informático, es sumamente importante para el estudio de dichos delitos, ya que mediante él se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas puesto que muchos de los delitos no son descubiertos por el desconocimiento del modus

operandi de los sujetos activos. Esto genera que la mayoría de estos delitos no sean denunciados y por ende, no sean investigados por las entidades correspondientes.

1.3 Características de los delitos informáticos

Derivado del estudio de los delitos informáticos se ha logrado determinar las características de los mismos. Destacando que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio utilizado para cometer tales delitos. En este orden de ideas, se entiende como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático. Y que a largo del estudio de tales delitos se ha fijado que las características de estos son:

" a) Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas;

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando;

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico;

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras;

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse;

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho;

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar;

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico;

i) En su mayoría son imprudencias y no necesariamente se cometen con intención;

j) Ofrecen facilidades para su comisión los menores de edad;

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación; y

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley."[7]

Con lo anterior se evidencia, que las características de este tipo de delitos no se enfocan solo a causar un daño económico sino que tienen una multiplicidad de propósitos en su mayoría, para obtener información personal o restringida.

1.4 Clasificación de los delitos informáticos

Los delitos informáticos se clasifican de acuerdo a dos criterios; sin embargo en Europa se cometen bajo tres preceptos ilícitos: acceso no autorizado, actos dañinos o circulación de material dañino e intercepción no autorizada. No obstante en la legislación internacional predominan dos supuestos para la realización de estos delitos, los cuales

[7] Téllez Valdés, Julio. **Derecho informático**. Pág. 188.

son: como instrumento o medio y como fin u objetivo. Los primeros son aquellas conductas que se valen de las computadoras como método o medio en la comisión del ilícito; y los segundos son las conductas dirigidas en contra de la computadora, accesorios o programas comprendidos como entidad física.

Lo anterior indica que los delitos informáticos como instrumento o medio son los hechos ilícitos que se cometen haciendo uso de computadoras, por ejemplo: intervenir líneas telefónicas, realizar espionaje, la clonación de tarjetas de crédito, fraude electrónico, *hackear* el correo electrónico, *crackear* sistemas del gobierno o empresas crediticias, entre otros.

Los delitos informáticos como fin u objetivo poseen una conducta ilícita dirigida en contra del *hardware* o *software* de un medio electrónico, por ejemplo: instalar o enviar virus con el propósito de dañar el disco duro de la víctima, y el uso no autorizado de programas, tales como: *spyware* y *malware* que envían información privada al usuario creador y causan la pérdida de datos. Los delitos como instrumento o medio pueden ser:

"a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d) Lectura, sustracción o copiado de información confidencial.
e) Modificación de datos tanto en la entrada como en la salida.
f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de cómputo.

i) Introducción de Instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso."[8]

En los delitos como fin u objetivo se encuadran las conductas criminales que van dirigidas contra las computadoras, elementos accesorios y programas como entidad física, como por ejemplo:

"a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)"[9] La clasificación antes listada, es la rectora en lo

[8] Quintero. **Op. Cit.** Pág. 5.
[9] **Ibid**.

referente a la división de los delitos informáticos, sin embargo, al hacer un recorrido por la doctrina penal se puede apreciar que existen otras clasificaciones de delitos, como lo son, las categorías a saber: Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito; los que manejan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo; y los que manipulan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica con objeto de dañarla.

1.5 Tipos de delitos informáticos

Derivado de la clasificación de delitos surgen los tipos de delitos informáticos que se pueden cometer y que se encuentran estrechamente ligados a acciones realizadas en contra de los propios sistemas.

Después de surgir los delitos informáticos se ha realizado una variedad de tipos delincuenciales informáticos, no obstante se logrado consensuar que los tipos de delitos informáticos básicos son: el acceso no autorizado, es decir, el uso ilegítimo de contraseñas y la entrada de sistemas informáticos sin la autorización del propietario, constituyendo así una violación a la privacidad; La destrucción de datos provocados en la red mediante la introducción de virus que buscan causar un daño severo en la computadora del sujeto pasivo; La infracción a los derechos de autor de una base de datos, usando la información almacenada sin ningún tipo de autorización de parte del propietario de dichos datos; la interceptación de correos electrónicos; las estafas

electrónicas, por medio de compras utilizando internet; y transferencias de fondos con el objetivo de sustraer dinero de una cuenta sin la debida autorización del propietario.

Las conductas antes mencionadas, como se indicó, son los temas de donde se deriva una variedad de acciones antijurídicas que tratan de causar un daño o lograr un beneficio económico. Por ello se hace necesario hacer mención de los tipos de delitos más comunes en la actualidad, puesto que con el desarrollo del internet han surgido nuevas formas de cometer actos delictivos, desde los más sofisticados, realizados por personas versadas en informática, hasta los más comunes cometidos por estudiantes o por personas con conocimientos elementales de internet.

El delito informático más común en la modernidad es el *hacking,* que es la conducta o acción de intervenir o realizar alteraciones en sistemas informáticos realizados por un hacker violando mecanismos de seguridad a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones. El sujeto activo del *hacking* es un hacker que es una persona con desarrollados conocimientos en tecnología, bien puede ser informática o electrónica, que se mantiene constantemente actualizado, y conoce a fondo todo lo relacionado con programación y sistemas que son difíciles de entender para una persona sin estos conocimientos específicos, es un investigador con capacidades únicas que se inclina ante todo por la curiosidad de acceder a datos ocultos y a cualquier tipo de información segura.

Es significativo resaltar que el *hacker* suele salir del sistema sin posteriores propósitos, no obstante, comúnmente son la antesala de violaciones graves contra la intimidad de

las personas, contra los derechos de propiedad intelectual o industrial o contra los secretos de empresas, sin importa el poder económico de la misma.

Esta figura delincuencial, el *hacker*, frecuentemente es confundida con los *crackers,* que más adelante serán explicados, debido a que las personas sin mayores conocimientos de informática, conocen a los *hackers* como personas que se dedican a romper la seguridad de empresas o de instituciones gubernamentales, pero en realidad se dedican a poner a prueba el nivel de seguridad de un sistema informático de una empresa, para determinar si es seguro y confiable, con el propósito de prevenir ataques en el futuro.

Para constituir el delito de *hacking*, el *hacker* deber hacer públicos los datos obtenidos, con el fin de obtener un beneficio. Los *hacker*, en sí se encargan de crear programas para proteger equipos de los ataques informáticos, generalmente no tienen intención de causar un daño y su desafío se basa en quebrantar sistemas de seguridad.

La tipificación penal del *hacking* es ciertamente confusa, ya que si la conducta se mantiene en el estricto ámbito de la intromisión informática, se debe considerar desde el punto de vista de su relevancia penal, como impune o atípica.

En muchas ocasiones las conductas de los *hackers*, ni siquiera llega a alcanzar la consideración de una tentativa o de un acto preparatorio para la comisión de un delito, debido a que no concurren los elementos típicos para determinar un hecho como un delito, puesto que, como se indicó anteriormente en el presente trabajo de tesis, la finalidad del *hacker* no es atentar contra la intimidad o contra la propiedad intelectual

como tampoco es dañar los sistemas o los programas informáticos en los que se entromete.

Con el progreso del *hacking* se ha evidenciado el surgimiento de nuevos tipos de *hackers.* Entre los cuales se puede mencionar: Los *black hat hackers, white hat hackers, gray hat hackers, script kiddies, phreaker, newbie* y los *lammers*.

Los *black hat hackers* son aquellos que se dedican a quebrantar la seguridad de un medio electrónico, creando algún virus con el propósito que los servidores sufran daños que provoquen la perdida de información.

Los *white hat hackers* son los *hackers* que contribuyen a la informática por medio de sus aportaciones. Por lo general son los que se dedican exclusivamente a encontrar vulnerabilidades en el sistema de seguridad de los ordenadores para las empresas para las cuales laboran.

Los *gray hat hackers,* son aquellos sujetos que utilizando sus conocimientos protegen o incrementan la seguridad o que por el contrario rompen la seguridad de los sistemas informáticos.

Los *hackers* llamados *script kiddies* son aquellas personas que no tienen los conocimientos suficientes sobre informática y utilizan una variedad de programas para irrumpir un determinado sistema o una red de computadoras, pero que en realidad no tienen idea de cómo esos programas afectan a un sistema.

Los *phreaker* son los *hackers* que poseen extensos conocimientos en telefonía, por lo que se dedican a intervenir dispositivos móviles para obtener un beneficio sin el consentimiento del titular del móvil.

El *hacker newbie* es una persona que se dedica a estudiar o ha estudiado sobre informática y navega por la red buscando información sobre como *hackear*. Se diferencian por ser curiosos ya que descargan programas sobre *hackeo* y los ejecutan para observar cómo funcionan.

Los *lammers* son aquellas personas que no tienen ningún conocimiento ni mucho menos habilidades para comprender lo que realmente pasa cuando se utiliza algún programa hecho para *hackear.*

Lo recién explicado se refiere únicamente al hacking, por otro lado en el tema de delitos informáticos se puede encontrar la figura del *crackeo* que es la operación de romper sistemas de seguridad, con la finalidad de causar daños en el sistema mediante diversos programas maliciosos, realizados por un *cracker,* generalmente para dañar plataformas de instituciones estatales o privadas.

El *craker* es la persona que dedica su tiempo a romper la seguridad de los sistemas y su principal objetivo es robar información, realizar transacciones ilícitas, asimismo, imposibilitar el buen funcionamiento de redes informáticas mediante algún malware o troyano, además crean puertas traseras en el sistema para poder entrar en otro momento más oportuno.

Otro importante delito a mencionar es el cibergrafitti, que no es más que causar un daño a una página web. En otros términos, es la conducta de ingresar a un sitio web con el propósito de modificar su contenido de forma intencional, poniendo imágenes pornográficas, amenazas o burlas por mencionar algunos.

El cibergrafitti es cometido por un *cracker* que se dedica a resquebrajar la seguridad de páginas web, aprovechándose de sus vulnerabilidades, con el fin de cambiar dicha página o crear otra para beneficio de este y como una manera de poder expresarse.

Otro delito importante que se ha incrementado en los últimos años es el de fraude, específicamente, el llamado fraude nigeriano que también ha recibido el nombre de pago por adelanto, el cual consiste en un mensaje por correo electrónico proveniente del extranjero solicitando ayuda para retirar una determinada cantidad de dinero de su país y ofrece al destinatario un porcentaje del dinero por ayudarle en la transferencia.

El fraude nigeriano ha impactado una variedad de países del mundo, pero sus orígenes son de países del continente africano. Este tipo de fraude es realizado por personas organizadas versadas en la informática y utilizando identidades falsas afirmando ser funcionarios del gobierno o empresarios con la finalidad de engañar a las víctimas.

Por su parte del delito de *phishing* se refiere a suplantar una identidad, que persigue apropiarse de datos confidenciales de los usuarios con el objeto de menoscabar patrimonios ajenos. Este consiste en recabar información crediticia, tal como: números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por

medio de engaños. El *phishing* se lleva a cabo habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

El *phishing* es cometido por un sujeto denominado *phisher* que se hace pasar por una persona o empresa de confianza, simulando una comunicación real en forma electrónica, en el cual se imita el contenido o la imagen, mayormente de una entidad bancaria para engañar al usuario, logrando obtener la información personal que facilita el acceso a sus cuentas, comúnmente mediante un correo electrónico, o haciendo uso de algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. A partir de la obtención de estos datos confidenciales, el *phisher* procede a apoderarse de los patrimonios ajenos ordenando transferencias bancarias.

Como se puede apreciar en lo recién explicado, existen unos delitos informáticos que son los más comunes en la actualidad pero que lamentablemente no son los únicos, por resaltar algunos se encuentran:

Ataques contra sistemas y datos informáticos
Usurpación de la identidad
Distribución de imágenes de agresiones sexuales contra menores
Intrusión en servicios financieros en línea
Difusión de virus Botnets.

Sin embargo, también existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información tales como:

Sexting

Acceso a material inadecuado

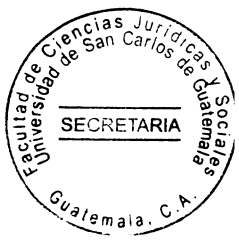
Adicción - procrastinación

Problemas de socialización robos de identidad

Acoso

Ciberbullying

Cibergrooming


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

CAPÍTULO II

2. Las redes sociales y plataformas de internet

En los últimos años la gran evolución en internet ha logrado el surgimiento de un servicio tecnológico que se encuentra presente en todos los ámbitos de la vida, como lo son las redes sociales, las cuales son plataformas virtuales que agrupan a personas con el fin de relacionarse entre sí y que comparten información e intereses comunes. Las redes sociales tienen como principal objetivo, establecer contactos entre personas ya sea para establecer una relación de amistad o para reencontrarse con viejos conocidos.

Es evidente que el avance de la tecnología de información y comunicación como lo son las redes sociales crean un sinnúmero de cambios y repercusiones en el comportamiento humano produciendo transformaciones de los ámbitos jurídicos y sociales de todo el mundo.

Toda esta unificación de la tecnología con la vida cotidiana se desenvuelve de la mano con la aparición de un nuevo entorno digital, constituyendo un medio en el que cada persona transmite, recibe, y obtiene información, el cual se realiza por medio de las redes sociales en las que el espacio físico y el tiempo son transformados por redes de comunicación cibernética que permiten procesar información y transmitirla en tiempo real desde cualquier lugar del mundo generando grandes recursos de información en forma de imágenes, textos, gráficos y sonidos, y como se mencionó en el párrafo anterior todo esto tiene consecuencias en múltiples ámbitos puesto que estas redes se han convertido

en un espacio social, siendo una alternativa al mundo real donde se desarrollan actividades comerciales, formativas, de holganza y también ilegales.

Antes de entrar a conocer en sí, las redes sociales se hace necesario saber sobre sus antecedentes, para la cual es importante resaltar que estas son relativamente nuevas, y que en los últimos años han alcanzado un sinfín de avances logrando una masificación de su uso, la cual fue posible debido a que los usuarios no solo pueden hacer uso de las redes sociales a través de su computadora, sino que además en los últimos tiempos se ha logrado que se pueda participar en este tipo de comunidades a través de una gran multiplicidad de dispositivos móviles, tales como teléfonos celulares o computadoras portátiles, marcando la nueva tendencia en comunicación.

Se considera que el origen de las redes sociales se remonta al año de 1995. Época en la cual el internet empieza su masificación. Se cree que Randy Conrads es el verdadero pionero del servicio de comunicación por medio del internet, mediante la creación del sitio web que llevaba por nombre *Classmates*, y el cual radicaba en una red social que brindaba la posibilidad de que las personas desde cualquier lugar pudieran recuperar o continuar manteniendo contacto con sus antiguos amigos, ya sea compañeros de colegio, de la universidad o de cualquier otro sitio, de distintos ámbitos laborales y demás, en medio de un mundo totalmente globalizado.

Pero recién dos años más tarde, en 1997, cuando aparece la página web SixDegrees.com se genera en realidad el primer sitio de redes sociales, tal y como se lo conoce en la actualidad, que permite crear perfiles de usuarios y listas de amigos.

No es hasta la primera parte de la década del 2000 que comienza a aparecer una gran variedad de páginas web dedicadas a ofrecer la posibilidad de comunicación dentro de lo que ahora se llama redes sociales, que en aquel entonces eran conocidas como círculo de amigos. Estos círculos se popularizaron en el año 2003, con el advenimiento de redes sociales específicas, que ofrecían ya no únicamente reencontrarse con amigos o crear nuevas amistades, sino como espacios de intereses afines.

A lo anterior se debe agregar que, la más grande de todas las explosiones de las redes sociales no tardó en llegar, puesto que en el año 2003 vieron la luz algunos de los sitios más multitudinarios que lograron hacer crecer exponencialmente el uso del servicio, y comunidades como MySpace, Friendster, Tribe y Xing, entre otras. Fueron precisamente estos sitios los precursores en lograr que las redes de interacción o círculos de amigos comenzaran a socializarse, con lo que captaron la atención de millones de usuarios de todo el mundo.

2.1 Concepto de red social

Internet y más específicamente de manera muy especial, las redes sociales conforman un nuevo contexto social caracterizado, por su alcance temporal y espacial de las comunicaciones, creando a través de ello, proximidades virtuales. Las redes sociales, cumplen, en la actualidad, una labor de socialización importante, puesto que las mismas despliegan una influencia en la sociedad y en cada uno de sus elementos. Para definir a las redes sociales es necesario describirlas como formas de interacción social, como una intercomunicación dinámica entre personas, grupos y organizaciones en diferentes

contextos sociales. Las redes sociales en la contemporaneidad son plataformas de comunicación que suministran actualizaciones automáticas, perfiles visibles, capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea.

Las redes sociales son sitios en línea mediante las cuales las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, y conocidos en cualquier lugar del planeta. De lo cual se deduce que estas fueron creadas para establecer un espacio virtual con el fin de lograr la interacción entre personas.

La interacción dentro de una red social está delineada por algunas características particulares como el anonimato total o parcial, como el usuario lo desee, la facilidad de contacto paralelo o anticuado, así como también la seguridad e inseguridad que dan las relaciones que se llevan a cabo por medio de estas y es por lo cual ofrecen a los cibernautas un lugar común para desarrollar comunicaciones constantes.

La base de la operatividad de las redes sociales es el mismo usuario, toda vez que estas redes son construidas y dirigidas por estos, quienes además constantemente las nutren de información.

Estas redes favorecen el cambio de estructuras sociales dando paso al desarrollo humano y comunitario, creando espacios de encuentro y reunión que sirven para compartir experiencias, para intercambiar información, para plantear problemas y generar sus respectivos proyectos de solución propagando información masivamente en instantes

sin ninguna restricción. Por lo tanto, se puede decir que las redes sociales constituyen un sistema que maneja multitud de datos personales, relativos a la identidad de las personas. En este orden de ideas, es prioritario que las distintas legislaciones establezcan reglas que se deben seguir para la correcta recepción y el uso de la información almacenada en tales servicios.

Es importante mencionar, que el internauta ya no es un mero sujeto pasivo, ahora también es un sujeto activo, puesto que, activamente, difunde información, opina en foros, comparte fotografías o grabaciones de vídeo, entre otros. Por ello mismo, los actos de los usuarios pueden acabar repercutiendo en los derechos de terceros.

Las redes sociales poseen una teoría llamada de los seis grados, por medio de la cual, la mayoría de personas mantiene un vínculo directo, permanente más o menos con alrededor de 100 personas. De acuerdo a esta teoría si 100 usuarios presentaran a sus 100 contactos respectivos se tendría a 10000 usuarios, y así sucesivamente hasta llegar a un sexto nivel, con un total de un billón de personas.

Por consiguiente, se puede concluir este apartado, indicando que las redes sociales son sitios web que ofrecen servicios y funcionalidades de comunicación diversa para mantener en contacto a los usuarios de la red en cualquier sitio; se basan en programas especiales con la finalidad de integrar numerosas funciones individuales: blogs, foros, chat, mensajería, entre otros, en una misma plataforma y que proporcionan la conectividad entre los diversos usuarios; y que son redes de relaciones personales, que proporcionan sociabilidad, información y un sentido de pertenencia e identidad social a

diferente grupos de la sociedad, en su mayoría de jóvenes con un sentido de pertenencia a un grupo con una cultura en la cual se comparten valores, normas y un lenguaje en un clima de confianza.

2.2 Tipos de redes sociales

En la actualidad existen tres tipos de redes sociales: redes personales, redes temáticas y redes profesionales. Aunque es probable que no se tomen en cuenta otros tipos de redes. Las tres antes mencionadas tienen un mayor nivel de visitas por sus usuarios.

Las redes sociales personales son aquellas que se integran por cientos de millones de usuarios en los que cada uno tiene su propio espacio con su información, fotos, música, entre otros. Y cada uno se puede relacionar con los demás miembros de múltiples maneras, aunque todas ellas involucran el uso de Internet de una u otra forma.

En las redes sociales personales los intercambios son esencialmente de tipo cerrado, es decir con un número selecto de personas y la intensidad del intercambio es definida por la distancia de los elementos la cual a su vez se subordina por tres factores como lo son lo social, lo físico y lo psicológico.

En lo referente a los tres factores indicados en el párrafo anterior, respecto a la distancia social, consiste en las prescripciones socialmente establecidas para el desarrollo del intercambio entre los individuos. En referencia a la distancia física es en cuanto a la intensidad del intercambio en función de la cercanía o lejanía que tienen los miembros

de la red. Entre más lejana es la ubicación de un elemento menor será la intensidad del intercambio y todo lo contrario cuando la ubicación es cercana; y en alusión a la distancia psicológica es primordialmente una variable que se relaciona con la voluntad o el deseo de establecer intercambios con alguien más sin importar la distancia, para lo cual, la distancia psicológica se relaciona directamente con la confianza.

Las redes sociales temáticas son aquellas que tiene mucha similitud con las redes personales, no obstante, se diferencian por el hecho de que frecuentan centrarse en un tema en concreto y proporcionan las funcionalidades necesarias para el mismo. Por ejemplo, una red de cine, una de informática o de algún tipo de deporte siempre y cuando se refiera al mismo campo o área.

Las redes sociales profesionales son un tanto distintas a las dos previamente explicadas. Estas se dedican exclusivamente al ámbito laboral, en todas sus áreas. Estas redes se utilizan para poner en contacto a aquellas personas que ofrecen algún tipo de trabajo y para crear grupos de investigación, por mencionar algunos. En ellas los usuarios y las empresas son los protagonistas que permiten dar inicio a las relaciones laborales, de esta forma permitiendo el intercambio de información multimedia entre sus miembros como son: fotos, videos, blogs entre otros recursos.

Las redes profesionales promueven el aprendizaje colaborativo por medio de los dispositivos electrónicos como un recurso eficiente en la gestión del conocimiento del ámbito empresarial. Así también, estas buscan la participación activa del capital intelectual en las diferentes organizaciones, a través de experiencias colaborativas, en la

conformación de grupos de discusión e intercambios de conocimientos que apliquen ideas del trabajo en línea. Por lo que las redes sociales profesionales han revolucionado, en cierta forma los métodos de búsqueda de empleo, por un lado, y los procesos de captación de candidatos por el otro, ya que las personas buscan algún empleo y por su parte, las empresas examinan los diferentes historiales de trabajadores con un perfil en estas redes

Por lo mencionado en el párrafo anterior, se puede distinguir que las redes sociales profesionales han implantado importantes cambios en el sector laboral, puesto que, estas: mejoran la comunicación con el cliente, facilitan la gestión del conocimiento, refuerzan el compromiso de los empleados, ofrecen nuevas vías de comunicación y facilitan la selección de recursos humanos.

Las redes sociales profesionales, tienen como principal finalidad estimular, incentivar y aumentar las relaciones entre profesionales, tanto de un mismo sector, como de sectores diferentes. Este tipo de redes tienen un crecimiento más homogéneo, son más estables en comparación a las redes personales y temáticas.

En la actualidad estas redes son consideradas, por los usuarios, como una excelente herramienta de trabajo para buscar empleo, seleccionar candidatos o hacer contactos para los fines profesionales más diversos. Estas son usadas cada vez más, por las diferentes empresas con el propósito de acceder a una cantidad mayor de profesionales a los que puede clasificar y contactar de una manera rápida, fácil y sencilla. Asimismo, para finalizar el presente apartado es loable mencionar que por medio de las redes

sociales profesionales las personas logran darse a conocer y destacar en determinados ámbitos, habitualmente vinculados a una carrera profesional; permite la interrelación de contenidos realizados por los propios usuarios enfocado a un ámbito artístico o laboral; y los usuarios buscan enriquecer sus relaciones profesionales o personales.

2.3 Redes sociales más importantes

Con el crecimiento de las redes sociales han ido surgiendo nuevas plataformas de comunicación a distancia, para lo cual es prominente mencionar a las redes sociales que en la actualidad predominan la web.

Hoy en día, la red social con más usuarios es *Facebook*, es la más representativa y usada a nivel mundial. En inicios era de uso exclusivo de universitarios, sin embargo, en setiembre del 2006, se amplió sus fronteras permitiendo así que cualquier persona que tenga un correo pueda acceder a dicha red.

Facebook ofrece dos tipos de cuentas: las de cualquier usuario normal y la que pueden abrir las empresas. Las primeras son gratuitas y permiten una comunicación fluida entre personas reales; las segundas se utilizan para ofrecer productos o servicios y mantener contacto entre empresas y clientes. Estas pueden ser gratuitas o de pago.

Por medio de las cuentas de uso normal que ofrece esta red social, cada usuario puede crear una página personal que recibe el nombre de: grupo, donde se muestran actividades o eventos a realizar por esa persona. Estos grupos frecuentan encontrarse

visibles para que cualquier usuario los encuentre aunque solo aquellos que forman parte de él pueden participar comentando o compartiendo contenido dentro del mismo. Con el fin de colaborar al entretenimiento de sus usuarios, *facebook* brinda aplicaciones y juegos a sus miembros, convirtiéndose en una plataforma que trasciende el contacto social entre amigos.

Por su parte, la red social, *Twitter*, es una aplicación gratuita que permite a sus usuarios estar en contacto en tiempo real con personas de su interés por medio de mensajes breves de texto que se denominan tweets.

Los usuarios de *Twitter* pueden suscribirse a los *tweets* de otros usuarios, siguiéndoles, y a estos usuarios, se les llama seguidores. En la mayoría de los casos los *tweets* de los usuarios son totalmente públicos, de manera que los pueden ver todas aquellas personas que estén registradas en *Twitter*, pero los mismos internautas pueden cerrar su cuenta de manera que sus *tweets* solo pueden ser vistos por aquellos a los que siguen y a su vez les siguen.

El éxito de *Twitter* ha sido tal que gobiernos la han incluido en la lista de los medios de comunicación para difundir acciones e información pública, en la cual, en algunos casos se incluye un blog y un listado de direcciones de *Twitter* de todas las secretarías y sus titulares, donde se detalla el tipo de manejo e información que se provee en esas cuentas. Así también, es rescatable mencionar que *Twitter* es la red social que más se ha desarrollado como herramienta profesional entre los periodistas, por delante de *Facebook*, *LinkedIn* y otros.

En el presente apartado, es relevante hacer un resumen de la red social profesional, llamada *LinkedIn*. Esta se orienta a ayudar a sus usuarios a establecer contacto con antiguos colegas, impulsar carreras con contactos directos cuando se busca un trabajo y además pone a disposición consejos de expertos en una multiplicidad de área laborales.

Por lo antes mencionado, se puede apreciar que *LinkedIn* es una red social proyectada a hacer conexiones profesionales y de negocios. *LinkedIn* posee como característica principal que permite publicar datos como experiencia, educación, páginas web y recomendaciones, asimismo permite establecer contacto con otros miembros enfocados a un ámbito profesional específico. También permite tener publicado el currículum vitae y actualizarlo de forma periódica, de tal forma que los contactos profesionales pueden conocer los cambios de trabajo así como localizar perfiles que más se adapten a un nuevo puesto u oportunidad de trabajo. En ese sentido, *LinkedIn* facilita realizar búsquedas por nombre completo, empresa en la que se trabaja, o se ha trabajado, y sector al que se pertenece.

Las tres plataformas de comunicación antes mencionadas son en la actualidad las más relevantes, no obstante, existen otras con una cantidad importante de usuarios, por ejemplo: la red social *PartnerUp* que es una comunidad enfocada en las necesidades de emprendedores y dueños de pequeñas empresas; *Plaxo* que inició como una simple libreta de direcciones en línea pero se ha transfigurado en una herramienta para compartir información con todos los miembros de dichas listas de contactos; la red social *Xing* permite gestionar y establecer contactos profesionales y se basa en el principio de la teoría de los seis grados, explicada anteriormente en el presente trabajo de tesis.

La red social *cofounder* es una comunidad privada para emprendedores, más que todo, programadores, diseñadores e inversionistas implicados con el inicio de nuevos proyectos. Es utilizada para crear equipos y obtener consejos para un determinado negocio.

Focus es un sitio en el cual los profesionales pueden ayudarse unos a otros a tomar decisiones de negocios, por ende, es otra comunidad para compartir y encontrar información sobre bienes y servicios.

E factor es una comunidad diseñada para emprendedores, por emprendedores. Es el lugar idóneo donde estos pueden hacer contactos profesionales, negociar, intercambiar información y publicitar productos y servicios que tengan a disposición.

Entrepreneur connect es otra red social mediante la cual pequeños empresarios pueden compartir experiencias, opiniones y consejos, además de hacer conexiones profesionales entre los usuarios de esta red.

Biznik es una comunidad de emprendedores y pequeños empresarios que se dedican a ayudar a cada uno de ellos a tener éxito en sus labores. Se basa en el principio de que la colaboración es mejor que la competencia y es utilizada para compartir ideas.

Para concluir esta sección, la red social española, *Tuenti* es un medio de comunicación móvil y de carácter social, que permite al usuario registrado crear su propio perfil, añadir a otros usuarios como amigos e intercambiar eventos, mensajes, fotos, vídeos o páginas

web. Además, ofrece un servicio de chat, individual y grupal, video chat. Esta red social es una de las pocas de acceso restringido a la que se accede solo por invitación de un usuario ya registrado y tiene un requisito de edad mínima de 14 años, como medida de seguridad.

2.4 Delitos cometidos en redes sociales

Con el auge de las redes sociales se ha ido incrementando el número de personas que hace uso de estas y esto ha conllevado que usuarios con fines delincuenciales participen de estas redes con el objeto de cometer delitos.

Los delitos cometidos dentro de las redes sociales han ido en crecimiento, para lo cual se hace necesario hacer un resumen de los que se considera que más se cometen en la actualidad. Entre los ataques más comunes se encuentran la suplantación de la identidad de las personas, enlaces falsos que conducen a un virus o perfiles *hackeados*. No obstante, muchas veces los propios usuarios desconocen si fueron víctimas de estos delitos.

Como se mencionó anteriormente en el presente trabajo de tesis, el delito de *phishing* es el utilizado por los *hackers* para adueñarse de datos y así poder usar esa información, por ejemplo, en sitios de compras. Respecto al delito de *phishing*, es importante mencionar que fue uno de los primeros en aparecer en redes sociales por medio de un enlace falso en facebook, en el cual un robot generaba un evento simulado que era enviado a los usuarios para que confirmaran su asistencia a tal evento, pero solo se

trataba de un link engañoso que obligaba a completar datos personales que podían ser utilizados de cualquier manera ilícita en internet.

El delito de robo de identidad, es uno de los que más afectan la vida personal de los usuarios. Como he dicho anteriormente, las redes sociales han sufrido un progreso inimaginable, de manera que permiten que millones de personas estén continuamente comunicadas en un momento determinado. El robo de identidad en las plataformas sociales más utilizadas se ha elevado en los últimos años. En muchas ocasiones suele venir relacionada con otro tipo de acciones delictivas como amenazas, coacciones, chantajes o estafa.

Mediante el robo de identidad la persona que efectúa dicho delito, obtiene o se apodera de datos, informaciones o documentos de un tercero y los maneja para hacerse pasar por el sujeto pasivo en muy diversos ámbitos de la vida cotidiana.

El robo de identidad, también llamado, suplantación de identidad, es un medio adecuado para cometer una multiplicidad de conductas delictivas. Frecuentemente, este delito se utiliza en relación a delitos de inmigración ilegal o terrorismo, pero también se puede cometer con el fin de lograr otros ilícitos menos graves, como fraudes o delitos contra el honor de una persona.

El robo de identidad, si bien existe desde antes de la creación de las redes sociales, lo cierto es que este tipo de delitos ganaron terreno en los últimos años de la mano de estas redes. Este se efectúa, mayormente cuando se recibe un correo electrónico con una

invitación para poder ver una determinada cosa, sin embargo, es una artimaña que aparenta ser una página real pero que en realidad se usa para captar datos personales, como correos electrónicos y contraseñas.

En el delito de robo de identidad, mayormente, se comete con la finalidad de obtener un enriquecimiento económico a costa de otras personas. En este tipo de casos es imperativo que además de obtener los datos de otro, dichos datos sean empleados en alguna operación de contenido económico que llegue a causar de manera efectiva un menoscabo en el patrimonio de la persona a la que se suplanta. De modo que al cometer este delito, el bien jurídico más dañado normalmente es el interés económico-patrimonial de la persona cuya identidad se suplanta.

En el ámbito de las redes sociales, el robo de identidad es usado en muchas ocasiones para dañar la privacidad y el honor de las personas, mediante el cual, se publican datos sobre las mismas que puedan afectar su reputación o a su entorno de intimidad. La mayoría de las veces, estas conductas son llevadas a cabo por personas menores de edad, que no son conscientes de las consecuencias jurídicas que pueden tener esos actos.

Las redes sociales, además de las conductas recién mencionadas en este apartado, han sido invadidas por acosadores. El acoso es uno de los delitos más cometidos y de más gravedad y posiblemente, el cometido con mayor frecuencia. Para que se pueda considerar acoso, una de las exigencias más importantes que se ha de observar a la hora de diagnosticar un caso es que la agresión sea repetida y no un hecho aislado.

"El acoso supone la realización de comportamientos amenazantes que una persona ejecuta de forma reiterada sobre otra."[10] Por lo que el acoso, es una conducta que se lleva a cabo con el propósito de mantener cualquier tipo de contacto de forma persistente, obsesiva y compulsiva que derive en daños psíquicos y morales graves para el acosado.

Para finalizar este delito se debe resaltar que "las conductas de acoso tienen un objetivo claro: la dominación del sujeto que realiza el acoso sobre la víctima. Sin embargo podemos encontrarnos, dentro de este objetivo de dominación, con finalidades distintas: una finalidad sexual (es el caso del grooming), una finalidad de hostigamiento (stalking o ciberacoso) o una finalidad de venganza personal."[11] Con lo cual, se demuestra que derivado del acoso, no se puede establecer un solo propósito, al que este pretenda dañar.

[10] Sanz Rodríguez, **Op. Cit**. Pág. 19.
[11] **Ibid**.

CAPÍTULO III

3. Los bienes jurídicos tutelados

A medida que se extiende el uso de internet, ha aumentado el riesgo de su uso con fines delincuenciales. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, dañando diferentes bienes jurídicos.

Antes de conocer los bienes jurídicos que se violan en las redes sociales, es necesario estar informado de los bienes jurídicos en general. Para lo cual, es importante mencionar que el objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Puesto que constituye la razón de ser del delito y no suele estar expresamente señalado en los tipos penales.

El bien jurídico cumple funciones de gran importancia para las ciencias penales. Entre ellas, la afectación de un bien jurídico permite sustentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito insoslayable para el ejercicio del *ius puniendi* por parte del Estado.

Tanto la importancia de un bien jurídico como su grado de afectación sirven de criterio para establecer por parte de los legisladores las penas proporcionales en base al daño causado. Por ello, el bien jurídico permite determinar el injusto específico de cada delito al sistematizar los tipos penales que conforman la parte especial de los códigos penales

y orientar la interpretación de los comportamientos que ellos reprimen. De ahí la importancia de puntualizar cuál es el bien jurídico protegido por un determinado delito.

Dentro de la doctrina penal, el concepto de bien jurídico ha cumplido hasta hoy importantes funciones en la dogmática penal, ya que ha contribuido para la clasificación de los delitos, y como elemento de base y límite al orden penal. Así pues, el bien jurídico ha servido al liberalismo como barrera contenedora del poder punitivo del Estado.

El bien jurídico tal y como se lo conoce en la actualidad es de vital importancia que preexiste al ordenamiento normativo. Estos no son creados por el derecho sino que este los reconoce y mediante ese reconocimiento, es que los bienes son protectores de los ciudadanos.

La idea de que el bien tutelado es un interés reconocido por el ordenamiento jurídico ha llevado a una variedad de autores a establecer que el derecho penal no crea bienes jurídicos, sino que se limita a sancionar con una pena determinadas conductas que lesionan ciertos bienes de alguna forma. El bien jurídico es creado por el derecho constitucional y en algunas ocasiones por el derecho internacional.

En el ámbito del derecho penal, el bien jurídico ha dado al principio de exclusiva protección de bienes jurídicos, mediante el cual solo es legítima aquella norma destinada a proteger bienes jurídicos. Con lo que se prescinde cualquier tipo de sanción respecto de pensamientos o comportamientos que no dañen a otro. Derivado de lo anterior y de la evolución del derecho penal moderno, se ha impulsado la idea que el legislador amenaza

con pena las acciones que vulneran o ponen en peligro determinados intereses de una sociedad determinada, como lo son: la vida, la libertad, el patrimonio, entre otros que son intereses o finalidades de la sociedad que el legislador quiere proteger conminando a quienes los ataquen con la aplicación de una pena, de tal forma que tales intereses se convierten, a través de su reconocimiento en el orden jurídico positivo, en bienes jurídicos.

Proveniente del desarrollo del derecho penal se puede distinguir dos clases de bienes jurídicos: los individuales y los colectivos. Los primeros son de titularidad o sirven a una persona determinada o a un grupo de personas determinadas. Por su parte, los bienes jurídicos colectivos son de titularidad o sirven a la generalidad de las personas que integran el conglomerado social. Estos también, constituyen presupuestos para la satisfacción de necesidades individuales.

La afectación de bienes jurídicos individuales influye directamente en el libre desarrollo de una persona determinada o de un grupo de personas determinadas, mientras que la afectación de bienes jurídicos colectivos incide indirectamente en el libre desarrollo de todas las personas. En este orden de ideas, para que el concepto de bien jurídico condicione y limite al *ius puniendi*, se requiere que la afectación de bienes colectivos incida, de alguna manera, en intereses concretos de personas determinadas, aunque estos sean intangibles.

Sobre los bienes jurídicos, la doctrina penal ha venido progresando; en la antigüedad se atendía a la definición formal del tipo y a su ubicación en los distintos códigos penales,

en la contemporaneidad, los bienes jurídicos se contemplan desde un punto de vista de la política criminal, en razón de su provecho y función, para el desenvolvimiento de la vida social.

3.1 Definición de bienes jurídicos

A lo largo de la historia del derecho penal, los bienes jurídicos siempre fueron objeto de discusión en la doctrina penal, sin embargo, en la actualidad, es mayoritario el criterio que sostiene que el derecho penal se encarga de la protección de bienes jurídicos, por lo que esta área del derecho, tiene una doble función: protege bienes jurídicos y fines públicos de prestación imprescindibles.

Es importante mencionar que los bienes jurídicos constituyen un límite al *ius puniendi*. El bien jurídico, desde una función utilitarista, se identifica con la validez de la norma. Desde esa perspectiva, el bien jurídico es entendido como un valor inherente a la persona humana de carácter universal, material o ideal, pero real, y que se lo describe como la relación de disponibilidad de un sujeto para con un objeto, siempre dentro del ámbito jurídico.

Así pues, el bien jurídico ha de entenderse como valor ideal del orden social jurídicamente protegido, en cuyo mantenimiento tiene interés la sociedad y que puede atribuirse, como su titular, tanto al particular como a la colectividad. El bien jurídico, entonces, es el bien ideal que se incorpora en el concreto objeto de ataque; y es lesionable solo dañando los respectivos objetos individuales de la acción que se realiza.

3.2 Bienes jurídicos en las redes sociales

En la actualidad, todavía, es complicado encontrar suficiente información proveniente de la doctrina penal, referente a los bienes jurídicos tutelados violentados en las redes sociales fundamentalmente porque constituyen vejámenes jurídicos relativamente nuevos.

Antes de entrar a conocer en profundidad, el tema sobre los bienes jurídicos que se violentan en las diferentes redes sociales, es importante hacer mención de lo referente a criminalidad informática. Este término suele utilizarse para hacer referencia a comportamientos delictivos que inciden, directamente, en un sistema informático. Por su parte, el concepto de cibercrimen suele apuntalarse para aludir a la criminalidad informática en un sentido amplio llevada a cabo a través de internet.

La criminalidad informática abarca tres ejes sobre los que se estructuran los delitos informáticos, es decir, aquellas conductas que implican destrucción o inutilización de datos o programas de sistemas informáticos, que frecuentan asociarse con el sabotaje informático; los comportamientos que suponen obtención o acceso indebido de datos o programas de sistemas informáticos, que suelen enlazarse con el espionaje informático; y las que implican alteración o manipulación de datos o programas de sistemas informáticos, que suelen ligarse con el fraude informático.

El presente apartado centrará su atención a los bienes jurídicos que se coaccionan a través de las redes sociales, puesto que estos ponen en peligro la confidencialidad, la

integridad y la disponibilidad de los sistemas, redes y datos informáticos, no solo de personas individuales, sino también, de grande compañías a nivel mundial.

Son indiscutibles los grandes beneficios que la introducción de las redes sociales ha producido, en términos de un mejor aprovechamiento de energías y recursos. Sin embargo, la creciente importancia que han adquirido estas redes ha provocado la vulnerabilidad de las sociedades y de las organizaciones que las utilizan, tomando en cuenta que son muchos los abusos que se pueden cometer al hacer un mal uso de estas.

Con el paso de los años, las redes sociales se han convertido en un medio de comunicación realmente efectiva para sus usuarios. Debido a esto, muchas personas consideran que tienen el derecho de comentar en las publicaciones, sin importarles el vocabulario utilizado, o los efectos que dichos comentarios pueden provocar. Por ello, en cuantiosas ocasiones, se suele incurrir en acciones que están penalizadas por la ley.

Ya entrados en materia, dentro de los delitos que se cometen en las redes sociales, se puede decir que a falta de una protección específica para estos delitos, la tendencia es que la protección a los bienes jurídicos, se haga desde la perspectiva de los delitos tradicionales, con una interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas legales originadas por los novedosos comportamientos delictivos. Por lo que, sin una ley específica sobre delitos en redes sociales los bienes jurídicos protegidos, serán los mismos que los delitos interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Por otra parte, en la doctrina penal, surge una vertiente que presume que la emergente sociedad de la información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección. Tomando en consideración la multiplicidad de diferencias entre la propiedad tangible y la intangible.

Según la nueva corriente penal se debe hacer una diferenciación entre los delitos cometidos en redes sociales y los de naturaleza común, puesto que los bienes jurídicos cibernéticos no pueden ser tratados de la misma forma en que se aplica la legislación actual a los bienes corporales, aunque dichos bienes tienen un valor intrínseco compartido.

La protección de los bienes jurídicos debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de detrimento. Así, una conducta solo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

3.3 Bienes jurídicos violentados en redes sociales

En la interacción que se lleva a cabo en las redes sociales suelen violarse una multiplicidad de bienes jurídicos tutelados, como consecuencia de acosos, insultos y burlas, entre otros, sin embargo, dentro del presente tema de investigación se mencionaran los más comunes y de mayor impacto en la sociedad, especialmente en los jóvenes.

Como consecuencia del flujo de información que se maneja en las redes sociales se cometen vejámenes en contra de la intimidad de las personas, sean estas o no usuarios de dichas redes.

La intimidad se refiere al conjunto de pensamientos, sentimientos o relaciones propias de una persona y que a la vez son la expresión de lo más profundo e interior de un individuo. La intimidad es una necesidad del ser humano, debido a que para que el hombre se desarrolle y geste su propia personalidad e identidad, es importante que disfrute de un área que comprenda diversos aspectos de su vida personal que se encuentre libre de la intromisión de extraños.

Se entiende por intimidad el conjunto de manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros. Se trata de tutelar la voluntad de una persona física o jurídica de que no sean conocidos determinados hechos que solo un determinado número de personas conoce. Además de esta vertiente negativa de la intimidad vista como un ámbito reservado, es decir, sin intromisiones ajenas, el tipo delictivo protege otra vertiente entendida como el derecho del ciudadano a controlar sus datos personales frente a los riesgos de conocimiento y utilización no consentidos generados en las sociedades modernas, especialmente a partir de su tratamiento informatizado.

Dentro de las redes sociales, la violación a la intimidad se efectúa cuando un desconocido accede a los sistemas informáticos de otro, para vulnerar los secretos que tenga

guardados o bien se acceda no estando autorizado para ello, a dichos secretos, usando medios ilegales de acceso, como puede ser vulnerando o accediendo a la contrasena mediante programas de *hacker* o pirata informático.

Otra variable de la violación a la intimidad es cuando un sujeto penetra en un sistema ajeno sin autorización y se mantiene en contra de la voluntad del titular o quien tenga derecho a excluirlo, sin que sea necesario que tome conocimiento de que está siendo invadido, ni que se acredite que el titular del derecho ha requerido al intruso su exclusión, sin haberlo conseguido.

En cualesquiera de las variables antes mencionadas, es suficiente con la intromisión para que el delito quede consumado, al igual que las acciones de acceder o facilitar a otro el acceso, y esto es así ya que no se trata de delitos de resultado, pues basta con realizar la acción del tipo porque se trata, de delitos formales, en otros términos, acceder, facilitar el acceso a otro, y mantenerse en el sistema informático contra la voluntad del titular del derecho.

En las redes sociales, también se puede cometer violaciones a la intimidad, cuando un profesional revela secretos ajenos, de los que tiene conocimiento por razón de su oficio o sus relaciones laborales; asimismo, al momento que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona.

En este segundo caso, se requiere que el autor realice la conducta de los tipos básicos con conocimiento y voluntad de difundir, revelar o ceder la información obtenida, es decir,

se exige dolo. Además, de exigirse de dolo de difundir revelar o ceder, la concurrencia de un especial elemento del injusto de tener conocimiento del origen ilícito de la información obtenida y divulgada. Esto da a entender que la violación a la intimidad y el delito de revelación de secretos se relacionan en muchos de sus elementos al momento de cometerse en las redes sociales.

Con el fin de terminar con estas prácticas de violación de la intimidad es necesario que la persona afectada o su presentante legal, en el caso de los menores de edad denuncien, el acto delictivo, ya que, a falta de denuncia es sumamente complicado para las autoridades encargadas de la investigación penal perseguir este tipo de delitos que lamentablemente se siguen cometiendo en la actualidad y cada vez más con mayor frecuencia. Sin embargo, en algunas legislaciones, se extingue la acción penal por el perdón del ofendido.

Para finalizar con el tema de violación a la intimidad en redes sociales, es importante mencionar que este se relaciona con la práctica denominada *sexting* mediante la cual se difunde, revela o cede a terceros imágenes o grabaciones audiovisuales en menoscabo de la intimidad de una persona.

Lo denominado como *sexting* puede ser definido como el envío, a través de internet o de un dispositivo móvil, mayoritariamente utilizando redes sociales, de mensajes de contenido sexual, producidos y protagonizados por el emisor, pero se tiene interés jurídico cuando este material es difundido a una persona o un grupo de personas sin la debida autorización del emisor del contenido.

Hasta el día de hoy, la difusión de *sexting* sin consentimiento del protagonista, no ha tenido presencia en la doctrina y en las legislaciones, no obstante, la importante exposición de la intimidad que se efectúa al emitir *sexting* sitúa al protagonista de los mensajes o imágenes en una situación de grave riesgo para sus derechos a la intimidad y a la propia imagen, en la medida en que los mensajes digitales recibidos pueden ser reenviados de forma indiscriminada por el receptor en las redes sociales. Por lo que la cultura de difusión de archivos ha hecho que este fenómeno deje de ser un hecho aislado para dar paso a una nueva forma de vulneración de la intimidad de las personas.

La intimidad de la persona es lesionada de forma grave cuando la difusión se produce con un alcance muy amplio y con publicidad. Es aquí cuando entran en juego las redes sociales, que tienen un amplio número de potenciales visitantes. Como consecuencia de esto, se debe mencionar que la violación a la intimidad no solo la comete quien difunde por primera vez la información, sino que también podría incurrir en él quien después contribuye a que se siga divulgando el contenido.

En las redes sociales, el honor es otro de los bienes jurídicos severamente violentados por los usuarios de estas redes. El honor es un bien jurídico que está íntimamente vinculado a la personalidad de la persona y, a la vez, está muy influenciado por las valoraciones culturales en cada sociedad, de esta forma resulta muy complicado concretar un concepto del tal bien jurídico. Como consecuencia de su carácter inmaterial y por la diversidad de sentidos extrajurídicos que posee histórica y socialmente. Por ello los problemas que presenta su tutela jurídica se originan, más en la falta de acuerdo sobre su contenido que en la falta de idoneidad o en la peculiaridades del instrumento de

tutela. El bien jurídico protegido por este tipo penal es el honor, concepto que puede entenderse desde dos perspectivas: subjetiva, la cual trata de la representación que el sujeto tiene de uno mismo; y una objetiva que es el prestigio o reputación de cara al público o a la sociedad en general.

De acuerdo a la doctrina penal, se exige como condición necesaria para entender vulnerado el derecho al honor que quede afectada la buena reputación de la persona. En todo caso debe tenerse presente la noción de dignidad de la persona a la hora de configurar el bien jurídico. En este orden de ideas, un sector de la doctrina explica el contenido de este bien jurídico de modo objetivo y en concordancia con derechos fundamentales reconocidos como es la dignidad de las personas y el libre desarrollo de su personalidad constituyendo, esto último, el enlace entre los aspectos interno y externo del honor.

El honor a las personas es violentado por ataques inmediatos a la dignidad de la estas, es decir, a su autoestima y fama. Aunado a esto, nace un problema en relación a la dignidad de las personas, dado que, las distintas posiciones y situaciones de los individuos hacen que el grado de respeto a esa dignidad tenga que ser determinado de forma circunstancial. En este orden de ideas, el trato adecuado a la dignidad de un niño no lo es para una persona adulta y viceversa. Lo que puede resultar lesivo para la dignidad de un particular puede no serlo para una personalidad pública.

Trasladando este bien jurídico a las redes sociales, se puede decir que este sufre vejámenes cuando por algún motivo un usuario de estas, publica o difunde material

imputando falsamente un delito de acción pública, cometiendo calumnia; y al momento de deshonrar, provocar desprecios o descredito en contra de otra persona sin importar si esta es o no usuario de redes sociales.

3.4 Sistemas informáticos como objeto de tutela penal

Un sistema informático es un conjunto de elementos que hace posible el tratamiento automático de la información y que permite almacenarla y procesarla. Este sistema se integra de tres componentes que son: componente físico, el cual está conformado por los aparatos electrónicos y mecánicos que realizan los cálculos y el manejo de la información; componente lógico es el que trata de las aplicaciones y los datos con los que trabajan los componentes físicos del sistema; y el componente humano, que está compuesto tanto por los usuarios que trabajan con los equipos como por aquellos que elaboran las aplicaciones.

Los sistemas informáticos en la actualidad son un tema de discusión en la doctrina penal, puesto que algunos autores mantienen la idea que los delitos informáticos protegen a estos sistemas per se y no se permite superar la amplitud atribuidas a la tutela de la información, la cual es contenida en un sistema informático. En este orden de ideas, se mantiene el debate sobre la supuesta protección a estos sistemas y otros bienes jurídicos relacionados, como: como la propiedad o el patrimonio.

Con lo expresado en el párrafo anterior, se debe resaltar que el sistema informático es tomado dentro del derecho penal como un bien de valor económico que se encuentra

bajo el poder de disposición de una persona y respecto del que su titular tiene una relación reconocida o al menos tolerada por el derecho. Por otro lado se mantiene la idea que el sistema informático es un bien jurídico puesto que al ser violentado se atenta contra la propiedad intelectual. "Además, la tutela penal del *software* parece mezclar dos conceptos que deben diferenciarse, a saber, el objeto material y el objeto jurídico del delito. En ese orden de ideas, es posible que un *software* sea objeto material de determinados delitos informáticos, del mismo modo que un documento puede ser objeto material de una falsedad o una cartera puede ser objeto material de un hurto. Pero con ello todavía nada se ha dicho sobre el bien jurídico protegido por esos comportamientos."[12]

Derivado de lo anterior, queda claro que la doctrina penal, hasta el momento no ha logrado unanimidad en cuanto a determinar el bien jurídico a proteger en el mundo cibernético.

[12] Mayer Lux, Laura. **El bien jurídico protegido en los delitos informáticos**. Pág. 242.

CAPÍTULO IV

4. Redes sociales y plataformas digitales como medios para la comisión de delitos y su falta de tipicidad en el sistema jurídico penal en Guatemala

En la administración pública guatemalteca, el avance tecnológico ha tenido un desarrollo relativamente lento, a nivel gubernamental a duras penas se ha propiciado el manejo de los medios electrónicos, solo en determinadas instituciones se ha visto un avance plausible en cuanto a materia informática.

En Guatemala a los delitos informáticos no se les ha dado la importancia que les corresponde, no porque estos no se hayan cometido, sino por desconocimiento de los mismos. Tomando en consideración que además de delincuentes informáticos propiamente tales, otros delincuentes han surgido como consecuencia de dichos delitos, por mencionar algunos: los pedófilos que, usualmente usando redes sociales buscan generar relaciones de confianza con menores de edad, para luego aprovecharse de ellos hasta llegar a secuestrarlos u asesinarlos; proxenetas, traficantes de armas, estafadores, defraudadores, falsificadores, secuestradores, sicarios e incluso hasta terroristas.

Derivado de los hechos delincuenciales en el ámbito informático, los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que han causado a la sociedad. No obstante, si bien es cierto existe un esfuerzo por parte de los países para tratar de erradicarlos, no existe en la actualidad, un consenso de cómo deben ser atacados. Por ese motivo se

hace indispensable que se continúe trabajando para llegar a la unificación de los criterios y de esta forma, sentar las bases con la finalidad de poder tener una legislación coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente y sustentándose en doctrina informática.

Teniendo en consideración que los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada es imperioso que se logre un consenso a nivel mundial o regional. Lamentablemente, aún faltan acuerdos acerca de qué tipo de conductas deben constituir delitos informáticos; en muchos casos faltan definiciones legales de tales conductas delictivas; no existe un criterio unificado de cómo se deben adecuar las leyes procesales con la finalidad de lograr una investigación objetiva y eficaz; y a una variedad de delitos no se les ha dado el carácter de trasnacionales con el fin de perseguirlos.

En el ámbito internacional, son pocos los países que cuentan con una legislación apropiada. Entre estos están: Chile, Argentina, Holanda, Estados Unidos, Alemania, Austria, Gran Bretaña, Francia y España. En el caso de Guatemala, la reacción fue tardía, derivado de factores tales como: falta de información, falta de claridad en la implementación de seguridad informática en las empresas del país, ausencia de políticas claras sobre seguridad informática, falta de conciencia en la utilización de los diferentes sistemas de flujo de información, y poco uso de herramientas de análisis y control.

Los delitos informáticos en Guatemala, solamente se encuentran regulados por el Decreto 33-96 del Congreso de la República de Guatemala el cual entró en vigencia el

tres de julio de 1996 y mediante el cual se reformó el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, específicamente adicionando los Artículos 274 A al 274 G, los cuales tratan sobre:

Destrucción de registros informáticos

Alteración de programas

Reproducción de instrucciones o programas de computación

Registros prohibidos

Manipulación de información

Uso de información

Programas destructivos.

Lo anterior evidencia la poca defensa jurídica que poseen los guatemaltecos al enfrentar cualquier delito informático y demuestra la importancia de la creación de una ley que tipifique la mayor cantidad de hechos delincuenciales que se cometen usando internet.

Desafortunadamente, en la legislación de Guatemala, no ha existido interés por crear una política criminal informática, solamente se ha intentado tipificar los delitos informáticos mediante la iniciativa 4055 del 2009, en la cual se ajustaba de mejor manera a la actualidad estos delitos, puesto que se tomaba como referencia las diferentes legislaciones y convenios internacionales en materia penal informática.

La iniciativa de ley en mención es de suma importancia para la sociedad guatemalteca, puesto que hacia una clasificación de los tres grupos de delitos más importantes: delitos

contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos relacionados con la propiedad y autenticidad; y los delitos relacionados con el contenido. Además, establecía un marco regulatorio sobre los posibles usos indebidos que perjudicaran transacciones y comercio electrónico. Asimismo, contemplaba las definiciones legales propias para el tema del delito electrónico y desarrollaba la referente a sancionar los actos de *hacking, cracking, phishing, smishing, vishing* y pornografía infantil.

El estudio de las consecuencias de los delitos informáticos es realmente importante para determinar qué acciones son las correctas a tomar ya que, a través de este estudio se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos y con objeto de prever las acciones que disminuyan estos hechos, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos y por la falta de denuncias por parte de los afectados, como consecuencia de la ignorancia de la ley, y que por ende, provoca un grado sumamente alto de impunidad.

A falta del estudio antes explicado, en Guatemala ha sido materialmente imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de estos no son descubiertos o no son denunciados a las autoridades responsables de la investigación penal y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto

pudiera ocasionar a su empresa y las consecuentes pérdidas económicas que acarrearían otro tipo de consecuencias en perjuicio de esta y de sus trabajadores.

Con la finalidad de contrarrestar los delitos informáticos se debe de proporcionar por parte del Estado de Guatemala las condiciones que revistan de protección jurídica a los guatemaltecos, teniendo en cuenta que la informática y principalmente los sistemas informáticos pueden proporcionar datos e informaciones sobre millones de personas, en aspectos tan fundamentales para el normal desarrollo del país y funcionamiento de diversas actividades como bancarias, financieras, tributarias, entre otras y de esta manera facilitar un ordenamiento jurídico-informático.

Por lo antes expuesto, los órganos institucionales guatemaltecos deben reconocer que para conseguir una prevención efectiva de la criminalidad informática se requiere, elementalmente, como primer presupuesto, un estudio exhaustivo de las necesidades de protección y de las fuentes de peligro que brinde protección contra todo tipo de delitos informáticos.

En conjunto con lo establecido en el párrafo anterior, como segundo lugar, la difusión de las posibles conductas ilícitas derivadas del uso de las computadoras y demás aparatos electrónicos, alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, vinculado con una legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas dentro del territorio de Guatemala.

Lo anterior es sumamente importante para la población guatemalteca. Si bien es cierto en Guatemala todavía no han existido delitos informáticos de gran impacto para la sociedad, es imperioso prevenir con una normativa que se ajuste a las bases ya establecidas por la comunidad internacional y aceptadas por varias legislaciones, puesto que seguramente la delincuencia informática irá en crecimiento en la medida en que la tecnología avance y los delincuentes encuentren formas cada vez más eficaces de cometer delitos de mayor perjuicio económico, tales como: la obtención de información ilegal y la filtración de datos.

En conclusión, para disminuir los efectos de los delitos informáticos o para evitar la comisión de estos el Estado de Guatemala, por medio de sus tres organismos debe desplegar las herramientas necesarias para estimular la denuncia de estos delitos y por ende, promover la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informático en el territorio de Guatemala.

4.1 Efectos de los delitos informáticos en personas individuales

Derivado del fracaso de la iniciativa de ley 4055, que disponía tipificar lo referente a los delitos informáticos que ocurrieren en Guatemala, protegiendo a las personas individuales y jurídicas; brindando seguridad informática, las personas dentro del territorio de Guatemala están sin una protección en este ámbito que les asegure o proteja, principalmente los sistemas informáticos y las bases de datos sin importar que estos pertenezcan a personas individuales o jurídicas.

Acerca de los efectos en las personas individuales de los delitos informáticos es loable mencionar los delitos que conllevan un detrimento económico para los guatemaltecos afectados, es decir, la estafa electrónica y *phishing*.

La estafa electrónica consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. Mediante este delito se suele sustraer dinero de las bancas electrónicas de los sujetos pasivos o se realizan transferencias de tarjetas de crédito sin la debida autorización del titular de estas.

El delito informático de estafa electrónica es un fenómeno delictivo que en los últimos lustros ha ido en crecimiento y cada vez más se realiza de diferentes formas con la finalidad de persuadir al afectado y escapar de las investigaciones penales. Este delito tiene como objetivo causar daños, provocar pérdidas o incluso impedir el uso de información de terceros.

Consecuencia de la falta de campañas de información por parte del Estado, los guatemaltecos son víctimas de este tipo de estafas por el desconocimiento de sus derechos y por la falta de legislación aplicable a esta forma de delitos.

El delito de *phishing* por su parte, también conlleva un detrimento económico, por lo general. Este se realiza mediante la captación de forma ilegal de datos confidenciales, por el desconocimiento de las personas respecto al mismo, ya que es uno de los más usados por los delincuentes cibernéticos para estafar y obtener información confidencial

de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. En Guatemala el *phishing* es cometido, mayormente, desde el extranjero usando técnicas de ingeniería social y haciéndose pasar por una persona de confianza el estafador simula ser una persona o una empresa de renombre por medio de un correo electrónico o algún tipo de mensaje instantáneo o hasta por medio de llamadas telefónicas

No solamente en Guatemala, sino a lo largo del mundo electrónico el phishing es cometido por la modalidad comúnmente denominada: *deceptive phishing* a través de un correo electrónico engañoso en el que se suplanta a una empresa o institución de prestigio. El receptor pulsa en el enlace contenido en el mensaje, siendo desviado de manera inconsciente a un sitio web fraudulento y causando un perjuicio al sujeto pasivo del phishing.

4.2 Efectos de los delitos informáticos en personas jurídicas

Las personas jurídicas, respecto a los delitos informáticos pueden ser víctimas y a su vez victimarios. Tomando en cuenta que requieren de los servicios en muchos casos de hackers con la finalidad de proteger sus sistemas informáticos, sin embargo, en algunas ocasiones esas habilidades de los hackers es utilizada para sustraer información de competidores.

Las personas jurídicas pueden cometer una variedad de delitos informáticos, siempre que la persona física que lo cometa sea miembro de la organización o la represente de

cualquier forma; y que la entidad reciba algún beneficio directo o indirecto por el hecho en sí y que no cuente con las medidas adecuadas para prevenir la comisión de ese delito en concreto. En este orden de ideas, uno de los delitos informáticos que puede cometer una persona jurídica es el de daños informáticos.

Los daños informáticos se producen al momento de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Estas técnicas, se cometen usando sabotajes informáticos por medio de: virus, gusanos y bombas lógicas o cronológicas.

El virus es una serie de claves programáticas que pueden conectarse a los programas legítimos y propagarse a otros programas informáticos. Además, un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método llamado caballo de troya.

Los gusanos son aquellos que se producen de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En contraposición de los virus, el gusano es benigno, es decir, es la antítesis de aquel. No obstante, el ataque de un gusano puede ser tan grave como el ataque de un virus.

Por su parte, lo que en informática se conoce como bombas lógicas o cronológicas son utilizadas para destruir o modificar datos; estos requieren de conocimientos más especializados que los virus y los gusanos.

Las bombas lógicas son utilizadas por las personas jurídicas puesto que, son difíciles de detectar antes de ver sus efectos; por ese motivo, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su efecto puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Las personas jurídicas pueden incurrir en responsabilidad penal, también por el simple acceso no autorizado a un sistema informático ajeno, o el hecho de mantenerse en él contra la voluntad de quien tenga el derecho de poder excluir del mismo al intruso. El delito se consuma con el simple acceso, sin necesidad de ningún ánimo especial, ni de que vaya seguido de daños, fugas de datos o revelación a terceros de lo conocido.

Lo anterior da a entender que lo que muchas personas toman como entretenimiento, constituye este tipo de delito informático. Esto derivado de la protección jurídica que la norma pretende conceder al representar una primera línea defensiva penal frente a ataques en contra de bienes jurídicos que pueden revestir un daño con consecuencias lamentables.

La protección jurídica que acarrea esta tipificación es más que todo para proteger a empresas u organismos de robo de claves, mediante el uso de sistemas de *Spyware*; o los accesos potenciales de antiguos empleados de una compañía por resentimiento o por estar vinculados a sus competidores, si conservan claves de acceso o conocen el modo

de obtenerlas, cometiendo no solo el delito en cuestión sino también competencia desleal entre personas jurídicas. Como se ha evidenciado dentro del presente apartado, los delitos de daños informáticos y el de acceso ilegal, activan la responsabilidad penal de las personas jurídicas cuando se comete en el seno de estas y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, estando autorizados para tomar decisiones en nombre de la persona jurídica u ostentando facultades de organización y control dentro de la misma o incluso por sus mismos empleados.

4.3 Consecuencias de los delitos informáticos en el Estado

La magnitud de los delitos informáticos es tal que hasta el Estado puede ser una de sus víctimas, por la comisión de una diversidad de estos delitos, principalmente por espionaje, a través del cual se obtiene acceso a sistemas informáticos gubernamentales con información de los ciudadanos. Mayormente, este delito se utiliza para obtener información privilegiada industrial o comercial que no debe salir de la órbita de su titular o encargado de manipular.

El espionaje es "un delito que comete quien, sea nacional o extranjero, con disimulo o bajo disfraz, procura el conocimiento de secretos de Estado, a fin de revelarlos a una potencia extranjera, lo que pone en peligro la paz o la seguridad de la nación. Naturalmente, para el país beneficiado es acto loable y muy bien remunerado."[13] De

[13] Ossorio, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. Pág. 380

manera que el espionaje es aquel "delito en que incurre quien, con la obtención y revelación de informes secretos, de carácter militar sobre todo, perjudica a un bando o país."[14]

El espionaje se lleva a cabo, principalmente por *adwares*, los cuales consisten en programas que recogen o recopilan información acerca de los hábitos de navegación del usuario o en este aspecto de algún funcionario público. El *adware* es un tipo de *software* que suele aparecer en ventanas emergentes o en una barra de herramientas en las computadoras. Este *software* realiza un seguimiento de los sitios que se visitan y hasta es capaz de registrar las pulsaciones del teclado, con la finalidad de obtener todos los detalles de la futura víctima.

El delito de espionaje también se comete por programas de acceso remoto que permiten el acceso de un tercero a un ordenador o cualquier dispositivo en el cual se pueda almacenar información, para un posterior ataque o alteración de los datos. Estos programas se ejecutan desde cualquier lugar con conexión a internet, siempre que se cuente con los requisitos necesarios con el fin de utilizar los datos, aplicaciones y recursos que se obtengan de manera remota sin que el afectado sepa que está siendo víctima de espionaje. Lo cual conlleva que este tipo de delito informático sea sumamente difícilmente de ser descubierto o perseguido ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito.

---

[14] Universidad Autónoma de Encarnación. **Diccionario jurídico elemental**. Pág. 123.

4.4 Proyecto de ley

PROYECTO DE LEY DE DELITOS INFORMÁTICOS COMETIDOS EN REDES SOCIALES Y PLATAFORMAS DIGITALES

DECRETO NÚMERO_____

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO

Que de conformidad con la Constitución Política de la República de Guatemala, es obligación del Estado brindar seguridad o certeza jurídica. De tal obligación es imperiosa la creación de mecanismos necesarios para regular la conducta de los habitantes de la república y proteger y sancionar los actos o abusos que se cometan en cualquier ámbito de interacción social.

CONSIDERANDO

Que es evidente que la evolución de las tecnologías de la información y la comunicación, así como de las actividades humanas vinculadas a ellas como la difusión de contenidos y las transacciones comerciales y por ende, las conductas antijurídicas se han incrementado, hacen inaplazable una revisión completa y minuciosa de sus estructuras y contenido con la finalidad inevitable de actualizarla a esta nueva realidad.

CONSIDERANDO

Que el proyecto de la actualización informática aborda no solo las normas penales materiales que tipifican y sancionan las acciones antijurídicas que atentan contra los derechos de las personas en materia informática, sino que profundiza también en algunas normas de carácter procesal penal, que faciliten y hagan más eficaz la investigación y sanción de dichos delitos.

CONSIDERANDO

Que es indispensable la aprobación de una ley especial que contenga disposiciones que tiendan a proteger integralmente a las personas, sistemas informáticos y bases de datos, a fin de garantizar certeza jurídica en todas las áreas cibernéticas.

POR TANTO

En ejercicio de las atribuciones que le confiere la literal a) del Artículo 171 de la Constitución Política de la República de Guatemala

DECRETA

La siguiente:

LEY DE DELITOS INFORMÁTICOS COMETIDOS EN REDES SOCIALES Y PLATAFORMAS DIGITALES

TÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto de la ley. La presente ley tiene por objeto prevenir y sancionar las conductas ilícitas que se lleven a cabo en las redes sociales y cualesquiera otras plataformas digitales que afecten bienes jurídicos de relevancia para el derecho penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la delincuencia que se desarrolla en el ámbito informático.

Artículo 2. Definiciones. A efectos de la presente ley se entiende por:

Redes Sociales: Son aquellas páginas web en las que los usuarios intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva.

Sistema Informático: Es cualquier dispositivo utilizado para la transferencia de información por la interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, entre los cuales se encuentren los sitios o páginas de internet.

Data (datos): Son todos los hechos, conceptos, instrucciones o caracteres simbolizados de una manera adecuada para que sean comunicados, transmitidos o procesados a través de medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

Información: Es el significado que se le asigna a la data utilizando los mecanismos conocidos y generalmente aceptados.

Procesamiento de datos o de información: Es la realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo de cualquier índole.

Hardware: Son los equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes del mismo.

Firmware: Es el programa o segmento de programas incorporados de manera permanente en algún componente del *hardware* que contribuyen a que este se puede desenvolver de forma adecuada.

TÍTULO II. DELITOS COMETIDOS EN REDES SOCIALES Y DEMÁS PLATAFORMAS DIGITALES

Artículo 3. Acceso ilícito. El que premeditada e ilegítimamente acceda a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

Artículo 4. Atentado contra la integridad de datos informáticos. Será castigado con pena privativa de libertad no menor de cuatro ni mayor de ocho años, el sujeto que ilegítimamente dañe, introduzca, borre, deteriore, altere, suprima o haga inaccesibles datos informáticos ajenos.

Artículo 5. Atentado contra la integridad de sistemas informáticos. El que utilizando tecnologías de la información o de la comunicación, inutilice, total o parcialmente, un sistema informático, impida el acceso a este o imposibilite su funcionamiento, será castigado con pena de prisión no menor de cinco ni mayor de ocho años.

Artículo 6. Favorecimiento culposo del daño. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena, con una reducción de una cuarta parte.

Artículo 7. Agravación. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 8. Responsabilidad de personas jurídicas. Cuando los delitos previstos en esta ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, estos responderán de acuerdo con su participación culpable. Además, la persona jurídica será sancionada con

multa que oscilará entre quinientos mil y un millón de quetzales, dependiendo del daño causado.

TÍTULO III. DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 9.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Será castigado con pena de prisión no menor de seis años ni mayor de doce, la persona que haciendo uso de internet u otro medio análogo contacte a un menor de edad para solicitarle u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él.

TÍTULO IV. DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 10. Hurto Informático. Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera o manipule de cualquier manera un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos de su poseedor, con el fin de procurarse un beneficio económico para sí o para otra persona, será sancionado con prisión de cuatro a seis años.

Artículo 11. Fraude Informático. Todo aquella persona que haciendo uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la información en ellos contenida, consiga insertar

instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a cinco años.

TÍTULO V. DELITOS CONTRA LA PRIVACIDAD DE LAS PERSONAS Y DE LAS COMUNICACIONES

Artículo 12. Violación de la privacidad de información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, información personal o sobre las cuales tenga interés legítimo, que estén incorporadas en una computadora o cualquier sistema que utilice tecnologías de información, será penada con prisión de cuatro a siete años sin perjuicio de cualquier otro delito cometido.

Artículo 13. Violación de la privacidad de las comunicaciones. Todo aquel sujeto que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, aunque no le genera un beneficio, será sancionada con prisión de cuatro a seis años.

Artículo 14. Revelación indebida de información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la información obtenidos por alguno de los medios indicados en los artículos 12 y 13, será sancionado con prisión de seis a diez años, así también, será penado con una multa entre cincuenta mil y doscientos cincuenta mil quetzales.

Artículo 15. Indemnización Civil. En los casos de sentencia condenatoria por cualquiera de los delitos previstos en esta ley, el tribunal impondrá una indemnización en favor de la víctima por un monto equivalente al daño causado más un cincuenta por ciento.

TÍTULO VI. DISPOSICIONES FINALES

Artículo 16. Vigencia. La presente ley entrará en vigencia treinta días después de su publicación en el diario oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, NOVIEMBRE DE DOS MIL DIECIOCHO.

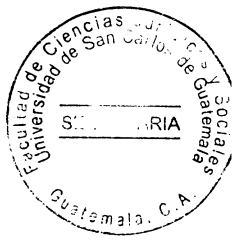
4.5 Beneficios de implementar la ley de delitos informáticos

Como se ha apreciado a lo largo de la investigación, la informática y el avance de la tecnología han sido de gran significación para la sociedad, pero este progreso ha conllevado una variedad de consecuencias negativas, no obstante, para frenar estas acciones negativas es imperiosa la creación de una ley de delitos informáticos, dado que de ella se derivarán los beneficios expuestos en este apartado.

La ley tiene entre sus beneficios esenciales desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la legislación guatemalteca,

además de organizar el sistema nacional de ciencia y tecnología y por ende definir los lineamientos que orienten políticas institucionales para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para generación, uso y circulación del conocimiento y de impulsar el desarrollo guatemalteco tecnológico.

Además de lo expresado en el párrafo anterior, la ley de delitos informáticos es de provecho para la sociedad guatemalteca, puesto que viene a proveer seguridad jurídica en materia informática por prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticas, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal-patrimonial, entre otros, que puedan ser afectados mediante la utilización de tecnología informática computacional, por lo que esta ley representa una garantía de condiciones mínimas para que las personas gocen del derecho a la libertad y desarrollo. Y con ello, la legislación de Guatemala se adaptará al ordenamiento penal internacional de esta materia específica.

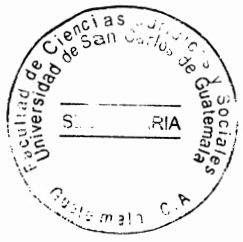

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SE RIA
Guatemala, C. A.

CONCLUSIÓN DISCURSIVA

Como consecuencia de la falta de regulación de delitos informáticos, en Guatemala se ha aumentado la comisión de estos, derivado del carecimiento de un cuerpo legal que preceptúe todo lo referente a estos actos antijurídicos, con lo cual, se expone que la entrada en vigencia de una ley penal informática es una urgencia, en el actual sistema jurídico, dado que, el ámbito informático se encuentra inmerso en un atraso que no permite un completo desarrollo, por ello, es una necesidad social que se cree y entre en vigencia tal ley con la finalidad de contar con fundamentos jurídicos en el territorio de Guatemala en relación a lo cibernético.

Es por lo anterior, la vital importancia de esta investigación en cuanto a las nuevas formas antijurídicas en internet y su caracterización, los sujetos que los realizan, la clasificación de las distintas formas en que se realizan, la legislación comparada que existe en esta materia, y la relevancia de la ley para regular estas maneras de delinquir y de cómo estas también influyen negativamente en la propiedad intelectual.

Por lo tanto, de esta investigación se deduce que es menester que el Congreso de la República de Guatemala, apruebe una ley penal informática que proteja a los ciudadanos y que faculte al Ministerio Público para contar con nuevas metodologías de investigación y además actualice a los miembros de los órganos jurisdiccionales con la intención primordial de lograr un juzgamiento objetivo de estos delitos y que como consecuencia se disminuyan los niveles de impunidad en el contorno informático.



BIBLIOGRAFÍA

CAMPOS, Pamela Ivette. **Delitos informáticos en México y sus formas de prevención.** Yucatán, México. (s.e.) 2016.

DEL PINO, Santiago. **Delitos informáticos: generalidades.** Quito, Ecuador. (s.e.) (s.f.)

HERNÁNDEZ, Leyre. **El delito informático**. San Sebastián, España: Ed. ISSN, 2009.

MAYER LUX, Laura. **El bien jurídico protegido en los delitos informáticos.** Santiago, Chile. (s.e.) 2017.

OJEDA, Jorge. **Delitos informáticos y entorno jurídico vigente en Colombia**. Bogotá, Colombia: Ed. Pontifica Universidad Javeriana, 2010.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. 32ª ed. Buenos Aires, Argentina: Ed. Heliasta S.R.L. 2000.

QUINTERO, René. **Delitos informáticos.** Caracas, Venezuela. (s.e.) 2002.

SANZ RODRÍGUEZ, Patricia. **Redes sociales y derecho penal**. Valladolid, España: Ed. Universidad de Valladolid. 2014.

TÉLLEZ VALDÉS, Julio. **Derecho informático**. 4ª ed. México D.F México: Ed. Universidad Autónoma de México (UNAM) 2008.

Universidad autónoma de encarnación. **Diccionario jurídico elemental**. Itapúa, Paraguay. (s.e.) (s.f.)

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Código Penal. Decreto 17-73 del Congreso de la República de Guatemala, 1973.