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

LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL GUATEMALTECO DECRETO 17-73 DEL CONGRESO DE LA REPÚBLICA DE GUATEMALA PARA PREVENIR Y SANCIONAR LOS DELITOS QUE SE COMETEN EN LAS REDES SOCIALES DE INTERNET

DANIEL EMILIO TERCERO CONTRERAS

GUATEMALA, MAYO DE 2015

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

LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL GUATEMALTECO DECRETO 17-73 DEL CONGRESO DE LA REPÚBLICA DE GUATEMALA PARA PREVENIR Y SANCIONAR LOS DELITOS QUE SE COMETEN EN LAS REDES SOCIALES DE INTERNET.

TESIS

Presentada a la Honorable Junta Directiva

De la

Universidad de San Carlos de Guatemala

Por

DANIEL EMILIO TERCERO CONTRERAS

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, mayo de 2015

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

DECANO:	MSc.	Avidán Ortiz Orellana
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Licda.	Rosario Gil Pérez
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Mario Roberto Méndez Alvarez
VOCAL V:	Br.	Luis Rodolfo Aceituno Macario
SECRETARIO:	Lic.	Daniel Mauricio Tejeda Ayestas

TRIBUNAL QUE PRACTICÒ
EL EXAMEN TÈCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic.	Emilio Gutiérrez Cambranes
Vocal:	Lic.	Belter Rodolfo Mancilla Solares
Secretaria:	Lic.	Carlos Alberto Cáceres Lima

Segunda Fase:

Presidente:	Lic.	Daniel Mauricio Tejeda Ayestas
Vocal:	Lic.	Bernardo de Jesús Osorio Ramírez
Secretario:	Lic.	Arnoldo Torres Duarte

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis". (Artículo 43 del Normativo para la 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, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 20 de agosto de 2014.

Atentamente pase al (a) Profesional, EDDY AUGUSTO AGUILAR MUÑOZ, para que proceda a asesorar el trabajo de tesis del (a) estudiante DANIEL EMILIO TERCERO CONTRERAS, con carné 200518031, intitulado LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL GUATEMALTECO DECRETO 17-73 DEL CONGRESO DE LA REPÚBLICA DE GUATEMALA PARA PREVENIR Y SANCIONAR LOS DELITOS QUE SE COMETEN EN LAS REDES SOCIALES DE INTERNET.

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.

DR. BONERGE AMILCAR MEJIA ORELLANA
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 23 / 09 / 2014 f)

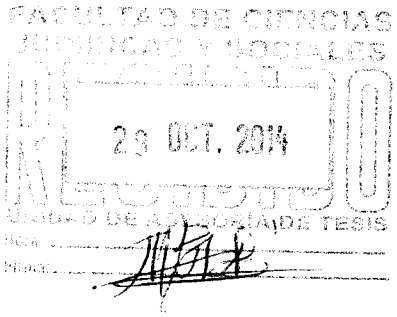
Asesor(a)
Lic. Eddy Augusto Aguilar Muñoz
ABOGADO Y NOTARIO

BUFETE CORPORATIVO
ABOGADOS, AUDITORES Y CONTADORES
11 Calle 4-52 zona 1 Ciudad de Guatemala
Edificio Asturias Oficina Número 4
Teléfono 2232-3916

Guatemala, 22 de octubre de 2014

Doctor:

Bonerge Amílcar Mejía Orellana
Jefe de la Unidad Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala



Dr. Mejía Orellana:

De manera atenta me dirijo a usted, para hacer de su conocimiento que he cumplido con la función de **ASESOR** de tesis del Bachiller **DANIEL EMILIO TERCERO CONTRERAS,** quien realizó el trabajo de tesis intitulado **"LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL GUATEMALTECO DECRETO 17-73 DEL CONGRESO DE LA REPÚBLICA DE GUATEMALA PARA PREVENIR Y SANCIONAR LOS DELITOS QUE SE COMETEN EN LAS REDES SOCIALES DE INTERNET",** manifestando las siguientes opiniones:

a. En relación al contenido científico y técnico de la presente tesis, opino que cumple objetivamente con cada uno de los capítulos elaborados permitiendo un análisis concreto así como conceptos y definiciones que puedan determinar que existe la necesidad de regular los delitos que se cometen en redes sociales de internet.

b. De igual forma la metodología utilizada se dio a través del método deductivo e inductivo, analítico, analítico, sintético y la utilización de la técnica del investigación bibliográfica, con lo cual se abarcó las etapas del conocimiento científico, planteado el problema jurídico-social de actualidad y buscándole una posible solución.

c. La redacción de este trabajo es adecuada y jurídicamente correcta.

BUFETE CORPORATIVO
ABOGADOS, AUDITORES Y CONTADORES
11 Calle 4-52 zona 1 Ciudad de Guatemala
Edificio Asturias Oficina Número 4
Teléfono 2232-3916

d. La contribución científica del trabajo de tesis en referencia, se centra en asegurar la necesidad de reformar la ley sustantiva penal para regular los delitos cometidos en redes sociales de internet, esto con el fin de hacer más viable los procesos penales.

e. La conclusión discursiva es congruente con el contenido del trabajo de tesis, ya que es un gran aporte al conocimiento del estudio del derecho.

f. En cuanto a la bibliografía empleada se comprobó que la misma ha sido correcta y suficiente para el presente trabajo.

En mi calidad de Asesor y de conformidad con lo que establece el Artículo 31 del Normativo para la Elaboración de Tesis de la Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público; de manera expresa manifiesto que no somos parientes, por tal razón emito **DICTAMEN FAVORABLE** estimando que el trabajo de tesis cumple con todos los requisitos establecidos en el normativo respectivo, a efecto se continúe el trámite.

Atentamente,

LIC. EDDY AUGUSTO AGUILAR MUÑOZ
ASESOR DE TESIS
Colegiado No. 6,410

Lic. Eddy Augusto Aguilar Muñoz
ABOGADO Y NOTARIO

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 29 de abril de 2015.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante DANIEL EMILIO TERCERO CONTRERAS, titulado LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL GUATEMALTECO DECRETO 17-73 DEL CONGRESO DE LA REPÚBLICA DE GUATEMALA PARA PREVENIR Y SANCIONAR LOS DELITOS QUE SE COMETEN EN LAS REDES SOCIALES DE INTERNET. 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
SECRETARIA
GUATEMALA, C. A.

BAMO/srrs.

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

Lic. Avidán Ortíz Orellana
DECANO

DEDICATORIA

ADIOS:

Ser Supremo que con su luz divina ha iluminado mi vida y camino, el entendimiento y la sabiduría para alcanzar esta meta.

A MIS PADRES:

Les doy gracias por su ejemplo y su esfuerzo, siempre me han demostrado serpersonas luchadoras, y su apoyo me ha brindado la oportunidad de lograr este triunfo.

A MIS HERMANOS:

Dios los bendiga, les deseo muchos éxitos y bendiciones en sus vidas, con tiempo hemos demostrado que si podemos lograr nuestros objetivos, así que a fijarnos nuevas metas.

A MIS AMIGOS:

Por las tantas alegrías, buenos y malos momentos ocurrencias y apoyo muto en nuestra formación profesional.

A NUESTRA GLORIOSA

Universidad de San Carlos de Guatemala, especialmente a la Facultad de Ciencias Jurídicas y Sociales, agradezco por darme la oportunidad de albergarme en sus aulas y haberme formado como todo un profesional.

A:

La Facultad de Ciencias Jurídicas y Sociales que con la ayuda de sus catedráticos quienes con su instrucción y colaboración, me permitieron adquirir los conocimientos necesarios para la culminación de mi carrera.

PRESENTACIÓN

El presente trabajo de investigación pertenece a la rama del derecho penal, siendo la misma una investigación cualitativa y se desarrolló tomando en cuenta la necesidad de regular el Código Penal Decreto17-73 del Congreso de la República de Guatemala con lo que pretendo tipificar nuevos delitos.

El actual Código Penal en el Libro Segundo Título VI Capítulo VII establece delitos informáticos pero es enfocado a los registros, información y programas de computación, no establece delitos que se puedan cometer en redes sociales de internet, por lo que facilitaría a los jueces dar la sentencia adecuada al actor de los delitos mencionados.

La presente investigación se realizó en los juzgados penales del municipio de Guatemala, departamento de Guatemala, durante los años 2012-2014. Siendo objeto de estudio las denuncias presentadas en el Ministerio Público. El aporte de la investigación es de regular la ley sustantiva penal adicionando una serie de delitos modernos que se comenten en redes sociales de internet con el fin de que las resoluciones judiciales sean lo más adecuado a la época.

HIPÓTESIS

En Guatemala existen diferentes delitos modernos que no están regulados, a falta de expertos en la materia no se puede lograr bajar los índices de delincuencia, estos delitos cometidos en Redes Sociales de Internet se realizó la siguiente investigación y se comprobó en personas entre los quince y treinta años durante los años dos mil doce al dos mil catorce dentro del municipio de Guatemala departamento de Guatemala que debe reformarse la ley penal.

La necesidad de reformar el Código Penal guatemalteco Decreto 17-73 del Congreso de la República de Guatemala para prevenir y sancionar los delitos que se cometen en redes sociales de internet para proteger la privacidad de los usuarios y protección de datos.

COMPROBACIÓN DE LA HIPÓTESIS

Como objetivo principal de la hipótesis es determinar los ilícitos penales que se cometen en Guatemala a través de las redes sociales de la Internet, ya que la seguridad en internet en el país es muy sensible que pueda ser atacado por un ciberdelincuente, estos delitos, fueron comprobados a través del método científico recolectando información de los agentes fiscales de delitos informáticos dentro del Ministerio Público, esa información es demostrada a través del planteamiento de la hipótesis y fue revisada con técnicas documentales, como libros de lectura, folletos, revistas, páginas de internet, y análisis de leyes.

Mi hipótesis es comprobada y veo que a partir de la adicción a Facebook, se han cometido muchos delitos; las personas sedentarias ven como delinquir sin salir de sus casas, únicamente con acceso a internet.

ÍNDICE

Pág.

CAPÍTULO III

Pág.

CAPÍTULO IV

INTRODUCCIÓN

En Guatemala es un país que carece de expertos en derecho de informática, y como consecuencia no existe un marco jurídico penal vigente que contemple nuevos ilícitos penales, la mayoría de guatemaltecos desconocen los delitos que son ocasionados con internet, actualmente no existe una edad para ser víctima de un delito cibernético, en la mayoría de situaciones el propio usuario desconoce que es víctima de estos delitos.

La importancia del presente estudio se realizó con el objetivo tipificar los delitos que se comenten en redes sociales de internet y la necesidad de reformar el Código Penal guatemalteco Decreto 17-73 del Congreso de la República de Guatemala, para que se tutelen los derechos inherentes a las personas, como ejemplo: suplantación de identidad, enlaces falsos, perfiles duplicados, etc.

Los objetivos de la investigación fueron: determinar los delitos cometidos en las redes sociales de internet, efectuar un análisis jurídico de los delitos que se cometen en las redes sociales de internet, determinar que personas pueden ser víctimas, determinar las sanciones que pueden imponerse a las personas que incurren en la comisión de uno o varios delitos en redes sociales de internet;derivado de lo anterior se plantea la hipótesis que formula, la existente necesidad de la formación de una iniciativa de ley por medio de la cual se regulen en los delitos cometidos en redes sociales de internet con el fin que fortalezca la legislación penal en Guatemala.

El informe final quedó dividido en cuatro capítulos: el primero señala las definiciones de delito, delito informático, red, red social, causas, efectos, elementos esenciales; El segundo describe los bienes jurídicos tutelados y la clasificación de los delitos

informáticos; el tercero se enfoca en la teoría del delito y los principios que pueden encuadrar a este tipo de delitos; el capítulo cuarto versa sobre la reforma del Código Penal Decreto 17-73, y la comparación con otros países a través del derecho comparado relacionado a los delitos cometidos en redes sociales de la Internet;

Los métodos utilizados en la investigación fueron el analítico, el deductivo y el inductivo; el primero utilizado para el análisis general de toda la doctrina y la legislación penal y constitucional, mediante la deducción se redactaron los resúmenes de contenido y el inductivo con el que se realizó cada fase del análisis de los temas más importantes que contiene la tesis. Toda la información fue obtenida mediante la técnica bibliográfica y documental.

Es la intención que esta tesis ayude a los lectores a comprender la importancia de la reforma del Código Penal guatemalteco Decreto 17-73 del Congreso de la República de Guatemala relacionado a los delitos que se comenten en redes sociales de la Internet, para evitar así lagunas de ley y las contradicciones entre ellas, asimismo busca su enseñanza desde la edad temprana como una forma de prevención de la violencia cibernética.

CAPÍTULO I

1. Delito informático

1.1. Antecedente histórico

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en el país, al igual que en otros muchos no han sido objeto de tipificación aún."

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes

penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."

Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma.

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente: No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen. La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa. Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una

protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

1.2. Definición

Delito informático o ciberdelicuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Debido a que la informática se desarrolla más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

Para Andrés Gabriel Cámpoli, los delitos informáticos son "todos aquellos en los cuales el sujeto activo lesiona un bien jurídico, que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, por medio de utilización indebida de medios informáticos. Surgen claramente de las nuevas tecnologías aplicadas y tienen como objeto de manera expresa de las mismas y por regla general no poseen definiciones de tipo posibles de ser utilizadas en modo alguno por estar referidos a bienes y conceptos inexistentes a la sanción de las leyes penales".[1]

[1]Cámpoli, Gabriel Andrés, **Delitos informáticos en la legislación mexicana**, pág.144.

1.3. Naturaleza jurídica

En todo el entorno cibernético, se establece en la sociedad humanitaria que el pensamiento permite descubrir sus verdaderas leyes y las fuerzas motrices del desarrollo de la realidad, en el que se establece que es de carácter virtual y público la naturaleza por sí mismo.

1.4. Delimitación del fenómeno

Guatemala debe iniciar a prepararse para el futuro, creando medidas necesarias para poder prevenir una seria de delitos tecnológicos, para que la población pueda guardar información relevante y utilizarla después de una forma segura. El problema no solo es en el área penal si no en todo el ordenamiento jurídico nacional.

1.4.1. Delincuencia informática y abuso informático

Son todos comportamientos ilegales y contrarios a la ética que tienen por objeto a los sistemas o elementos informáticos, que concierne a un tratamiento automático de datos y/o transmisión de datos, pudiendo presentar múltiples formas de lesión de varios bienes jurídicos tutelados.

1.4.2. Criminalidad informática

Es todo comportamiento criminológico en el cual la computadora está involucrada como material o como objeto de acción para el empleo de actos antijurídicos que puedan ocasionar daños patrimoniales a terceras personas.

1.5. Delitos informáticos reconocidos por la Organización de las Naciones Unidas

Existen varios criterios para determinar la clasificación de los delitos informáticos, ya que doctrinariamente no existe una normativa a seguir, el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos aporta la siguiente clasificación de delitos informáticos:

- "Fraudes cometidos mediante la manipulación de computadoras:
    1. Manipulación de los datos de entrada.
    2. Manipulación de programas.
    3. Manipulación de datos de salida.
    4. Fraude efectuado por manipulación informática.
- Falsificaciones informáticas:
    1. Utilizando sistemas informáticos como objetos.
    2. Utilizando sistemas informáticos como instrumentos.

- Daños o modificaciones de programas o datos computarizados:
    1. Sabotaje informático.
    2. Virus.
    3. Gusanos.
    4. Bomba lógica o cronológica.
    5. Acceso no autorizado a sistemas o servicios.
    6. Piratas informáticos o hackers.
    7. Reproducción no autorizada de programas informáticos con protección legal".[2]

1.6. Clasificación de los delitos informáticos

El eje principal de los delitos informáticos se da en la manipulación de los datos de entrada, programas y salidas de computadoras, así como la falsificación de los sistemas informáticos, y el espionaje de información, lo que produce en el sujeto pasivo un daño en su patrimonio; por ello estimamos que los ilícitos cometidos a través de Internet en su mayoría causan una afectación al patrimonio de los pasivos.

[2]López Betancourt, Eduardo, **Delitos en particular**, pág. 271.

1.6.1. Delitos patrimoniales

El fraude electrónico causa una gran afectación a los usuarios de la banca, siendo el principal blanco de dichos ataques, los ataques informáticos se generan en contra de los clientes y no en contra de la institución crediticia, lo que obedece a los sistemas de protección que gozan las instituciones bancarias, tales ataques se llevan a cabo a través de dos programas que se denominan: Phising y Pharming, el propósito de esos programas es hacerse de los recursos del usuario de la banca, aprovechándose de dos factores básicos que toman en consideración los defraudadores, los cuales son el nivel cultural del usuario y la natural curiosidad del ser humano.

Ante los ataques de los defraudadores cibernéticos se han instrumentando sistemas básicos de protección que debe tener cualquier usuario de internet, entre los cuales destacan:

1. Tener una herramienta de antivirus vigente y actualizado.
2. Poseer herramientas anti intrusos.
3. Tener un firewall personal.
4. Tener autorizados parches de seguridad.
5. Controlar las entradas y salidas de las unidades usb y disquetes para evitar las descargas de impresiones fotográficas, entre otras.

1.6.2. Delitos pornográficos

La distribución de pornografía por todo el mundo a través de la Internet está en aumento. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material "ofensivo" que se transmita o archive.

El fenómeno de la pornografía en Internet, se engloba dentro de los denominados delitos computacionales, al suponer una nueva manifestación del delito ofensas al pudor, cuya comisión afecta el bien jurídico de la libertad sexual[3].

1.6.3. Delincuencia organizada

El objeto y necesidad de fundamentar los delitos informáticos vinculados en la participación de algún miembro de la delincuencia organizada, así como los hechos, circunstancias, datos, y demás elementos que se pretenda probar.

La persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizarán; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención.

---

[3]Reyna Alfaro, Luis, **"Pornografía e Internet: aspectos penales"**, AR: Revista de Derecho Informático, núm. 050, septiembre de 2012.

El objeto de la intervención de las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

1.7. Legislación sobre delitos informáticos en Guatemala

La tecnología y el internet son herramientas que han permitido al hombre desarrollar sus actividades laborales y sociales, al mismo tiempo su uso indebido ha ocasionado daños tanto individuales, empresariales e inclusive instituciones de gobierno. Así mismo en Guatemala, se ha reportado un aumento en delitos informáticos en los últimos años, los más comunes son el fraude, robo de identidad, robo de base de datos, infiltraciones.

En la actualidad Guatemala, dentro de los nueve países con mayores detecciones de códigos maliciosos en Latinoamérica ya que es uno de los países con mayores descargas de copias ilegales de software, por lo que muchos medios de protección son obsoletos por la cantidad de datos que existen en la red de internet.

La legislación en Guatemala, necesita una nueva regulación solo en aquellos aspectos donde se produce un vacío legal; en lo concerniente al Código Penal, no se da en ninguno de los títulos los delitos informáticos cometidos a través de redes sociales. Por

eso, dadas las características de esta problemática solo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos".

En materia penal se encuentran tipificadas una serie de acciones antijurídicas punibles en el Código Penal guatemalteco en su capítulo VII referente a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos de acuerdo a lo regulado en los Artículos; 274 "a" "b" "'c" "d" "e" "f" "g". Así también cómo en el Artículo 275 y 275 bis.

Los bienes jurídicos tutelados que establece el Código Penal establecen una leve protección de datos, por lo que es necesario proteger la privacidad, acceso a propiedad privada, acceso a la información no autorizada, situándolas como nuevas modalidades de delitos informáticos que operan a través de las redes sociales.

Debe establecerse que, "hechos que generen conductas indebidas deben ser tipificados en la legislación correspondiente. Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a prevenir la utilización abusiva de la información reunida y procesada mediante el uso de computadoras".[4]

[4] Velázquez Elizarraras Juan Carlos. **Instauración de un marco legal internacional de internet**. Pág. 289.

Existen actualmente dos iniciativas de ley una por el diputado Francisco Contreras del partido de Acción de Desarrollo Nacional (ADN) la iniciativa 4055 de "Ley De Delitos Informáticos" la cual tiene por objeto la protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información. Así como la prevención y sanción de los delitos cometidos relativos a fraude Informático, daño informático, acceso ilícito, falsificación informática, espionaje informático, violación de la disponibilidad, reproducción de equipos, etc. y la segunda propuesta la diputada Nineth Montenegro, de Encuentro por Guatemala con la cual busca castigar a las personas que mediante perfiles falsos engañen a menores de edad con fines sexuales, cometan extorsiones o difamaciones; dicha iniciativa podría atentar contra la libertad de expresión, por lo que es un análisis de estudio para los parlamentarios.

CAPÍTULO II

2. Redes sociales

Para comprender un poco este fenómeno cabe citar en lo básica que permita comprender qué es una red social, Internet y algunas nociones sobre su historia. principio alguna definición cómo funcionan éstas en: Según definición de la enciclopedia digital Wikipedia: "Las redes sociales son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos".[5]

En las redes sociales en internet existe la posibilidad de interactuar con otras personas aunque no las conozcamos, se construye a través del aporte de cada suscriptor de la red.

El software germinal de las redes sociales parte de la teoría de los Seis grados de separación, según la cual toda la gente del planeta está conectada a través de no más de seis personas.

Existe una patente en los Estados Unidos de Norteamérica conocida como six degrees patent usada en su mayoría por las redes sociales Tribe y LinkedIn.

---

[5] http.//es wikipedla.org/wlki/**Red soclal**. Enciclopedia Digital Wikipedia consultada el 15/09/2014.

Existen otras muchas patentes que protegen la tecnología para automatizar la creación de redes y las aplicaciones relacionadas con éstas.

La teoría fue propuesta inicialmente en 1929 por el escritor Húngaro FrigyesKarinthf "El concepto está basado en la idea que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y solo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera".[6]

Los fines que han motivado la creación de las llamadas redes sociales son varios, principalmente, el de diseñar un lugar de interacción virtual, en el que millones de personas alrededor del mundo se reúnan, comuniquen y compartían intereses en común.

Las funciones de las redes sociales varían, por lo general la informalidad y espontaneidad de estas crean vínculos de compañía y apoyo, desarrollándose lazos afectivos con familiares y amigos.

Una red social, es un sitio donde varias personas se interrelacionan con intereses comunes, tomando como premisa que las redes sociales son medios principalmente de comunicación, dejando de un lado los sitios web considerados para compartir

[6] **Ibid.**

información, creando así un nuevo tipo de redes sociales, comúnmente denominadas redes para compartir.

El concepto de red social en internet supone una nueva forma de relación humana que ha ido posicionándose como uno de los medios de comunicación en línea más populares, "llegando a superar en algunos casos los 132 millones de usuarios recurrentes según datos facilitados por la empresa ComscoreWorldMetrix en agosto de 2010, que la utilizan como principal forma de comunicación".[7]

En los últimos años han proliferado dentro del universo de ¡internet las denominadas redes sociales (como Facebook; LinkedIn, Sónico, Hi5 y Twitter entre otros), entendidas como espacios virtuales en la web donde personas de distintos lugares del mundo pueden conocerse entre sí, permitiendo el desarrollo de relaciones sociales que talves desconocen los límites regulares de este tipo de interacciones (como la distancia, el idioma e incluso las diferencias horarias).

En un inicio surgieron varios esfuerzos para lograr la comunicación entre individuos a través de las computadoras, como Usenet, Arpanet y EIES: Murray Turoff basada en el servidor de Servicio de intercambio de información Electrónica.

---

[7] http/www.redinamiza.com/action/fi e/download?fileguid=751.**Red Social de Aprendizaje**Consultada el 20/09/2014

Ninguno de los anteriormente mencionados, funcionaba como un sitio web, eran muy específicos, y además difíciles de usar, por tal motivo con la creación de la gran red, el internet nacen los primeros sitios ya como redes sociales, como lo son:

"Classmates.com (1995), centrándose en los vínculos con el antiguo colegio y SixDegrees.com (1997), centrándose en los vínculos indirectos; son dos modelos diferentes de la creación de redes sociales que se produjeron a partir de 1999 y que fueron basados en la confianza, desarrollado por Epinions.com, y basada en la amistad".[8]

Para 1999 se creó LiveJournal.com, éste fue uno de los primeros servicios de redes sociales en ofrecer blogs y diarios en línea, en ese año comienzan a crecer el número de sitios de redes sociales, pero fue hasta el año de 2003 con la salida de Myspace uno de los sitios que aún sigue siendo referente en cuanto lo que se refiere a redes sociales. Convirtiéndose en ese momento en el referente de lo que debía ser una red social, sobre todo ya enfocada a lo que se denomina Web 2.0.

Ese mismo año una de las empresas más importantes en la industria informática Microsoft, ingresa al mundo de las redes sociales, con sus MSN Spaces, hoy conocido como Windows Live Spaces, aprovechando que la mayoría de los usuarios de internet, tienen cuenta de Hotmail, MSN, o live que pertenece a esta empresa, aunque en realidad no ha logrado el éxito de ninguna de las otras redes, integra varias cosas,

[8]hilp//cienshanime.forosactivos.net/t923 **Redes sociales, Foro activo** Consultada el 23/09/2014

compartir fotos, archivos, blog; pero aun sin agregar algo novedoso, junto con esta nace otras de las grandes redes, sobre todo en América Latina, me refiero a His, este sitio es famoso por su interactividad, pues hace de una simple cuenta de usuarios una especie de tarjeta de presentación virtual, y la gran variedad de aplicaciones informáticas que fueron saliendo para ésta, en estos momentos esta red social se encuentra en rediseño.

En el año 2004, nace la que en estos momentos es la líder en el mundo de las redes sociales, Facebook, originalmente era un sitio para estudiantes de la Universidad de Harvard, en sus comienzos funcionaba por medio de invitaciones, a partir del año 2006 está abierta a cualquier persona que desee ingresar.

En el año 2006, se crea una de las redes que está subiendo en el ranking denominada Twitter, esta red se llama en microblogging que permite a los usuarios enviar pequeñas entradas de texto, denominadas tweets, de una longitud máxima de 140 caracteres.

Gracias a su forma de uso tan simple se encuentra cada día agregando nuevos usuarios a esta, y además que da la ventaja de poder subir los tweets, sin necesidad de entrar a su página.

2.1. Clasificación de redes sociales

La siguiente clasificación previa búsqueda en el sitio web de Pablo Burgueño aporta que existen dos clases fundamentales de redes sociales:

Analógicas o redes sociales Off-Line: "Son aquellas en sociales, con independencia de su origen, se desarrollan sin sistemas electrónicos".[9]

Las que de mediación de relaciones aparatos o Digitales o redes sociales On-Line: "Son aquellas que tienen su origen y se desarrollan a través de medios electrónicos".[10]

También aporta que para comprender la nueva realidad social debe conocerse en profundidad los diferentes tipos de redes sociales digitales que operan en la red, razón por la cual propone la clasificación siguiente:

Por su público objetivo y temática:

Redes sociales Horizontales: "Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Se basan en una estructura de celdillas permitiendo la entrada y participación libre y genérica sin un fin definido, distinto del de generar masa. Los ejemplos más representativos del sector son Facebook, Orkut, Identi.ca, Twitter".[11]

Redes sociales Verticales: Están concebidas sobre la base de un eje temático agregado. Su objetivo es el de congregar en torno a una temática definida a un colectivo concreto. En función de su especialización, pueden clasificarse a su vez en:

---

[9] Pablo Burgueño. **Clasificación de las redes sociales** http//www.pabloburgueno.com/2009/03/clasificación de redes-sociales/ consultado el 24/09/2014
[10] **Ibid.**
[11] **Ibid.**

a. Redes sociales verticales profesionales: Están dirigidas a generar relaciones profesionales entre los usuarios. Los ejemplos más representativos son Viadeo, Xing y LinkedIn.

b. Redes sociales verticales de ocio; Su objetivo es congregar a colectivos que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc. Los ejemplos más representativos son Wipley, MinubeDogster, Last.FIvl y Moterus.

c. Redes sociales verticales mixtas: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales en torno a sus perfiles: Yugulo, Unience, pidecita, 11870. [12]

Por su público objetivo y temático:

a. **Redes sociales Humanas:** Son aquellas que centran su atención en fomentar las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Ejemplos de este tipo de redes los encontramos en Dopplr y Tuenti.

b. **Redes sociales de Contenidos:** Las relaciones se desarrolla uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Los ejemplos más significativos.

[12] **Ibid.**

c. **Redes sociales de Objetos:** Conforman un sector novedoso entre las redes sociales. Su objeto es unir marcas, automóviles y lugares. Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red. El ejemplo más llamativo es Respectance

Por su localización geográfica

a. **Redes sociales Sedentarias:** Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos de este tipo de redes son: Blogger, Plaxo, Bitacoras.com, Plurk .

b. **Redes sociales Nómadas:** A las características propias de las redes sociales sedentarias se le suma un nuevo factor de mutación o desarrollo basado en la localización geográfica del sujeto. Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son: Foursquare, Latitude, Fire Eagle y Skout.

2.2. Facebook

Es una red social de internet que permite a los usuarios interactuar en el mundo informático a través de la creación de perfiles, compartiendo contenido, imagines,

videos, música y documentos digítales. Actualmente es un sitio gratuito con el cual después de registrados podemos gestionar nuestro espacio personal.

La principal utilidad de facebook es compartir recursos, impresiones e información con amigos y familiares, aunque también se puede utilizar para conocer gente nueva o crear un espacio para gestionar un negocio con sus clientes.

Facebook ofrece actualmente accesibilidad desde terminales móviles, que ha permitido que la red crezca muy rápidamente en poco tiempo, aunque también ofrece una serie de mini aplicaciones disponibles para jugar, hablar, etc., con otros usuarios.

2.2.1. Historia de Facebook

El 4 de Febrero 4, 2004, Mark Zuckerberg lanzó "Thefacebook", originalmente localizado en el sitio web thefacebook. Originalmente era para los alumnos de Hardvard con la ayuda de Eduardo Saverin (tema de negocios), DustinMoskovitz (programador), Andrew McCollum (artista gráfico) y Chris Hughes pronto se unieron a Zuckerberg para ayudarlo a promocionar el sitio. Hacia finales del año 2004 se fundó Facebook como compañía, finalmente a partir del 26 de septiembre del año 2006, abre sus puedas a todo el mundo. La condición básica para participar en esta red, es ser mayor de 13 años y tener una cuenta de correo electrónico válida.

2.2.2. Privacidad y protección de información personal

Facebook al ser la red social más usada en Guatemala cabe mencionar que la cantidad de usuarios cada día es mayor, por lo que la información personal debe ser protegida, ya que existen medios que pueden controlar los contenidos y privacidad que se logran compartir, ya que toda clase de red gira alrededor de varias personas y muchas personas comparten información de su propia vida. Sin embargo la mayoría de los datos son públicos, se puede controlar la manera en que los demás pueden ver el perfil y de qué manera se desea aparecer frente a los demás dentro de esta red social.

Hay gente que no está en Facebook por razones de privacidad preocupaciones legítimas y justificadas. Facebook, consciente de esta situación, modifica continuamente sus esquemas de privacidad y las herramientas que te permiten configurarla.

"A continuación indicare algunas medidas que debe tomar el usuario de Facebook para poder proteger su seguridad:

1. Solo acepta solicitudes de gente que conoces o sabes que son personas reales.

   Existe una cantidad muy grande de personas con perfiles falsos con diversas motivaciones. Para proteger la privacidad, deben tener cautela al aceptar invitaciones de personas que no conocen o que sospechan no son reales.

2. Organiza a tus amigos en listas.

Las listas de amigos son una herramienta muy útil en la organización de tu privacidad ya que te permite definir permisos en base a grupos, en lugar de hacerlo por individuo

3. Personaliza la privacidad de tu perfil.

Facebook te permite configurar quien puede ver partes específicas de tu perfil, como por ejemplo: lista de amigos, datos de trabajo, etc.

4. Define privacidad a tus fotografías y álbumes de fotos.

Esto te garantiza que puedes compartir tus álbumes de fotos con los grupos adecuados, por ejemplo fotos de trabajo con compañeros de trabajo. Además de que evitas que gente fuera de la lista de amigos puedan verlos.

5. Define la privacidad de tu biografía.

Garantiza que tus fotos y publicaciones no sean vistas por personas que no conoces.

6. Controla publicaciones automáticas a tu biografía.

Puedes evitar que ciertas historias generadas automáticamente se publiquen en tu biografía.

7. Define tu nivel deseado de privacidad para las aplicaciones y juegos de Facebook.

Puedes definir si deseas que tus actividades con aplicaciones y juegos sean publicadas en tu muro o en noticias".[13]

2.3. Delito informático en redes sociales

En la actualidad los delitos informáticos en particular en las redes sociales es un tema que cada día da más que hablar. Los usuarios van tomando conciencia de que en Internet no todo vale, y de que los delitos en la vida real, también lo son en la vida virtual. En los últimos tres años se aumentó la nueva forma de delitos informáticos los cuales se generan en redes sociales, lo cual indica que los delincuentes informáticos están comenzando a centrar sus esfuerzos en estas plataformas cada vez más populares.

---

[13] http://aprenderinternet.about.com/od/SeguridadPrivacidad/tp/Siete-Practicas-Para-Proteger-Tu-Privacidad-En-Facebook.htm ,**Aprende Internet**, consultada el 25/09/2014.

Uno de cada cinco adultos conectados a la red ha sido víctima de un delito informático a través de las redes sociales, específicamente que alguien había hackeado su perfil simulando ser ellos, estafas mediantes enlaces falsos entre otros delitos. Los delincuentes informáticos están cambiando de tácticas para dirigir sus ataques a las plataformas de redes sociales, donde los consumidores son menos conscientes de los riesgos de seguridad.

La mayoría de adultos conectados a la red informan que se les ha notificado sobre el cambio de contraseña de su correo electrónico, por lo que tienden a cambiar también la de su red social dado que las personas envían, reciben y almacenan desde fotografías personales, correspondencia y documentos relacionados con el trabajo, hasta resúmenes bancarios y contraseñas de otras redes. Por lo que pueden tener una puerta de acceso potencial para los delincuentes que buscan información personal y comercial.

Existen diferentes tipos de plataformas de redes sociales en los que se inicia la delincuencia, pero Facebook y Twitter son las más comunes.

Los delincuentes utilizan las redes sociales para reunir información de sus víctimas, pero los métodos utilizados difieren según la naturaleza del delito en cuestión. La ciberdelincuencia, el robo y los delitos sexuales son las tres categorías de delitos que son más a menudo iniciados en los medios sociales.

Cuanto antes se den cuenta las personas de todo esto, más pronto van a ser capaces de protegerse en línea.

1.1. Sujetos del delito informático en redes sociales

Los sujetos del delito son aquellas personas que intervienen tanto autores y cómplices del delito, como las víctimas de éste. Los autores y cómplices son personas responsables criminalmente de los delitos y faltas; no obstante, existen diferencias entre ellos. De esta forma los autores como tal son quienes realizan el hecho por sí solos, en grupo o quienes inducen directamente a otro/s a ejecutarlo y quienes cooperan en su ejecución con un acto sin el cual no se habría efectuado el acto. Los cómplices son aquellos que cooperan en la ejecución del hecho con actos anteriores o simultáneos y que no pueden enmarcarse en ninguna de las características de los autores. Las víctimas son las personas a las que se les ha ocasionado algún daño.

Los sujetos involucrados en la comisión de delitos informáticos son: sujeto activo y sujeto pasivo.

Los diferentes ilícitos que cometen los delincuentes informáticos y electrónicos, debido a que muchos de los delitos son descubiertos casualmente por el desconocimiento del modus operandi de los sujetos activos.

2.4.1. Sujeto activo

El sujeto activo, son las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentren en lugares estratégicos en los que se maneja información de carácter sensible.

Los autores de los delitos informáticos son muy diversos, y la diferencia radica en sí en la naturaleza de los delitos cometidos. "De esta forma, la persona que entra 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".[14]

Edwin Sutherland penalista estadounidense expresa que "tanto la definición de los delitos informáticos como los denominados de cuello blanco, no es de acuerdo con el interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos destaca que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por poca inteligencia". [15]

[14] Zavala Antelmo. **El impacto social de la informática jurídica en México**, www.unam.edu.mx. Consultada e 20/09/2014.
[15] Estrada Garavilla, Miguel, **Delitos informáticos**. www.derecho.org consultada el 26/07/2014.

Diego Moisés Aparicio expresa, "este nivel de criminalidad se puede expresar por la dificultad de reprimirla en forma internacional, en virtud que los usuarios están esparcidos por todo el mundo, y en consecuencia, está la posibilidad latente que el agresor y la victima estén sujetos a leyes nacionales diferentes. Además aporta que los acuerdos de cooperación internacional y tratados de extradición bilaterales intentan remediar de alguna forma las dificultades ocasionadas por los delitos informáticos, debido a que sus posibilidades son limitadas"[16].

2.4.2. Sujeto pasivo

Sujeto pasivo del delito, es la persona física o moral que resiente la actividad delictiva, es el titular del bien jurídicamente tutelado que es dañado o puesto en peligro por la conducta del agente, y en los casos de los delitos informáticos pueden ser individuos particulares, personas morales como sociedades mercantiles, instituciones crediticias, gobiernos etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, mediante él se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos, debido a que muchos de los delitos son descubiertos casualmente por desconocimiento del modus operandi de los sujetos activos.

---

[16]Abaili Aparicio, Diego Moisés. **Necesidad de la reforma penal en materia de delitos informáticos.** Pág. 19

Se debe distinguirse que sujeto pasivo o víctima del delito "es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros".

Resulta imposible conocer la verdadera magnitud de los delitos informáticos, la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades correspondientes, si a esto se le suma la falta de leyes que protejan a las víctimas de este tipo de 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, así mismo provoca que las estadísticas sobre este tipo de conductas se mantenga bajo la llama de cifra negra u oculta.

Además se destaca que los organismos internacionales, han adoptado resoluciones similares en sentido que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para destacar, investigar y prevenir los delitos informáticos.

2.5. Bien jurídico tutelados en los delitos informáticos

El bien jurídico nace de una necesidad de protección de ciertos y cambiantes bienes inmanentes a las personas. De otro lado es claro que no aparece otro factor que se revele como más apto para cumplir con la función limitadora de la acción punitiva, pues como hemos observado solo los bienes jurídicos de mayor importancia para la convivencia social y cuya protección por otras ramas del derecho hagan insuficiente la prevención que cualquier transgresión los afecte.

Los bienes jurídicos tutelados en los delitos informáticos se protegen mediante la creación de sus tipos penales son específicamente la de la privacidad.

Al penalizarse las conductas ilícitas tipificadas dentro del rubro de los delitos informáticos, se intenta proteger diversos bienes jurídicos, como la intimidad o privacidad, la integridad de los sistemas informáticos, es decir de la información contenida en ellos, la libertad y la propiedad, entre otros; lo cual atiende al tipo de delito que se trate, en correlación directa a la persona u objeto, que sea afectado o dañado, es lo que le da sentido y fundamento.

Pablo Palazzi establece: "de conformidad al bien jurídico tutelado clasifica a los defectos informáticos en: delitos contra el patrimonio, contra la intimidad, de la

Seguridad pública y las comunicaciones, falsificaciones informáticas y contenidos ilegales en Internet, como la pornografía infantil".[17]

En el Código Penal guatemalteco ya están tipificados algunos de los delitos informáticos y electrónicos, los cuales no propician aún lograr un ambiente seguro para los negocios y comunicaciones electrónicas e informáticas.

Ya que se contempla que se constituye el delito si se accesa a un sistema informático protegido por un mecanismo de seguridad. La justicia no puede reducirse solo a aquéllos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad. El Código Penal guatemalteco no define qué debe entenderse por .mecanismo de seguridad. Esta vaga redacción sin duda, traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto. El mejor ejemplo es el ataque de .Denegación de Servicios, cuyo objetivo no es .modificar, destruir o provocar pérdida de información, sino simplemente imposibilitar o inhabilitar un servidor temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas mientras el servidor esta caído.

La legislación en materia de delitos informáticos dista mucho de ser perfecta, sin embargo es solo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país.

---

[17]Palazzi, Pablo Andrés, **Delitos informáticos**, pág. 32.

La dignidad y el derecho al honor van íntimamente ligados ya que en el momento en que se produce un ataque al honor de una persona se lesiona también su dignidad.
A través de la protección dispensada a la dignidad y al derecho al honor se protege a los individuos tanto de forma subjetiva, teniendo en cuenta la esfera personalísima de este valor y este derecho así como de forma objetiva pues se pretende salvaguardar la reputación de cada uno, entendida como aquella concepción que de uno mismo puedan tener los demás.

En cuanto al derecho a la intimidad personal y familiar y la propia imagen constituyen un bien jurídico que se protege de forma indirecta pues solamente se lesiona cuando se utiliza el ciberbullying para difundir imágenes o datos que pertenecen a la esfera íntima de la persona sin contar con su consentimiento o autorización.

El autor del delito de ciberbullying está cometiendo también un delito de revelación de secretos por cuanto, al difundir expresiones injuriosas o vejatorias a través de las redes sociales en internet hace públicos datos o informaciones que pertenecen a la intimidad de la persona y que esta no quiere que los demás conozcan o bien si quiere difundirlos prefiere hacerlo en un círculo restringido de amigos de su red social.

2.6. Clasificación de los delitos informáticos regulados en el Convenio de las Naciones Unidas sobre la ciberdelincuencia

El Convenio de Budapest firmado el 21 de Noviembre de 2001 en el marco del Consejo de Europa, este instrumento jurídico internacional, es uno de los más importantes que se afirmado hasta el día de hoy.

Actualmente, el Convenio sobre la Ciberdelincuencia del Consejo de Europa es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional).

Este convenio surgió a partir de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional, y en la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada rápida y operativa.

De conformidad con el la investigación científica de los delitos informáticos cabe mencionar que La Organización de las Naciones Unidas, enuncia los siguientes "tipos de delitos informáticos:

Fraudes cometidos mediante manipulación de computadoras; Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede accesar a tos tipo de registros y programas.

La manipulación de programas: Mediante el permitan estar manejando los distintos programas de cualquier organización.

Programas auxiliares que tiene en los departamentos uso de que se Manipulación de los datos de salida: Cuando se asieran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo.

Fraude efectuado por manipulación informática: Accesando a los programas establecidos en un sistema de información, y manipulándolos para obtener una ganancia monetaria Falsificaciones informáticas: manipulando información arrojada por una operación de consulta en una base de los, Sabotaje informático: Cuando se establece una operación tanto de programas de cómputo, como un suministro de electricidad o cortar líneas telefónicas intencionalmente.

El convenio hace la siguiente clasificación:

A. "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos.

- Acceso ilícito: El acceso deliberado e ilegitimo a la totalidad o a una parte de un sistema informático ya sea infringiendo medidas de seguridad con la intención de obtener datos informáticos.
- Interceptación ilícita: Interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.
- Interferencia en los Datos: Comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
- Interferencia en el sistema: Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.
- Abuso de los dispositivos: Comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta"[18].

B. "Delitos informáticos

- Falsificación informática: Cometer de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos

[18] **Ibid**.

legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

- Fraude Informático: Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, cualquier interferencia en el funcionamiento de un sistema informático"[19].

C. Delitos relacionados con el contenido

- Delitos relacionados con la pornografía infantil: Comisión deliberada e ilegítima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos. Se entiende como pornografía infantil, todo material pornográfico que contenga representación visual de un menor comportándose de una forma sexualmente explicita, una persona que parezca un menor comportándose de una forma sexualmente explicita, imágenes realistas que representen a un menor

[19] **Ibid.**

comportándose de una forma sexualmente explicita"[20].

D. "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Se refiere a acciones ilícitas en contra de la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, que hasta la fecha ampara á nivel internacional el derecho de los autores, con el fin de que tengan el privilegio de controlar el uso sobre sus obras literarias, artísticas o científicas, así como recibir una retribución por su utilización; así como las asumidas por el Tratado de la Organización Mundial de Propiedad Intelectual (O.M.P.I) sobre propiedad intelectual, Convenio de Roma"[21].

2.7. Clasificación de los delitos informáticos regulados en el Código Penal guatemalteco

La Legislación sobre delitos informáticos en Guatemala, de conformidad con la legislación guatemalteca, sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección existentes en Guatemala, creando una nueva regulación solo en aquellos aspectos en los que, basándose en las

---

[20] **Ibid**

[21] http://www.uncjin.org/Documents/congr10/10s.pdf, **Décimo Congreso de las Naciones Unidas**, consultada el 25/09/2014

peculiaridades del objeto de protección, sea imprescindible y no solo usando la figura de la analogía.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas.
Si a ello se agrega que existen bancos de datos, empresas o entidades (infornet, Transfusión) dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado, a agrupaciones políticas, empresas, particulares e incluso al crimen organizado.

Se establece la colocándonos frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas.

Asimismo, la amenaza futura será directamente, en forma proporcional a los adelantos de las tecnologías informáticas, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos qué el ordenamiento jurídico institucional debe proteger.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo e informático. "Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

Dadas las circunstancias y las características de esta problemática solo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.
En materia penal se encuentran tipificadas una serie de acciones antijurídicas punibles en el Código Penal guatemalteco en su capítulo VII referente a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos de acuerdo a lo regulado en los Artículos; 274 "a" "b""c" "d" "e" f "g". Así también cómo en el Artículo 275 y 275 bis. Regulan lo siguiente:

Artículo 275. Violación a los derechos de propiedad industrial.

Artículo 275 bis. Violación a los derechos marcarios.

CAPÍTULO III

3. El delito informático y la teoría del delito

Las conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

La falta de acuerdos globales acerca de qué tipo de conductas debe constituir delitos informáticos, y la ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

La ausencia de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos, la armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En síntesis, es destacable 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.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que de modo creciente aumenta aún en países latinoamericanos, conlleva también a la posibilidad progresiva de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones de los funcionarios judiciales".

Bacigalupo afirma, "que la Teoría del Delito *es una teoría de la aplicación de la ley penal*, y como tal pretende establecer un orden para el planteamiento y la resolución de los problemas que implica la aplicación de la ley penal. La misma cumple una doble *función mediadora*, por un lado entre la ley y la solución del caso concreto; y por otro lado, una mediación entre la ley y los hechos que son objeto del juicio"[22].

3.1. Principio de legalidad

Para el principio de legalidad para que se dé un delito tiene que cumplirse cada uno de los tipos o elementos que estén en el Código. No debe confundirse que el hecho que la acción sea típica ya es un delito ya que este es un indicio, pero nos faltan elementos como la acción antijurídica.

---

[22]BACIGALUPO, Enrique. (1994). ***Lineamientos de la Teoría del Delito***. Ed. Hammurabi, 3º edición, Bs. As., pág. 25.

Acciones típicas antijurídicas: Si va en contra de la norma son acciones típicas y antijurídicas. Hay acciones típicas que no necesariamente son antijurídicas como matar en legítima defensa, es decir está tipificado el delito de homicidio y por ello es típica dicha acción pero es antijurídica porque fue en legítima defensa.

El Principio de Legalidad, exige como condición esencial, la existencia de un régimen jurídico que formule la descripción del hecho o conducta criminal y de la pena a imponerse, previamente al hecho que califica a ella como criminal, para imputar a una persona como autora del delito. La concreción legislativa de nuevos supuestos de incriminación que supongan nuevos delitos, es un paso importante para llevar a cabo en la legislación guatemalteca.

Si bien, y como ha quedado demostrado en los puntos anteriores, a nivel mundial existen varios pronunciamientos y reformas legislativas tendientes a la protección de bienes jurídicos o intereses como ser el "software", la "información", "la intimidad", etc, debemos remarcar que dicha nueva normativa, brinda una solución parcial a la problemática que nos ocupa. Por ello, ante determinadas situaciones, sería conveniente contemplar situaciones puntuales de violación a los sistemas informáticos, a través de figuras tipo, contempladas en los Códigos Penales.

Ricardo Núñez, enumera las consecuencias que derivan de dicho principio que son: "la indelegabilidad de la facultad legislativa penal, el Principio de Reserva penal con sus

presupuestos (la tipicidad del hecho punible, la prohibición de la aplicación de la ley penal por analogía y la irretroactividad de la ley penal), y la predeterminación legal de la pena aplicable"[23].

Pero el inconveniente surge de la necesidad de incorporar una serie de delitos informáticos y delitos que se cometan en redes sociales al Código Penal.

3.2. Principio de reserva penal

El Principio de Reserva Penal, se encuentra en la garantía de la legalidad. Es decir, que el ámbito de lo punible debe estar determinado exhaustivamente por la ley, y que todo lo que queda al margen de ese ámbito está reservado como esfera de impunidad. En el derecho penal existe la forma idónea de poder establecer la reserva de forma legal ante un tipo penal preestablecido ante la sociedad.

Este principio se encuentra consagrado en el Artículo 12 de la Constitución Política de la República de Guatemala y consiste en que nadie podrá ser condenado ni privado de sus derechos sin antes haber sido citado, oído y vencido en un proceso judicial, y el Código Procesal Penal lo desarrolla debidamente, ya que el procesado tiene desde la primera actuación judicial hasta la eventual condena una serie de facultades y deberes que le permiten conocer todas las actuaciones judiciales y contar con defensa técnica, a excepción de dos casos: la ley de narcoactividad que permite reserva de actuaciones

[23]Nunez, Ricardo C. (1987). **Manual de Derecho Penal. Parte General**, Ed. Marcos Lerner, Córdoba, Argentina, 3° ed., pág 79.

en las fases de investigación y preparatoria, y el Artículo 314 del CPP que establece que el Ministerio Público podrá tener en reserva las actuaciones, incluso ante las partes cuando no se hubiere dictado el auto de procesamiento.

.

El debido proceso comprende numerosas instituciones relacionadas tanto con las partes como con la jurisdicción que han de preservar la certeza en el proceso. Busca, en suma, rodear al proceso de las garantías mínimas de equidad y justicia que respaldan en legitimidad la certeza en derecho de su resultado. A través del debido proceso se precipitan todas las garantías, derechos fundamentales y libertades públicas de las que es titular la persona en el Estado Social y Democrático de Derecho.

"El Debido Proceso Legal es la institución del Derecho Constitucional procesal que identifica los principios y presupuestos procesales mínimos que debe reunir todo proceso jurisdiccional para asegurar al justiciable la certeza, justicia y legitimidad de su resultado."

Está integrada a esta garantía genérica, en cuanto es parte indispensable de un enjuiciamiento equitativo que limite el poder del aparato estatal, la garantía del ne bis in ídem, el mismo que tiene un doble significado: procesal, según el cual nadie puede ser enjuiciado dos veces por los mismos hechos, y material, en virtud del cual nadie puede ser sancionado dos veces por una misma conducta.

Esta garantía funciona contra quien es objeto de una imputación penal, sin que a ello objete que se formule en sede judicial, que se esté en cualquier fase del proceso o se tenga o no formalmente la calidad de imputado. Constituye, una manifestación privilegiada del derecho a defenderse de una imputación penal. El imputado tiene el derecho a introducir válidamente al proceso la información que considere adecuada. Él es quien tiene el señorío y el poder de decisión sobre su propia declaración. Sus principales efectos son los siguientes:

- La no declaración no permite inferencias de culpabilidad (no es un indicio de culpabilidad).
- El imputado tiene el derecho de declarar cuantas veces quiera, pues es él quien controla la oportunidad y contenido de las informaciones que desea incorporar al proceso.
- Rige solo cuando se obligue al imputado a emitir una declaración que exteriorice un contenido, de ahí que cuando se le obliga a someterse a una confrontación o careo, a una identificación, a una pericia (dar muestras de sangre, de orina o de cualquier fluido corporal, o muestras caligráficas o someterse compulsivamente a experimentos de voces o a usar determinada ropa, etc.) no se viola esta garantía; en rigor, lo que se protege son las comunicaciones o testimonio del individuo, no la evidencia real o física derivada de la persona del imputado.

"Las Garantías Procesales son las seguridades que se otorgan para impedir que el goce efectivo de los derechos fundamentales sea conculcado por el ejercicio del poder estatal, ya sea limitando ese poder o repeliendo el abuso."

En cuanto se trata de un derecho fundamental, destinado a la protección de todos aquellos que acuden al órgano jurisdiccional en defensa de sus derechos e intereses legítimos, la ley ordinaria no puede impedir la actuación de medios de pruebas sustanciales para la defensa, ni priorizar otros intereses o bienes jurídicos, que no tengan expresa relevancia constitucional o igual nivel.

Junto a la pertinencia, el Derecho ha incorporado otros dos límites extrínsecos a la actividad probatoria: la utilidad y la licitud. La primera es aquella en que por existir una manifiesta inadecuación de medio a fin, se puede conjeturar razonablemente que no alcanzará el resultado pretendido. La segunda es aquella que respeta otros derechos fundamentales y no quebranta disposición ordenatoria alguna de la actividad probatoria.

Este derecho comprende no solo el poder de lograr la comparecencia compulsoria de testigos y peritos, así como la incorporación de todo documento, informe o dato pertinente al proceso. También comprende lograr la información que éstos puedan proporcionar y, en su caso, a posibilitar careos o confrontaciones con testigos de cargo o coimputados. Lo esencial en este último supuesto es asegurar al oponente la oportunidad de contrainterrogar, de formular directamente preguntas y de obtener respuestas inmediatas.

3.3. Algunas consideraciones sobre la configuración del ilícito informático a la luz de la teoría del delito

3.3.1. Antijuridicidad

En el elemento de la antijuridicidad el objetivo es establecer si la conducta prohibida por la legislación es contraria al orden jurídico en general, y por ello al hecho típico y antijurídico se le denomina "injusto". Por el contrario, si el hecho típico está amparado por alguna causa de justificación ya no hay delito.

En la conducta-típica, la preocupación natural de la doctrina, es ocuparse de delimitar si la conducta encuadra en el tipo y podría ser particularmente considerada como una conducta prohibida para el derecho penal, en contrapartida, en la categoría de la antijuridicidad se analiza si esa conducta prohibida se justifica de cara a todo el orden jurídico por las circunstancias materiales que concurrieron en el momento de su realización o si, por el contrario, se constata que el hecho resulta un injusto.

Las precisiones anteriores servirán como punto de partida para establecer el terreno en que deben ubicarse los delitos informáticos, puesto que en su mayoría resultan de nueva creación por el legislador y por lo mismo requieren de una atención especial, ya que en algunos casos su descripción legal no corresponde precisamente a las conductas que originalmente se tuvo presentes para sancionar, errores que en ocasiones por la mala integración de la averiguación previa, posteriormente conducen a

un resultado adverso al no lograrse el enjuiciamiento y dictado de la sentencia correspondiente.

En la doctrina científica del Derecho Penal, las causas de justificación son el negativo de la antijuricidad o antijuricidad como elemento positivo del delito, y son aquellas que tienen la virtud de convertir en lícito un acto ilícito, es decir, que cuando en un acto delictivo aparece una causa de justificación de lo injusto, desaparece la antijuricidad del delito y como consecuencia se libera de responsabilidad penal al sujeto activo.

3.3.2. Acción u omisión

Es la voluntad de las personas de manifestarse mediante un hacer o mediante un no hacer. Esta es una doble caracterización de la "acción", que no quiebra la unidad de la misma, ya que en el no hacer se proyecta al mundo exterior, una manifestación de la voluntad del autor.

En este punto coincidimos en que la gran mayoría de delitos que se cometen mediante sistemas informáticos son delitos de acción positiva, o sea se cometen a través de un hacer. Casos como el Hacking (o mero intrusismo informático), Cracking (como sabotaje informático), Phishing (estafa informática), para citar algunos, siempre se perpetran mediante conductas (acciones positivas) con la voluntad de causar o generar

dichos resultados negativos (desobedecer mandatos imperativos) sobre los bienes jurídicos que vulneran.

Pero, también creemos que es posible, cometer delito de omisión dentro de la especie de delitos informáticos. Aclaramos que no hemos visto regulado en forma específica (por lo menos en la legislación nacional e internacional que pudimos analizar) – lo que no significa que en algún país efectivamente se haya regulado de dicha manera – algún delito informático perpetrado por omisión.

3.3.3. Tipicidad

La tipicidad es importante aclarar la necesidad actual, tanto nacional como a nivel mundial, de tipificar la mayor cantidad de conductas que puedan configurar delitos informáticos. En este sentido, mencionamos en forma precedente, los esfuerzos a nivel mundial, de organismos internacionales, como también de los Estados parte de sistemas de integración regional, en lo que respecta a esta preocupación legislativa.

Adoptar políticas conjuntas en lo que hace a seguridad, ya sea en el uso de Internet, como así también en el comercio electrónico, o en tráfico de datos, es indispensable para lograr un efecto integrador de los instrumentos de control social, a nivel mundial. Además, también encontramos actitudes ilícitas que jurídicamente ya están configuradas como delitos en el ordenamiento penal, pero estimamos que la legislación

debe perfeccionar debido al vertiginoso desarrollo que viene alcanzando el uso de la tecnología informática.

3.3.4. Culpabilidad

La culpabilidad consiste en un juicio sobre el autor mediante el cual se determina si se le puede reprochar el haberse comportado de manera contraria a lo que establece el orden jurídico. La culpabilidad se conforma de tres elementos: la imputabilidad del sujeto, su conciencia sobre la antijuridicidad de la conducta y la ausencia de causas excluyentes de la culpabilidad.

El fortalecimiento de este principio requiere:

1. *La culpabilidad debe establecerse mediante sentencia judicial;*
2. Que la condena se base en prueba que establezca con certeza el hecho criminal y la culpabilidad;
3. Que la sentencia se base en pruebas jurídicas y legítimas;
4. Que la prisión provisional sea una medida cautelar de carácter excepcional para asegurar la presencia del inculpado en el proceso y la realización de la justicia (Artículo 259 del CPP).

CAPÍTULO IV

4. Análisis jurídico de los delitos en redes sociales en Guatemala

Dentro del tema de investigación en los delitos que se cometen en redes sociales de internet en Guatemala pude verificar que existen lagunas legales en las leyes tanto sustantivas como adjetivas.

Guatemala es un país muy vulnerable a recibir ataques en redes sociales ya que no existe regulación alguna por lo que es necesario que los legisladores se capaciten en Derecho Informático, para poder establecer nuevos tipos penales que puedan prevenir y sancionar a los actores de dichos delitos.

Existen redes sociales que claramente establecen en que tribunal y en qué país debe acudir a un litigio o reclamación de usuarios, esta cláusula establece que renuncia al fuera de su domicilio lo que no es conveniente para el usuario, tratándose de un contrato de adhesión, con ningún posibilidad que el usuario pueda proponer condiciones favorables para el mismo. La gran mayoría ni siquiera lee los términos legales y aceptan todas las clausulas para poder aventurarse en un mundo digital.

4.1. Naturaleza Jurídica de servicios de redes sociales

Para establecer la naturaleza jurídica se analiza la relación obligacional que surge de la prestación del servicio entre la empresa titular del sitio web y el usuario, estaríamos claramente ante un contrato por adhesión.

Los contratos por adhesión son aquellos en los cuales el contenido contractual ha sido determinado con prelación, por uno solo de los contratantes, al que se deberá adherir el co-contratante que desee formalizar la relación jurídica obligatoria.

En el contrato de adhesión las cláusulas están dispuestas por uno solo de los futuros contratantes de manera que el otro no puede modificarlos o hacer otra cosa que aceptarlas o rechazarlas. El usuario al realizar el proceso de registración en cualquier sitio web que preste este tipo de servicios, tales como Facebook, Hi5, Orkut, debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente.

La naturaleza jurídica del contrato que rige la relación, llamados comúnmente "Términos de Uso" (Terms of Service), "Términos y condiciones", Políticas de Privacidad (PrivacyPolicy), es la de un contrato por adhesión.

Una de las problemáticas jurídicas que se plantea de acuerdo a la naturaleza jurídica de estos contratos en Internet, lo es en torno al verdadero consentimiento informado del usuario al aceptar las cláusulas en el momento de la registración, ya que la mayoría de los usuarios no suelen leer detenidamente los términos y condiciones del sitio web.

Según lo expresa el Dr. Ricardo Lorenzetti: "la regla es la disminución de la información que se obtiene para actuar, derivada de su alto costo marginal y de oportunidad; disminuye la racionalidad y aumenta la fe en los sistemas complejos, distantes, abstractos, que llega a ser casi religiosa. El acto de relacionamiento con el sistema se automatiza, se simplifica de modo que el sujeto que lo celebra no tiene conciencia de sus efectos jurídicos"[24].

No se trata de discriminar ni restarle validez al consentimiento del usuario expresado por medios electrónicos, el cual es perfectamente válido, sino de plantear la problemática típica de los contratos por adhesión llevada al ámbito de internet en relación a la información necesaria que debe tener el usuario a fin de actuar con un debido consentimiento informado en la manifestación de su voluntad al hacer "click" en "Acepto", o tildar la casilla de aceptación.

4.2. Derecho a la protección de información personal

Analizando la ley de acceso a la información pública protege la información que se encuentra en poder de la administración pública, así como el libre acceso a todas las instituciones y dependencias del estado.

Por lo que la protección de información personal en lasas redes sociales cuentan con un nivel de riesgo superior a las páginas web tradicionales, dado que los usuarios exponen no solo sus datos de contacto o información profesional como formación,

[24](LORENZETTI, Ricardo Luis. **La oferta como apariencia y la aceptación basada en la confianza**. Revista de Direito do Consumidor 35/11. Sao Paulo, 2000, p.12.)

experiencia laboral, sino que se pueden exponer de manera pública las vivencias, gustos, ideología y experiencias del usuario, lo que conlleva que el número de datos de carácter personal puestos a disposición del público. Asimismo, se tratan datos especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado. En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa, etc.

El principio básico de ésta norma legal consiste en que los datos son propiedad del usuario mientras él mismo no permita su uso a una empresa o a un tercero. La autorización se concede, por ejemplo, al rellenar un formulario de adhesión que permite el acceso a un sitio.

4.3. Propiedad intelectual en las redes sociales

La realidad de los delitos que se comentes en redes sociales es una forma fácil de reproducir y distribuir contenidos de Internet uno de los principales medios de crecimiento para los contenidos de propiedad intelectual, al tiempo que supone uno de

los principales retos en lo que respecta al control y protección de los derechos de autor, en la medida en que los contenidos se encuentran en formato digital y, por tanto, su distribución y comunicación pública es mucho más sencilla que en otro tipo de formato.

Los posibles riesgos que se pueden producir contra la protección de la propiedad intelectual en Internet y en los servicios de redes sociales. Muchos usuarios se ven afectados de los contenidos que son titularidad de terceros y que el usuario decide publicar dentro de la red social sin autorización de los titulares del derecho de propiedad intelectual.

En estos supuestos el usuario se encuentra violando derechos de autor, y en consecuencia deberá responder por los daños y perjuicios.

Una problemática que se presenta en relación a este punto, es cuando los usuarios deciden dar de baja su suscripción o "cuenta" a la red social, siendo que en ese caso se debería dejar de difundir y publicar los contenidos de su autoría.

A causa de este tipo de situaciones, este año la red social Facebook.com decidió modificar unilateralmente sus términos y condiciones estableciendo que los usuarios cedían y licenciaban de manera irrevocable y perpetua sus contenidos a la empresa norteamericana, argumentando la necesidad de seguir contando con esos contenidos online en caso de que el usuario diera de baja su cuenta.

Esto causó un revuelo en los internautas, que recibieron la noticia con gran descontento, lo que obligó a la empresa a retornar a su política anterior.

La propiedad intelectual en los sitios de redes sociales viene a perjudicar al empresario que se dedica al desarrollo de contenido digital, en vista que es de fácil distribución y cualquier persona que tenga acceso a internet pueda copiar el contenido del creador. En la actualidad en Guatemala existen lagunas legales respecto al respeto de los Derechos de Propiedad Intelectual en los sitios de redes sociales de internet.

Por este motivo, es importante que los usuarios conozcan qué ocurrirá con sus obras una vez que son publicadas en una red social y que exista alguna forma de supervisión y control de contenidos.

Asimismo, puede ocurrir que el contenido publicado de un usuario permanezca disponible para el público aun habiendo solicitado la baja de la plataforma o red social, el problema principal que se plantea es la imposibilidad técnica de controlar o supervisar contenidos por parte de los prestadores de servicios de internet (ISP).

4.4. Análisis de aporte en el derecho comparado sobre los delitos en redes sociales de internet

En el presente trabajo de investigación pude analizar a través de un cuadro comparativo de las medidas que se han tomado a nivel latinoamericano para atender el problema de la criminalidad informática, debe analizarse a la comunidad internacional latinoamericana, su forma de abordar el problema y su incidencia en cuanto a falta de consensos sobre delitos informáticos, definición jurídica, conductas delictivas, así como la falta de tratados sobre extradición.

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos y especialmente en redes sociales, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

Alemania: Este país sancionó en 1986 la Ley contra contempla los siguientes delitos; Espionaje de datos, datos, sabotaje informático, estafa informática, alteración de datos cibernéticos.

Austria: La Ley de reforma del Código Penal, sancionada el 22 de diciembre de 1987, en el Artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o

por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Inglaterra: Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

El hecho de liberar un virus tiene penas desde un mes a cinco años de cárcel, dependiendo del daño que causen, cual se penaliza el hacking, el phreaking (utilización de servicios de telecomunicaciones aviando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus para dañar el sistema de cómputo en cuanto a la tecnología virtual.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará un mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta cuatro años de prisión.

Francia: En enero de 1988, se dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta Ley tipifica en el Artículo 462 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte, el Artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).
Por último, esta Ley en el Artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

España: En el Código Penal de España de 2009, el Artículo 263 establece que, el que causare daños en propiedad ajena. En tanto, el Artículo 264-2 preceptúa, aplicará la

pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa. Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreaking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

4.5. Propuesta de reforma al Código Penal Decreto Número 17-73

Proyecto de reforma

DECRETO NÚMERO 19-2015

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que el Derecho Penal es un derecho realista y objetivo, debe estudiar al futuro Delito en su realidad social y debe resolver los casos determinados a base de una bien entendida equidad, es indispensable enfocar ante todo la posición no solo económica sino social de los futuros tipos penales frente al Juez, previendo y resolviendo los diversos problemas que con motivo de su aplicación surjan, con criterio social y a base de hechos concretos y tangibles.

POR TANTO:

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

DECRETA:

La siguiente:

Reforma al Artículo 164 del Decreto 17-73 del Congreso de la República de Guatemala

ARTÍCULO1. Reforma del Artículo 164 Bis, el cual queda así:

ARTÍCULO 164 Bis. Comete delito de difamación electrónica quien utilice cualquier medio electrónico para difundir, revelar ceder o transmitir una o mas imágenes, grabaciones audiovisuales o texto para causarle a una o varias personas deshonra, descrédito, perjuicio o exponerla al desprecio y humillación pública.

Al responsable de este delito se le impondrá una pena de prisión de uno a cinco años Inconmutables y multa de cinco mil a diez mil quetzales. Si la víctima es menor de edad, la sanción será de cinco a diez años de prisión inconmutables y una multa de diez mil a veinte mil quetzales.

ARTÍCULO2. Reforma del Artículo 164 Ter, el cual queda así:

ARTÍCULO 164 Ter. Quien utilice medios electrónicos de redes sociales con engaño y promesa de beneficios económicos o remuneraciones laborales para realizar actos con fines sexuales o eróticos a otra persona, será sancionado con prisión d cinco a diez años.

La pena señalada en el párrafo anterior se aumentara en una tercera parte si de los hechos indicados hubiera secuestro o muerte de la persona

ARTÍCULO 3. El presente Decreto entrará en vigencia el día siguiente de su publicación íntegra en el diario oficial.

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

DADO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, A_____ DÍAS DEL MES DE_____ DE DOS MIL QUINCE.

CONCLUSIÓN DISCURSIVA

Las nuevas tecnologías de la información, han sido utilizadas por la delincuencia y comúnmente a través de redes sociales de la Internet, siendo estas en Guatemala un lugar donde se puede realizar cualquier delito de esta materia, ya que no existe una norma que tipifique y regule la comisión de un sinfín de delitos en redes sociales de la Internet.

Actualmente los jueces del ramo penal del municipio de Guatemala, departamento de Guatemala, emiten sentencias que no se adecuan a la actualidad, al no estar tipificados en la legislación guatemalteca, por lo tanto muchos casos se llegan a sobreseer.

En la práctica muchas denuncias no logran su objetivo al no poder plantear su teoría del delito, ya que deben cambiar el delito, al no estar tipificado los delitos cometidos por medio de las redes sociales de la Internet. Por lo que es necesario proponer al Congreso de la República de Guatemala reforme el Libro Segundo Título VI Capítulo VII del Código Penal e incluir los delitos que se comenten en redes sociales de la Internet, esto con el afán que en los juicios se logren las sentencias adecuadas a la realidad.

Esta reforma aplica al actual Ministerio Público, Institución que tendría que crear una Fiscalía de Delitos Cibernéticos para contar con especialistas en la materia, que puedan reducir los índices delincuenciales en redes sociales de la Internet.

BIBLIOGRAFÍA

CÁMPOLI, Gabriel Andrés. **Delitos informáticos en la legislación mexicana. Instituto Nacional de Ciencias Penales.** México 2007.

ESTRADA GARAVILLA, Miguel. **Delitos informáticos**. www.derecho.org Evolución Tecnologías Web. http://tecnoinfocomgaleoncom/evolucionwebpdf.

GARRONE. José Alberto. **Diccionario jurídico elemental**. Buenos Aires, Argentina. Ed. AbeledoPerrot, 1993.

GONZALEZ, FREA, Leandro. **Aspectos legales de las redes sociales: Legislación normativa, Facebook, regulaciones legales en Argentina**.

GONZÁLEZ FREA, Leandro. **Contratación de Servicios Turísticos por Internet, consentimiento, condiciones generales de contratación.**

LÓPEZ BETANCOURT, Eduardo. **Delitos en particular**. México, Editorial Porrúa, 2001.

REYNA ALFARO, Luis. **"Pornografía e Internet: aspectos penales"**, Argentina. AR: Revista de Derecho Informático.

VELÁZQUEZ ELIZARRARAS, Juan Carlos. **Instauración de un marco legal internacional de internet**. México.

Guías de ayuda para la configuración de la privacidad y seguridad de las redes sociales, proyecto de investigación conjunto entre INTECO y la Universidad Politécnica de Madrid, España.

http://es.wikipedia.org/wiki/Delito(Consulta, 15/07/2014)

http://es.wikipedia.org/wiki/Internet(Consulta, 20/07/2014)

http://www.alegsa.com.ar/Dic/delito%20informático.php(Consulta, 20/07/2014)

http://www.cxo-community.com/articulos/blogs/blogs-seguridad-informatica/2701-**delitos-en-las-redes-sociales** (Consulta, 20/07/2014)

http://www.elnuevodia.com/cuandolasleyesseenfrentanalasredessociales-973707.htm1 **Cuando las leyes se enfrentan a las redes sociales**. (Consulta, 22/07/2014)

http://www.franciscocontreras.org/ **ley-de-delitos-informáticos** (Consulta, 22/07/2014)

http://www.informatica-hoy.com.ar/redes-sociales/**La-historia-de-las-redes sociales**.php (Consulta, 22/07/2014)

http://www.justiniano.com/revista_doctrina/delitoinformatico.htm**delito informático** (Consulta, 13/08/2014)

http://www.tuabogadodefensor.com/**proteccion-redes-sociale**s/#tipos(Consulta, 20/08/2014)

http://wvvw.m.tecnológico.com/Main/AntecedentesHistoricosRedes.**Antecedenteshistó ricos de las redes sociales** (Consulta, 25/08/2014)

http://www.monografias.com/trabajos64/contratos-mercantiles-guatemala/contratos-mercaniiles-guatemala2.shtml **Contratos Mercantiles en Guatemala** (Consulta, 29/08/2014)

http//www.pabloburgueno.com/2009/03/clasificación de redes-sociales/, **Clasificación de las redes sociales,** (Consulta, 10/09/2014)

http://www.uncjin.org/Documents/congr10/10s.pdf, **Décimo Congreso de las Naciones Unidas**, (Consulta, 20/09/2014)

http://aprenderinternet.about.com/od/SeguridadPrivacidad/tp/Siete-Practicas-Para-Proteger-Tu-Privacidad-En-Facebook.htm, **Aprende Internet**, (Consulta, 28/09/2014)

Legislación:

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

Declaración Universal de los Derechos Humanos.

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

Ley de Propiedad Intelectual. Congreso de la República de Guatemala, Decreto número 57-2000.