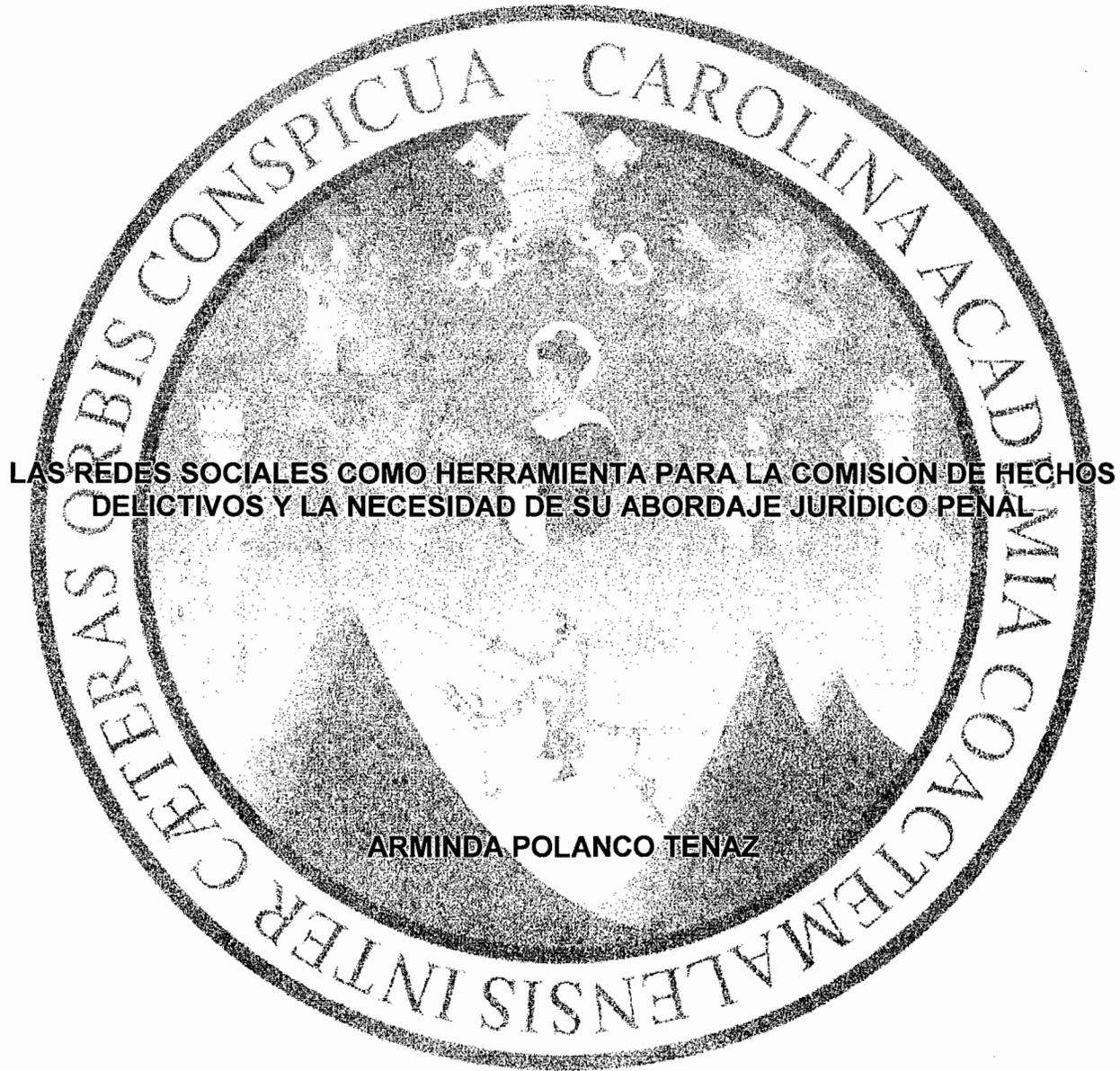


Handwritten mark or signature.

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



**GUATEMALA, SEPTIEMBRE 2015**

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

LAS REDES SOCIALES COMO HERRAMIENTA PARA LA COMISIÓN DE HECHOS  
DELICTIVOS Y LA NECESIDAD DE SU ABORDAJE JURÍDICO PENAL



**Abogada y Notaria**

Guatemala, septiembre 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 PRACTICÓ EL  
EXAMEN TÉCNICO PROFESIONAL**

Primera fase:

Presidente:	Lic. Héctor David España Pinetta
Vocal:	Lic. José Dolores Bor Sequen
Secretario:	Lic. José Luis Guerrero

Segunda fase:

Presidente:	Lic. Edwin Leonel Bautista Morales
Vocal:	Lic. Jorge Mario Yupe Cárcamo
Secretaria:	Lic. Ileana Noemí Villatoro Fernández

**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).



UNIDAD DE ASESORÍA DE TESIS FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.  
 Guatemala 19 de agosto de 2014.

Atentamente pase a el LICENCIADO JORGE MARIO LÓPEZ ARGUETA , en sustitución del asesor propuesto con anterioridad LICENCIADO DIXON DIAZ MENDOZA, para que proceda a asesorar el trabajo de tesis de la estudiante ARMINDA POLANCO TENAZ, carné:199822382 intitulado "LAS REDES SOCIALES COMO HERRAMIENTA PARA LA COMISIÓN DE HECHOS DELICTIVOS Y LA NECESIDAD DE SU ABORDAJE JURÍDICO PENAL".

Me permito hacer de su conocimiento que está facultado para recomendar a la estudiante, si así lo estima conveniente la modificación del bosquejo preliminar de temas y de las fuentes de consulta originalmente contempladas, asimismo, el título del punto de tesis propuesto. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

  
 DR. BONERGE AMILCAR MEJIA ORELLANA  
 JEFE DE LA UNIDAD DE ASESORÍA DE TESIS

cc.Unidad de Tesis, interesado y archivo  
 BAMO/iyf.

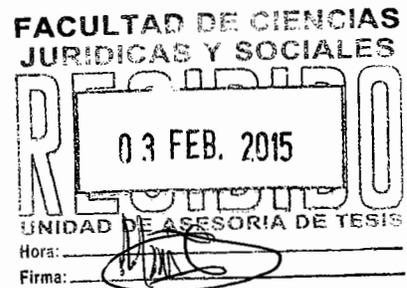


Lic. Jorge Mario López Argueta  
Abogado y Notario  
Colegiado 9,503

11 calle 8-14 zona 1, 2do. Nivel oficina 25, Edificio Tecún



**Dr. Bonerge Amilcar Mejía Orellana**  
**Jefe de la unidad de asesoría de tesis**  
**Facultad de ciencias jurídicas y sociales**  
**Su despacho.**



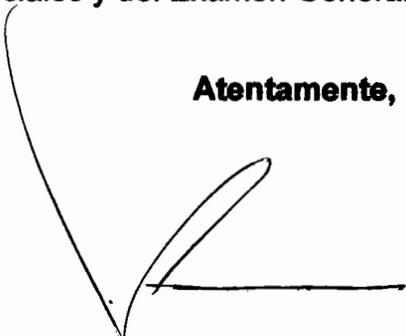
De conformidad con la resolución de nombramiento de fecha diecinueve de agosto del año dos mil catorce, recaído en mi persona, me permito informar a usted que he asesorado el trabajo de tesis de la Secretaria Bilingüe ARMINDA POLANCO TENAZ, intitulado "LAS REDES SOCIALES COMO HERRAMIENTA PARA LA COMISIÓN DE HECHOS DELICTIVOS Y LA NECESIDAD DE SU ABORDAJE JURÍDICO PENAL", para lo cual me permito manifestar lo siguiente:

1. La tesis abarca un contenido científico y técnico, analizando jurídicamente lo fundamental que es la necesidad de proteger a la población guatemalteca de las personas que delinquen mediante los mecanismos técnicos actuales especialmente las redes sociales.
2. La bachiller ARMINDA POLANCO TENAZ, en la elaboración de su tesis utilizó un lenguaje correcto y el contenido de la misma es de interés para la ciudadanía guatemalteca. El trabajo es un aporte científico tanto para los estudiantes, catedráticos y profesionales a quienes interese el tema. Dicho aporte merece ser tomado en cuenta por ser un impacto social, que afecta a los guatemaltecos en general.
3. Los métodos y técnicas utilizados por la sustentante para la elaboración de su tesis fueron acordes para el desarrollo de la misma. La sustentante utilizó los métodos analítico-sintéticos con los cuales determino la importancia del tema trabajado. Mediante el sistema inductivo-deductivo estableció la realidad que viven muchas personas que ven amenazada su privacidad por personas que utilizan la tecnología para cometer delitos. Durante el desarrollo del presente trabajo utilizó las técnicas bibliográficas y la entrevista, con la cual obtuvo la información acorde para la elaboración de la tesis con datos actualizados.



4. Las conclusiones y recomendaciones planteadas por la sustentante son acordes y se relacionan con el contenido de la tesis, en virtud que dejan evidenciado la necesidad de regular lo relativo al uso de las redes sociales.
5. La bibliografía utilizada en la elaboración de la tesis es la adecuada y actualizada. De manera personal me encargué de guiar a la estudiante en los lineamientos de todas las etapas correspondientes al proceso de investigación científica, aplicando para el efecto los métodos y técnicas acordes para resolución de la problemática relacionada.
6. El trabajo de tesis efectivamente reúne los requisitos de carácter legal, por lo que me permito emitir **DICTAMEN FAVORABLE** de conformidad con el cumplimiento de los requisitos establecidos en el Artículo treinta y dos (32) del Normativo para la Elaboración de Tesis de Licenciatura en ciencias Jurídicas y Sociales y del Examen General Público.

**Atentamente,**



*Lic. Jorge Mario López Argueta*  
ABOGADO Y NOTARIO

**Lic. Jorge Mario López Argueta.**

**Asesor.**

**Colegido 4163**



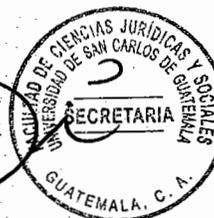
**USAC**  
**TRICENTENARIA**  
Universidad de San Carlos de Guatemala



DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 02 de julio de 2015.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante ARMINDA POLANCO TENAZ, titulado LAS REDES SOCIALES COMO HERRAMIENTA PARA LA COMISIÓN DE HECHOS DELICTIVOS Y LA NECESIDAD DE SU ABORDAJE JURÍDICO PENAL. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

BAMO/srrs.



Lic. Aridán Ortiz Orellana  
**DECANO**





## DEDICATORIA

- A DIOS: Por ser ese ser maravilloso, que me inspira, me motiva y me da vida. Me llena de sabiduría e inteligencia para poder alcanzar mis objetivos, hacer realidad mis sueños, realizar mis proyectos y llegar a la meta. Y todo lo encomiendo en sus manos para que sea ejemplo de justicia y derecho, el mejor abogado a quien debo seguir, gracias por existir.
- A MI ESPOSO: Porque me ha acompañado, siempre me ha dado su apoyo y su presencia me ha motivado.
- A MIS HIJAS: A esas pequeñitas que con su linda sonrisa y su ternura, me llenan de alegría mi vida.
- A MIS PADRES: Gracias porque me han transmitido grandes valores porque son para mí ejemplo de honestidad sencillez de lucha y espiritualidad, gracias por su amor que es recíproco.
- A MIS HERMANOS: Especialmente quiero hacer un reconocimiento a Concepción, Sonia y Addy, porque han sido para mí además de hermanos, padre y madre. Así mismo, a Josefina, Miriam, Misael, Gregorio, Dalila, Geovanny, Roxy para todos mi más gran admiración, los amo con todo mi corazón.



A MIS SUEGROS: Todo mi respeto y cariño.

A MIS CUÑADOS: Especialmente a Glenda Sandoval, por su gran apoyo incondicional.

A MIS SOBRINOS: Paty, Luis, Osvin, Stancy, Mayra, Marleny, Idania, Karen, Alejandro, Skarlet, Samantha, André, Josué, Ángel, Yoami, Juan Pablo, Mishelle, Pablo, Cristian gracias por su cariño.

A mis compañeros: Samuel, Víctor, William, Claudia, Kenny, Rafael, Hugo, Ligia, Lucky, Genobeba y especialmente Darlee Gramajo, por su apoyo y cariño.

A: La Facultad de Ciencias Jurídicas y Sociales por proveerme de conocimiento, por su gran enseñanza profesional y científica, para poder alcanzar la meta.



## ÍNDICE

Pág.

Introducción .....	i
--------------------	---

### CAPÍTULO I

1. Aspectos doctrinales relacionados con el derecho informático y la teoría del delito ....	1
1.1. Antecedentes de la problemática .....	1
1.2. Origen etimológico de la palabra cibernética e informática .....	2
1.3. Definición de derecho informático .....	2
1.4. Naturaleza jurídica del derecho informático .....	3
1.5. Diferentes acepciones de la palabra informática jurídica .....	4
1.6. Informática jurídica operacional o de gestión .....	5
1.7. Informática jurídica registral .....	6
1.8. Informática jurídica documental.....	7
1.9. Regulación del derecho informático .....	7
1.10. Aspectos doctrinarios relacionados con el concepto delito .....	8
1.10.1. Concepto y origen etimológico de delito.....	8
1.10.2. División tripartita del concepto delito.....	8

### CAPÍTULO II

2. Los delitos informáticos .....	13
2.1. Aspectos generales de los delitos informáticos .....	13
2.2. Concepto de delito informático .....	13
2.3. Sujetos que participan en la comisión de los delitos informáticos .....	14



Pág.

2.3.1. Sujeto activo .....	14
2.3.2. Sujeto pasivo .....	16
2.4. Definición de los delitos informáticos.....	17
2.5. Características de los delitos informáticos.....	18
2.6. Clasificación de los delitos informáticos .....	20
2.7. Bienes jurídicos tutelados.....	20
2.8. Delitos contra el patrimonio y la propiedad intelectual.....	21
2.9. Delitos informáticos que atentan contra la privacidad, la intimidad y la indemnidad sexual .....	24

### **CAPÍTULO III**

3. Las redes sociales y la comisión de hechos delictivos .....	27
3.1. Antecedentes de los diferentes medios informáticos.....	27
3.2. Clasificación y tipos de redes sociales .....	31
3.2.1. Primera clasificación de redes sociales, en atención al grupo objetivo a quienes se dirigen y el eje temático que desarrollan .....	32
3.2.2. Segunda clasificación de redes sociales, en atención al sujeto de la relación .....	34
3.2.3. Tercera clasificación, en atención al área geográfica en la que se ubican y por su movilidad se subdividen en .....	35
3.2.4. Cuarta clasificación, en atención al espacio y/o la plataforma en la que se expanden se dividen en .....	35
3.3. Aspectos derivados del uso de las redes sociales.....	36

3.4. Características de las redes sociales .....	38
3.5. La problemática jurídica de las redes sociales .....	38
3.6. Protección de datos personales .....	45
3.7. Derechos de propiedad intelectual en las redes sociales .....	46
3.8. Delitos informáticos en las redes sociales .....	48

#### **CAPÍTULO IV**

4. Diversas modalidades en la comisión de hechos delictivos a través de las redes sociales y la urgente necesidad de que se incluya en el Código Penal.....	51
4.1. Aspectos considerativos .....	51
4.2. Acciones delictivas tipificadas en la legislación penal guatemalteca .....	52
4.2.1. Delitos que atentan la indemnidad sexual .....	52
4.2.2. Delitos de explotación sexual .....	53
4.2.3. Implementación de la ley contra el femicidio y otras formas de violencia contra la mujer.....	54
4.2.4. De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos .....	55
4.3. La era de la tecnología y las comunicaciones dentro del ámbito guatemalteco .	64
4.4. Guatemala supera un índice elevado en el uso de teléfonos móviles .....	66
4.5. Forma de comisión de los delitos a través de las redes sociales .....	67
4.5.1. El Modus operandi de los delincuentes informáticos.....	67
4.5.2. Presupuestos del ciber crimen en la red .....	68
4.5.3. Ley de Registro móvil para la prevención y el combate del delito .....	70



**Pág.**

4.6. Las nuevas modalidades delictivas a través de las redes sociales.....	71
4.6.1. Delito de trata de personas y los nuevos avances tecnológicos.....	71
4.7. Institucionalización del día internacional contra el delito de trata de personas..	74
4.8. Sumario de acontecimientos relacionados con el uso inapropiado de las redes sociales.....	75
4.8.1. Caso facebook.....	75
4.8.2. Caso de sexting y acoso sexual en el departamento de Jalapa .....	76
4.9. Influencia negativa .....	77
4.10. Víctimas de sociópatas .....	78
<b>CONCLUSIONES .....</b>	<b>83</b>
<b>RECOMENDACIONES.....</b>	<b>85</b>
<b>ANEXOS.....</b>	<b>87</b>
<b>BIBLIOGRAFÍA.....</b>	<b>99</b>



## INTRODUCCIÓN

El objetivo de este trabajo de tesis de grado es determinar en qué consiste las redes sociales, como funcionan y los ilícitos que se cometen a través de ellas, analizando dos casos y lo que sucede en la legislación comparada, especialmente en cuanto a las nuevas modalidades acerca de los delitos de extorsión, secuestros, acosos sexuales, pornografía infantil, entre otros, determinando la necesidad de que estas se incluyan en el Código Penal.

En alusión a las técnicas empleadas para la realización de esta investigación es menester indicar que fueron de gran ayuda análisis de documentales, material recopilado de delitos cometidos y estudios sobre el tema de delitos informáticos. Las fichas bibliográficas se utilizaron para documentar las diferentes fuentes citadas. Así también estadísticas, gráficas e índices referenciales de los cambios de modalidad de modus operandi de la delincuencia en la actualidad, se realizaron entrevistas a las personas usuarias de los diferentes medios informáticos para el análisis de este trabajo de tesis de grado.

Las ciencias jurídicas han observado una ágil recaudación con respecto a los niveles de modernización y actualización relacionadas tanto en sistemas de operatividad como lo relacionado con la información jurídica.



Para una mejor comprensión, el trabajo ha sido dividido en cuatro capítulos: En el primer capítulo, se desarrollan los conceptos relacionados con aspectos doctrinales relacionados con el derecho informático y la teoría del delito; el capítulo dos, se encuentra lo relativo a la naturaleza propia de los delitos informáticos y la amplia incidencia en la actualidad; el capítulo tres, contiene conceptos relacionados con las redes sociales, desde su origen, clasificación, utilidad, ventajas y desventajas, así como los riesgos; el capítulo cuatro, conceptualiza las diversas modalidades en la comisión de hechos delictivos a través de redes sociales y la urgente necesidad de que se incluya en la legislación penal guatemalteca. Finalmente se encuentran las conclusiones, recomendaciones, bibliografía y una sección de anexos que brinda de manera gráfica el resultado obtenido a través de la presente investigación.

Los métodos utilizados para esta investigación fueron el analítico, en la cual se estudió la legislación internacional el cual protege los derechos de los usuarios para el uso adecuado de las redes sociales; el deductivo para establecer que en la legislación nacional especialmente en el Código Penal aún no se encuentra tipificado el delito de protección de la identidad del usuario de redes sociales; por último los métodos de la síntesis y la inducción que permitieron establecer que es necesario incorporar al ordenamiento jurídico una sanción para aquellos que violen los derechos de los usuario de redes sociales; la técnica bibliográfica permitió la recolección y el análisis del material de referencia, esperando que la propuesta sea tomada en cuenta por las autoridades de Guatemala.



## CAPÍTULO I

### **1. Aspectos doctrinales relacionados con el derecho informático y la teoría del delito**

#### **1.1 Antecedentes de la problemática**

En la actualidad, las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria de los ciudadanos en todo el mundo y además desempeñan un papel fundamental en el éxito de la economía universal.

Cada vez son más las redes interconectadas así como mayor la convergencia de los sistemas de información y las redes. Esta tendencia implica sin duda numerosas y evidentes ventajas, pero van acompañadas también de un riesgo inquietante que se traduce en la presencia de ataques malintencionados en contra de los sistemas de información.

Dichos ataques pueden adoptar diversidad de formas, incluido el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicio. Cabe mencionar que es posible realizar este tipo de acciones perjudiciales desde cualquier lugar hacia el resto del mundo y en cualquier momento.

Este tipo de maniobras contra los sistemas de información, constituyen una amenaza para la creación de una sociedad de la información más segura y en un espacio de libertad, seguridad y justicia, por lo que es importante abordar la temática con la mayor seriedad posible.

## 1.2 Origen etimológico de la palabra cibernética e informática

El término cibernética proviene del griego Kybernees (timonel o gobernador) fue aplicado por vez primera en el año de 1948 por el matemático estadounidense Norbert Wiener, refiriéndose a la teoría de los mecanismos de control. “Esta ciencia surgió de los problemas planteados durante la segunda guerra mundial, al desarrollar los denominados cerebros electrónicos y los mecanismos de control automático en el equipo militar”<sup>1</sup>. Cabe mencionar que el matemático no tenía noción del auge que alcanzaría esta ciencia. La palabra informática es un neologismo derivado de los vocablos información y automatización, este término fue sugerido por Phillippe Dreyfuss en el año de 1962, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones. El Diccionario de la Real Academia de la Lengua Española **RAE** define a la informática de la siguiente manera: “Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de ordenadores.”<sup>2</sup>

## 1.3 Definición de derecho informático

De conformidad con el tratadista Julio Téllez, se define concretamente así: “Ciencia del derecho que aplica las nuevas tecnologías en el campo de las ciencias jurídicas y el sinnúmero de actos y contratos que deben revestir el amparo y la legalidad en todas y cada una de sus fases.”<sup>3</sup>

---

<sup>1</sup>Weiner, Norbert, Cibernética, **Control y Comunicación**, Pág. 191

<sup>2</sup>**Diccionario de la Real Academia Española**. Versión Digital

<sup>3</sup>Téllez Valdés Julio Alejandro **Delitos Informáticos** Pág. 15

Se define como un conjunto de principios y normas que regulan los efectos jurídicos. Es la rama del derecho especializado en el tema de la informática, regula sus usos, aplicaciones e implicaciones legales.

El derecho informático: Es el sector normativo de los sistemas dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir la informática y la telemática.

#### **1.4 Naturaleza jurídica del derecho informático**

El derecho informático suele tener implicaciones jurídicas dentro del ámbito del derecho público, relacionado con la regulación del flujo internacional de datos informatizados que interesan al derecho internacional público, así como la libertad informática o bien la defensa de las libertades frente a eventuales agresiones perpetradas por la tecnología de la información y las comunicaciones objeto de especial atención por parte del derecho constitucional y del derecho administrativo, y a los delitos informáticos que son objeto de investigación y estudio, del derecho penal.

De igual manera el derecho informático, incide directamente en el campo del derecho privado, observando cuestiones relacionadas con: Contratos de adhesión, contratos de arrendamiento, leasing, copropiedad y demás asuntos relacionados con la contratación de servicios a distancia.



En resumen puede establecerse que por tener pertenencia recíproca dentro del ámbito de acción del derecho público y del derecho privado; el derecho informático está considerado como una rama autónoma del derecho, que responde a la continua demanda de actualización impuesta por el alto grado de avance tecnológico.

El derecho informático es una rama de las ciencias jurídicas que contempla a la informática desde 2 puntos de vista diversos:

1. Como instrumento: Informática jurídica y
2. Como objeto de estudio: Derecho de la informática.

El eje de acción de la informática jurídica se define como el conjunto de aplicaciones en el ámbito del derecho, es además una técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática en general, aplicables a la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesaria para lograr dicha recuperación.

### **1.5 Diferentes acepciones de la palabra informática jurídica**

Inicialmente se utilizó el término "JURIMETRICS"<sup>4</sup> (Jurimetría) esta modalidad fue creada por el juez estadounidense Lee Loevinger en el año 1940.

---

<sup>4</sup>Loevinger Lee **Minnesota Law Review** Vol. No. 34 Pág. 16

Posteriormente fue reconocido con el término “IUSCIBERNETICA, es decir la ciencia cibernética aplicada a la ley o al derecho, término promulgado por el tratadista Mario G. Lozano”.<sup>5</sup> Lo básico en todo caso es dejar específicamente la gran incidencia que la informática ha aportado al desarrollo y actualización en las ciencias jurídicas y sociales.

Básicamente se puede traducir en operaciones claves dentro del ambiente administrativo y judicial, de tal forma que se puede enunciar así:

- Informática jurídica operacional o de gestión
- Informática registral e
- Informática documentaria o documental.

### **1.6 Informática jurídica operacional o de gestión**

Esta rama de la informática es la que organiza el desarrollo de las actividades jurídico adjetivas, es decir esta rama se encarga de establecer el margen de aplicación, admisión y emisión de documentos. El sistema digital en relación y acción conjunta con los operadores de justicia, facilita el monitoreo de manera eficaz y permite conocer los motivos por los que una averiguación, consulta o asunto por resolver, se encuentra en reserva, o pendiente de resolver. Con ello se erige un serio obstáculo que es común en la práctica, consistente en que un expediente se archive maliciosamente, es decir que evita el soborno y corrupción de los empleados públicos.

---

<sup>5</sup> Lozano Mario, **Sociología del Delito** Pág. 10



## 1.7 Informática jurídica registral

“Se ocupa de todo tipo de registros, sean estos públicos o privados. Su objetivo es facilitar a los usuarios los datos fehacientes y los documentos que amparan dicha información que obra dentro del registro, dicha labor es eficaz, inmediata, situación que agiliza y disminuye el engorroso retraso burocrático y la corrupción.”<sup>6</sup>

Los sistemas operativos registrales cuentan con toda clase de control a nivel de seguridad y confiabilidad en el resguardo de la información que obra dentro de los mismos.

La informática registral además de facilitar el archivo y la búsqueda de datos permite llevar a cabo labores complementarias como la estadística entre otras.

Para formar, organizar y actualizar archivos y registros, el computador cuenta con varios recursos entre los cuales se puede mencionar:

- a) El procesador de datos: que permite introducir cualquier texto en el computador, modificando el formato o aplicación que se requiera.
- b) Gestor de base de datos; permite mayor capacidad de almacenamiento en menos tiempo y menos espacio, adicional a ello contribuye con la eficiencia y facilidad en el momento de recuperar la información, así como en la búsqueda de datos que obran en los registros.

---

<sup>6</sup> Téllez Valdés **Ob.cit.** Pág. 20

## **1.8 Informática jurídica documental**

La información jurídica está contenida en diversidad de fuentes tales como: manuscritos, libros, enciclopedias, digestos, archivos físicos, etc. pero fundamentalmente se encuentra en leyes, reglamentos, circulares, dictámenes, instrucciones, etc.

La informática jurídica documental provee al usuario interesado un amplio banco de datos y referencias bibliográficas, al cual se puede acceder de manera inmediata por medio de una visita al sitio o de la página institucional respectiva.

## **1.9 Regulación del derecho informático**

“El derecho informático deberá contar con una legislación integral que incluya los siguientes aspectos:

- Regulación de la información, ya que la información como bien requiere un tratamiento jurídico.
- Protección de datos personales y resguardo del Derecho a la privacidad.
- Regulación de jurídica del Internet.
- Propiedad Intelectual: Referente a los derechos de autor, uso y registro y regulación de nombres de dominio ambos derivados de las acciones de piratería o ciberocupación.
- Delitos Informáticos: La comisión de actos ilícitos en los que se utilicen el sistema de cómputo como instrumento o como fin.

- Contratos Informáticos: En función de esta categoría contractual particular con evidentes repercusiones fundamentalmente económicas.

Comercio electrónico: A fin de regular las nuevas tendencias de comercialización automatizada de bienes y servicios y el uso de la firma digital.”<sup>7</sup>

## **1.10 Aspectos doctrinarios relacionados con el concepto delito**

### **1.10.1 Concepto y origen etimológico de delito**

Etimológicamente la palabra delito deviene de la raíz en latín Delinquere, que se traduce como la acción malsana e intencionada cuya finalidad específica es provocar daño.

Delito es el acto típicamente antijurídico, culpable, sometido a una penalidad.

El jurista Franz Von Litz lo define así: Delito es un acto humano culpable, contrario al Derecho y sancionado con una pena.

Por su parte el tratadista Ricardo Nieves agrega: “El delito es una acción típica, antijurídica, culpable subsumible bajo una sanción penal adecuada y que satisfaga las condiciones de punibilidad.”<sup>7</sup>

### **1.10.2 División tripartita del concepto delito**

Esta modalidad establece que el delito concurre siempre y cuando hay presencia de tres elementos o atributos esenciales siendo estos:

1. Tipicidad: Aspecto descrito por la ley
2. Antijuricidad: Contraria al orden jurídico y lesiva de un interés social.

---

<sup>7</sup> Nieves Ricardo, **Teoría del Delito Contemporáneo**, Pág. 37

3. Culpabilidad: La exigencia de conexión psicológica entre el sujeto y el hecho perpetrado.

Los anteriores son los presupuestos de causa-efecto y el resultado es concebido como una transformación de la realidad ocasionada por el movimiento corporal y este a su vez responde a impulsos de voluntad.

El delito es un término que se traduce en una infracción punible o un hecho o acto punible, crimen o conducta delictiva, hecho penal, ilícito penal, hecho criminal, contravención o falta.

En la actualidad existen diversos criterios para definir el delito, dentro de los que destacan básicamente los siguientes:

a) Criterio legalista: Desde la denominada edad de oro del derecho penal a principios del siglo XIX, se deja ver un criterio legalista para definir al delito, por tanto delito es el acto prohibido por la ley.

Para el criterio legalista es la infracción a la ley del Estado promulgada para brindar protección a la seguridad de los ciudadanos la cual es el resultado de un acto externo del hombre, el cual puede ser positivo o negativo, políticamente dañoso y moralmente imputable.

b) Criterio Filosófico: debido a la intrascendencia del legalismo muy probablemente por los trastornos ocasionados por los postulados de la escuela positiva en oposición a la



escuela de juristas, hizo que los estudiosos del crimen de la época se encaminaran por senderos filosóficos tomándolos en consideración desde distintos aspectos: primeramente se hace alusión al aspecto moral por parte de los teólogos quienes identificaban al delito con conductas amorales y pecaminosas y seguidamente el delito es definido como una conducta contraria a la justicia y a la moral, para posteriormente enfocarlo como violación al deber.

El delito se refiere a acciones determinadas por motivos individuales y antisociales que alteran las condiciones de existencias y lesionan la moralidad media en un momento determinado.

Es fundamental estudiar el delito independientemente a las disciplinas fenomenalistas y por ello el criterio natural sociológico al definir al delito no tiene relevancia jurídica alguna.

c) Criterio técnico jurídico: después de que se superó la crisis por la cual paso el derecho penal durante la mitad del siglo XIX, cuando se encontró sometido a las más exageradas especulaciones del positivismo. Para este criterio la tipicidad consiste en uno de los caracteres primordiales del delito, además señala que la construcción del delito tiene que tomarse en cuenta en base a los elementos pertenecientes a la legislación positiva, o sea al concepto formal que por abstracción lleva a cabo el legislador de los distintos hechos que son objeto de estudio de la parte especial de los códigos penales.

Basándose en la tipicidad se define al delito como una acción típica contraria al derecho, culpable, sancionada con una pena adecuada y suficiente a las condiciones objetivas de la penalidad.

El jurista Francisco Muñoz Conde señala que: “muchos criminalistas han intentado formular una noción del delito en sí, en su esencia, una noción de tipo filosófico que sirva en todos los tiempos y en todos los países para determinar si un hecho es o no delictivo, tales tentativas han sido estériles, pues hallándose la noción del delito en íntima conexión con la vida social y jurídica, aquella ha de seguir forzosamente los cambios de esta y por consiguiente es muy posible que lo penado ayer como delito se considere hoy como lícito y viceversa.”<sup>8</sup>

---

<sup>8</sup> Muñoz Conde, Francisco. **Teoría General del Delito**. Pág. 37



## CAPÍTULO II

### 2. Los delitos informáticos

#### 2.1 Aspectos generales de los delitos informáticos

La doctrina legal indica que Delito es la conducta típica, antijurídica y culpable con características específicas a la que se le asocia una pena como consecuencia.

La comunidad académica y científica conjuntamente coincide en referirse a las acciones provenientes del uso indebido del sistema informático, independientemente de las siguientes maneras:

- a) Delitos de la tecnología informática.
- b) Delitos electrónicos
- c) Delitos informáticos, este término es el más aceptado.

#### 2.2 Concepto de delito informático

- Conducta por medio de la cual una persona maliciosamente hace uso de una base de datos, sistemas de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información
- Cualquier conducta criminógena o criminal que en su realización haga uso de la tecnología electrónica ya sea como método, medio o fin.
- Delito en el campo de la información: Es cualquier acción legal en el que la computadora es el instrumento u objeto del delito.

- Acción típica y antijurídica que se sirve o utiliza de una computadora para su realización o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático o a producir un resultado de daño en esta o de los sistemas que la misma hace operar.

## **2.3 Sujetos que participan en la comisión de los delitos informáticos**

### **2.3.1 Sujeto activo**

Es la persona que realiza la conducta descrita en el tipo penal, el criminólogo estadounidense Edwin Sutherland afirma que los delitos informáticos son delitos de cuello blanco (White collar) en donde los autores no solo reúnen condiciones técnicas o profesionales muy singulares, sino que han logrado un cierto dominio de su oficio que les permite ejecutar el delito. El obrar delictivo esta precedido por la atenta observación del accionar de quien será su víctima o su herramienta: La computadora.

Dentro de los sujetos activos se incluyen a los técnicos y profesionales vinculados a la computación tales como:

- a) Operadores: Pueden modificar, agregar, eliminar o sustituir información y/o programas, copias, archivos para venderlos a la competencia.
- b) Programadores: Pueden violar o inutilizar controles protectores del programa y/o sistema, atacar el sistema operativo, sabotear páginas, modificar archivos, acceder a información confidencial

**c) Analista de sistemas:** Son los únicos que conocen la operación de un sistema completo, pueden estar con el usuario, programador y operador.

**d) Analista de comunicaciones:** Es la persona que diseña la seguridad del sistema de comunicaciones por lo que conoce los métodos para violar la seguridad con fines de fraude.

**e) Supervisores:** Tienen conocimiento global de las operaciones y debilidades del sistema de seguridad, pueden manipular los archivos de datos y los ingresos y salidas del sistema pueden modificar, agregar o eliminar información.

**f) Personal técnico y de servicio:** Tienen libre acceso al centro de cómputo, tienen mayores conocimientos de los sistemas operativos y de base de datos, así como de sus debilidades.

**g) Funcionarios superiores:**

Tienen conocimiento general de los proyectos por lo que implican una amenaza potencial

**h) Auditores:** Conocen las debilidades del sistema ya que implementan las medidas de seguridad, instalando controles preventivos, que a posteriori, permiten detectar el fraude antes que la persona involucrada pueda escapar.

- i) Bibliotecarios de programación y operación: Son los responsables del mantenimiento de la documentación de sistemas, pueden destruir información o bien sustraerla y comercializarla.
  
- j) Usuarios: Pueden hacerse pasar por otros usuarios y modificar, omitir o agregar información con propósitos de fraude, efectuar un uso no autorizado.
  
- k) Personal de mantenimiento y agentes de seguridad: Pueden fotografiar documentos, sustraer información, sabotear el sistema con explosivos, ingresar repetitivamente a las instalaciones en horarios extraordinarios, etc.

### **2.3.2 Sujeto pasivo**

En primer término se debe distinguir al sujeto pasivo de la víctima, que es el ente sobre el que recae la conducta de acción u omisión que realiza el sujeto activo. En el caso de víctimas pueden ser individuos, instituciones crediticias, que usan sistemas automatizados de información, generalmente conectados a otros sistemas, obviamente también se trata de personas individuales.

Comprende tanto a los titulares y demás beneficiarios legítimos del sistema, como a los usuarios y terceros de buena fe. Las principales víctimas han sido Entidades Bancarias, Compañías de Seguros e incluso Instituciones Estatales de Servicios Públicos



## 2.4 Definición de los delitos informáticos

De conformidad con la teoría expuesta por el tratadista Julio Téllez Valdés, los delitos informáticos pueden ser clasificados.

Como instrumento o medio: La finalidad es ejecutar acciones en provecho de un acceso no autorizado para sacar ventaja de la información o bien con ánimo extorsivo, dentro de esta categoría se encuentran las conductas criminales que se valen de las computadoras, como medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo: En esta categoría se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, dentro de esta clasificación de acciones se encuentran:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

## **2.5 Características de los delitos informáticos**

De conformidad con el criterio del tratadista Julio Téllez, "las características primordiales de los delitos informáticos son las siguientes:

- a) Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.
- g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.”<sup>9</sup>

## 2.6 Clasificación de los delitos informáticos

“El Tratadista Blossiers afirma que los delitos informáticos pueden dividirse en tres grandes grupos:

1. Delitos que se cometen con el uso indebido o manipulación fraudulenta de elementos informáticos de cualquier tipo.
2. Acciones físicas que atentan contra la integridad de los equipos informáticos destinados a causar perjuicio no solo por destrucción de activos sino para paralizar sus actividades.
3. Los delitos relacionados con la propiedad intelectual o copia indebida de programas informáticos generalmente de manera informal”<sup>10</sup>

## 2.7 Bienes jurídicos tutelados

Son aquellos derechos, valores o atributos de la persona que el Estado encuentra merecedores de protección a través del Derecho Penal, en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro.

Las acciones que van dirigidas al sabotaje, el daño o la destrucción o pérdida de equipos de computación es decir, que afectan, lesionan o ponen en peligro el bien

---

<sup>9</sup> Téllez Valdés Julio **Ob.Cit.** Pág. 188

<sup>10</sup> Ibid.

jurídico del patrimonio, los delitos que se sirven o utilizan un equipo informático para su realización pueden de igual manera afectar diversos bienes, como lo serían la indemnidad sexual (caso de pornografía infantil) la privacidad o el mismo patrimonio en los casos de fraudes informáticos cometidos por Internet.

También debe tomarse en cuenta el uso de ordenadores para llevar a cabo la reproducción ilícita obviando claro está los derechos de autor de obras literarias, (libros, ebooks) material musical (videofilms) y películas reproducidas por compañías cinematográficas reconocidas, que no cuentan con permisos de ley ni con la licencia de reproducción o la autorización de comercialización debida. Dichas actividades afectan valores de propiedad intelectual pero implícitamente estas acciones tienen una motivación económica por lo que a su vez redundan en la afectación al bien jurídico patrimonio.

A continuación se enumeran y definen algunas modalidades de delitos informáticos dentro de las que se encuentran las siguientes:

## **2.8 Delitos contra el patrimonio y la propiedad intelectual**

a) Delito de Copia ilegal de software, películas y música: En este grupo se incluyen las conductas delictivas que van encaminadas a la obtención de datos, de manera ilegítima. Lo común es el apoderamiento de datos de investigaciones, listados de clientes, balances, etc. En la gran mayoría de casos el objeto de apoderamiento es el mismo software que suele tener un importante valor económico.

b) Delito de defraudación por medio de publicidad engañosa: El Internet es considerado un alto medio de comunicación masiva de igual trascendencia que la televisión y la radio, de tal modo que este espacio es un medio aprovechado para publicitar toda clase de bienes, productos y servicios. Por lo que es usual encontrar en las páginas de la red la oportunidad de acceder a compras y utilizar como medio de pago tarjetas de crédito y débito. Dentro de las prácticas comerciales normales se espera el cumplimiento en la entrega de bienes y servicios, sin embargo existe la acción delictiva, de personas inescrupulosas que aceptan el pago pero no se hace entrega de ningún beneficio a cambio.

Cabe mencionar que este tipo de conductas es repetitivo, y escapan a la acción penal, por la ausencia de un lugar físico en el cual se pueda ubicar al sujeto y por ende deducir responsabilidades por la acción perpetrada.

c) Delito de fraude cometido por acceso y manipulación a sistemas informáticas bancarios: Este tipo de conducta va dirigido a la manipulación de datos contenidos en sistemas informáticos con el objeto de obtener ganancias ilícitas, generalmente opera dentro de sistemas bancarios, se le reconoce con el nombre de técnica de salami, pues esta aprovecha las repeticiones automáticas del proceso de cómputo y consiste en introducir al programa instrucciones para que se remita a una determinada cuenta cantidades provenientes de otras cuentas corrientes

d) Delito de sabotaje a sistemas informáticos: Según el Diccionario RAE de la Real Academia de la Lengua Española, el termino sabotaje equivale a daño o deterioro que

se hace en las instalaciones, productos, etc. Así mismo se refiere a la oposición u obstrucción disimulada contra proyectos, ordenes, decisiones, ideas y otros.”<sup>11</sup>

En aplicación directa al ámbito de las computadoras el sabotaje implica cualquier acción dolosa tendiente a provocar daños en el hardware o el software, es decir los programas que utiliza el computador para operar.

La forma del sabotaje informático admite acciones tales como la infección directa al sistema por medio de virus, y demás operaciones destructivas, (Caballo de Troya) bombas lógicas, etc.

e) Delito de uso no autorizado de sistemas informáticos ajenos: Esta modalidad se perfecciona al hacer uso y aprovechar el acceso no autorizado a varias computadoras o sus programas o bien en la utilización inadecuada del sistema, ya sea para el uso irracional y abiertamente con el deseo de causar daño, o bien con el aprovechamiento del sistema para tareas eminentemente personales y con fines distintos a los que está establecido.

f) Delito de espionaje informático: En términos generales se refiere al acceso no autorizado al sistema o archivos informáticos de una empresa, gobierno o entidad con fines de análisis recopilación y traslado de información considerada útil para el espía o su organización, el caso clásico es el abordaje a sistemas relacionados con datos de inteligencia y contrainteligencia estatal.

---

<sup>11</sup> **Diccionario de la Real Academia Española.** Versión Digital. Consulta 10/06/2013

g) Delito de falsificación de documentos a través de la computadora: Se incluye dentro de este tipo de conductas todas aquellas cuyo objetivo es obtener copias fraudulentas de tarjetas de crédito débito, (clonación) o cheques, firmas electrónicas. Estas acciones tienen como finalidad de defraudar en su patrimonio tanto a personas individuales como a personas jurídicas.

## **2.9 Delitos informáticos que atentan contra la privacidad, la intimidad y la indemnidad sexual**

Dentro de esta clasificación de acciones delictivas se encuentran las acciones y omisiones en las que incurre el sujeto activo y que lesionan o ponen en riesgo el bien jurídico tutelado privacidad, entendida ésta, como el ámbito de la vida privada y la cual se tiene el derecho de proteger de cualquier intromisión.

El tratadista Jorge Bustamante anota al respecto: “Los delitos informáticos contra la privacidad constituyen un grupo de conductas que de alguna manera afectan la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.”<sup>12</sup>

“Dentro de los delitos informáticos que atentan a la privacidad de las personas encontramos:

1. Violación a la privacidad de la información personal o a las comunicaciones, que se refiere a las conductas tendientes a la interceptación de información o de mensajes ajenos.

---

<sup>12</sup> Bustamante Alsina, Jorge. **La informática y la protección de la vida privada**. Pág. 826.



2. Revelación indebida de información personal: delito en el que se incurre por la simple revelación o publicación de la información ajena obtenida con o sin ánimo de lucro.
3. Pornografía infantil a través de internet: Grabación y distribución por medio de la red de imágenes de contenido sexual de niñas, niños o adolescentes.”<sup>13</sup>

---

<sup>13</sup> Noriega Salazar, Aarón Hans, **Delitos Informáticos**, Pág. 37



## CAPÍTULO III

### 3. Las redes sociales y la comisión de hechos delictivos

#### 3.1 Antecedentes de los diferentes medios informáticos

Las redes son formas de interacción social definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Consisten en un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

Las llamadas redes sociales online consisten en servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que se puede plasmar datos e información personal. Adicional a ello se puede disponer de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado. El modelo de crecimiento de estas plataformas se basa fundamentalmente en un proceso viral, en el que un número inicial de participantes, mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al sitio web.

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados comunicación, movimientos políticos, deportes, entretenimiento, profesionalización, etc. “Uno de los principales objetivos de la red social se alcanza en el momento en el que sus miembros utilizan el medio online para convocar actos y acciones que tengan efectos en el mundo off-line.”

El primer sitio de redes sociales reconocibles puesto en marcha en 1997 fue: SixDegrees.com permitía a los usuarios crear perfiles, lista de amigos y amigos de sus amigos. De 1997 a 2001, AsianAvenue, Blackplanet y MiGente permitían a los usuarios crear relaciones personales y profesionales, creando perfiles que permitían a los usuarios identificar amigos en sus redes sin pedir la aprobación de esas conexiones.

Desde entonces diversas redes se han creado unas permanecen y otras han desaparecido, según la zona geográfica el líder puede ir cambiando, pero a la fecha los principales competidores a nivel mundial son:

- Facebook: Antes el boom de internet, el término Facebook se utilizaba para referirnos a las publicaciones que hacían algunas universidades al comienzo del curso, las cuales contenían los datos y las fotografías de los estudiantes con el objetivo de ayudar a conocerse. En el año 2004, un estudiante de la universidad de Harvard, Mark Zuckerberg, crea lo que hoy conocemos como Facebook. Se trataba de una red en internet en la que aparecía diversa información sobre los estudiantes de dicha universidad, es decir que en un inicio la red Facebook se encontraba destinada a utilizarse en la universidad de Harvard, sin embargo esta red logro extenderse a otras universidades exitosas.

Mediante su evolución tecnológica, la red social del momento fue ampliando sus servicios que en un inicio eran más bien limitados, conforme el transcurso del tiempo se implementaron mejoras por ejemplo lo relacionado a noticias, y el botón **I Like**, es

decir el click en la frase Me gusta, se expandió su uso en los celulares o bien en la aparición de las páginas de empresa, entre muchas otras novedades.

Facebook fue alcanzando el auge que posee en la actualidad por diversidad de aspectos, u dato importante es el segmento de edad con más presencia en la red, la cual oscila entre los 18 y los 35 años. Los principales usos que se le da a las redes sociales como Facebook es como medio de comunicación con familia y amigos, entretenimiento, la relación con los productores, conseguir servicios y promociones, emitir nuestra opinión sobre algún aspecto, en oportunidades se utiliza como medio para encontrar empleo y contactos profesionales..

Por tanto Facebook no solo ha revolucionado las redes sociales del momento, sino que también ha cambiado la comunicación interpersonal, la forma en que las personas se comunican y expresan sus ideas, opiniones, gustos.

En términos de marketing publicitario se puede afirmar que una de las ventajas de esta red, es el tipo de comunicación y la bidireccionalidad, es decir su feedback o retroalimentación, así como la generación o engagement, neologismo en ingles que se traduce en enganchamiento o compromiso tácito al continuar con el intercambio de información, datos en cadena.

- Twitter: Es una de las redes sociales más extendidas y populares, se inició en 2006 como un servicio de microblogging, de la mano de Jack Dorsey en San Francisco California. En la actualidad la plataforma del Twitter cuenta con más de 500

millones de usuarios registrados, aproximadamente se tiene cifras que se escriben más de 65 millones de tuits al día.

El software germinal de las redes sociales parte de la teoría de los Seis grados de Separación<sup>14</sup> Según la cual toda la gente del planeta está conectada a través de no más de seis personas. Esta teoría fue inicialmente propuesta en 1929 por el escritor húngaro Frigyes Karinthy derivada de una corta historia llamada Chains (cadenas). El concepto está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en cadena, y solo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera.

Se puede afirmar que crecimiento de las redes sociales en Internet ha sido exponencial a partir de la etapa de la "Web 2.0, donde el usuario de Internet dejó de ser un simple observador y consumidor de contenidos a un verdadero generador de los mismos."<sup>15</sup>

En la actualidad todo está conectado, las redes sociales han transformado al mundo en distintos aspectos, en esencia las redes sociales son la nueva tendencia, es decir la línea a seguir, hoy por hoy forman parte de nuestra vida cotidiana, pero si se profundiza algunos sitúan el surgimiento de las redes sociales a partir del Medioevo europeo con el profesor de la Soborna Yves Demazeau, experto en redes sociales e inteligencia artificial. "Algunos otros conocedores como Jeremy Rifkin o Manuel Castells

---

<sup>14</sup> [www.es.wikipedia.org](http://www.es.wikipedia.org), fecha consultada el 06/08/14

<sup>15</sup> Noriega Salazar, Aarón Hans, **Delitos Informáticos**, Instituto de la Defensa Pública Penal. Guatemala Pág. 37

establecen que las redes sociales están desplazando los mercados, los datos estadísticos establecen que más de 127 millones de latinoamericanos visitaron un sitio de redes sociales desde su hogar o su trabajo. Las redes sociales no son una moda, sino una tendencia que la tecnología ha impuesto es decir una nueva forma de ver el mundo.<sup>16</sup>

A continuación se enumeran algunos niveles de adaptabilidad generados por la presencia de las redes sociales:

- Es un medio masivo
- Es un medio hecho por y para personas.
- Es público, accesible y tecnológicamente preparado para compartir
- Es universal
- Es en tiempo real, lo que constituye una gran oportunidad.

De conformidad con estudio lanzados por CB ConsultingGroup, se puede observar algunas consideraciones, por ejemplo que una gran mayoría de empresas ya utilizan redes sociales como parte de sus políticas, todas estas tecnologías han generado un nuevo tipo de consumidores y seguidores, es decir mucho más inquisitivos y selectivos en cuanto a calidad y diversidad de servicios.

### **3.2 Clasificación y tipos de redes sociales**

Fundamentalmente se dividen en dos grandes tipos:

---

<sup>16</sup> [www.publinews.gt](http://www.publinews.gt), fecha consultada 15/06/14,

- a) Analógicas o redes sociales Off-Line: fuera de línea, son aquellas en las que las relaciones sociales, con independencia de su origen, se desarrollan sin mediación de sistemas electrónicos.
  
- b) Digitales o redes sociales On-Line: en línea son aquellas que tienen su origen y se desarrollan a través de medios electrónicos.

### **3.2.1 Primera clasificación de redes sociales, en atención al grupo objetivo a quienes se dirigen y el eje temático que desarrollan**

Redes sociales horizontales: Las denominadas redes 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 de este tipo de redes son Facebook, Orkut, Identi.ca, Twitter.

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

Redes sociales verticales de nivel profesional: Están dirigidas a generar relaciones profesionales entre los usuarios. Los ejemplos más representativos son Viadeo, Xing y Linked In.

Viadeo: Esta red posee gran cantidad de usuarios interesados en hacer contacto con antiguos compañeros de estudio o hasta posibles candidatos a ser contratados por una empresa según al sector al que se pertenece, a través de Viadeo, es posible publicitar productos y servicios empresariales o profesionales.

XING: Esta red especializada en asuntos y datos a nivel laboral, posee amplia aceptación. Básicamente es utilizada como canal de referencia en la contratación de personal a nivel empresarial e institucional.

Linked IN: Linked In, presenta un completo bosquejo en lo que experiencia laboral se refiere, es decir en oportunidades el transcurso del tiempo hace que involuntariamente se pierda los contactos laborales que se han recopilado. Gracias a esta red social, es posible encontrar contactos afines a la profesión de que se trate pues en ella convergen cantidad de profesionales (inclusive es posible realizar búsquedas por centros de estudios)

Redes sociales verticales de diversión y pasatiempo: 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.FM y Moterus.

Wipley: Los juegos se han convertido en una de las industrias más potentes en la actualidad. Sus cifras son impresionantes así como la cantidad de personas que disfrutan de este entretenimiento. A través de wipley, se puede interactuar y comentar, sobre contenidos y novedades del mundo del entretenimiento.

Dogster: Una red especializada en el mundo de las mascotas y sus cuidados, salud, alimentación, juegos etc. Sirven como sitios de enlace para intercambiar vivencias y conocimientos relacionados con las mascotas.

Redes sociales verticales mixtas: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales en torno a sus perfiles: Yuglo, Unience, PideCita.

### **3.2.2. Segunda clasificación de redes sociales, en atención al sujeto de la relación**

Redes sociales humanas: Son aquellas 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. Ejemplo de este tipo de redes los encontramos en Koornk, Dopplr, Youare y Tuenti.

Redes sociales de contenidos: Las relaciones se desarrolla uniendo perfiles a través del contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Los ejemplos más significativos son Scribd, Flickr, Bebo, Friendster, Dipity, StumbleUpon y FileRide

### **3.2.3. Tercera clasificación, en atención al área geográfica en la que se ubican y por su movilidad se subdividen en**

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: Rejaw, Blogger, Kwippy, Plaxo, Bitacorras.com, Plurk

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: Latitud, Brighkite, Fire Eagle y Scout

### **3.2.4. Cuarta clasificación, en atención al espacio y/o la plataforma en la que se expanden se dividen en**

Red social MMORPG y metaversos: Normalmente contruidos sobre una base técnica Cliente-Servidor (WOW, SecondLife, Lineage).

Red social web: Su plataforma de desarrollo está basada en una estructura típica de web. Algunos ejemplos representativos son: MySpace, Friendfeed y Hi5

MySpace: Esta red dispone de una gran cantidad de usuarios dados de alta (se estima que más de 180 millones hasta la fecha) La interfaz completamente traducida es muy

sencilla de usar, por lo que cualquier persona una vez se dé de alta en el servicio recibe el beneficio de enviar y mensajes por ella perfectamente de manera inmediata.

Establecer contactos es muy sencillo, ya que con escribir mensajes sobre las opiniones de los usuarios es suficiente. Adicional a ello, las posibilidades de configuración del espacio personal son bastante elevadas y es posible dar un aspecto profesional.

De igual modo dispone de apartados de espacio para fotografías, vídeos y música, el buscador de personas es de los más avanzados y dispone de una gran cantidad de filtros lo que asegura resultados óptimos.

### **3.3 Aspectos derivados del uso de las redes sociales**

#### **a) Ventajas derivadas del uso de las redes sociales**

1. Pueden ser utilizadas en el sector académico y laboral, para el intercambio de diversas experiencias innovadoras.
2. Los empresarios que hacen uso de las redes sociales han demostrado un nivel de eficiencia y un acertado trabajo en equipo, consolidando proyectos de gestión del conocimiento.
3. Favorecen la participación y el trabajo de equipo entre las personas, es decir que los usuarios participan en un proyecto en línea desde cualquier lugar.
4. Permiten construir una identidad personal y/o virtual debido a que es posible a los usuarios compartir todo tipo de información con los cibernautas.
5. Facilitan el aprendizaje integral fuera del aula escolar y permiten poner en práctica los conceptos adquiridos.

6. Facilitan las relaciones entre las personas evitando barreras físicas y culturales.
7. Por el aislamiento social del mundo actual el contacto es inmediato, se pueden intercambiar actividades, intereses, información, aficiones, etc.

c) Desventajas derivadas del uso de redes sociales:

1. Personas inescrupulosas y con segundas intenciones pueden invadir la privacidad de otras provocando problemas, para un hacker es sumamente sencillo obtener información confidencial.
2. En algunos países ser usuario de redes sociales se convierte en una amenaza para la seguridad nacional.
3. Si no se hace uso correcto de las redes sociales, fácilmente se puede convertir en una adicción.
4. Gran cantidad de casos de pedofilia y delitos relacionados con pornografía y explotación sexual en menores se han manifestado por medio de las redes sociales.
5. En oportunidades se ha mostrado información personal, dejando al descubierto datos que implican riesgo sustancial para la privacidad de las personas.

Con las redes sociales se tiene la posibilidad de interactuar con otras personas, a pesar de la distancia y las diferencias de horario, el sistema es abierto y se va construyendo obviamente con lo que cada suscrito a la red aporta.

Por tanto la comunicación por medio de las redes sociales es más amplia, el costo promedio de una llamada telefónica difiere considerablemente de la navegación en la

Web y la interconexión con la red, lo cual además de conveniente para el bolsillo del usuario.

### **3.4 Características de las redes sociales**

- Están basadas en el usuario: las redes sociales son constituidas y dirigidas por los mismos usuarios además las nutren con el contenido.
- Son un medio interactivo: las redes sociales poseen además de un conjunto de salas de Chat y foros, una serie de aplicaciones basadas en una red de juego como una forma de conectarse y divertirse con los amigos.
- Establecen relaciones: las redes sociales no solo permiten descubrir nuevos amigos sobre la base de interés, sino que también permite volver a contactar con viejos amigos con los que se ha perdido contacto desde muchos años.
- Intercambian información e intereses: las redes sociales permiten que el contenido publicado por un usuario se difunda a través de una red de contactos, subcontactos mucho más grande de lo que se pueda imaginar.
- Ofrece variedad de servicios: intercambio de todo tipo de información, fotografías, servicios de telefonía, chat room, foros, etc.

### **3.5. La problemática jurídica de las redes sociales**

Los servicios de redes sociales han experimentado gran auge entre el público. "Entre otras cosas, estos servicios ofrecen medios de interacción basados en perfiles personales que generan sus propios usuarios registrados, lo que ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de las personas

interesados (y de terceros), lo cual es altamente perjudicial en caso de no tener un manejo adecuado en el banco de datos personales.<sup>17</sup> Es aconsejable recordar que los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades sin precedentes, incluidas enormes cantidades de fotografías y vídeos digitales; sin perjuicio de las distintas actividades delictivas que se pueden llevar a cabo usando estas redes como medios para la comisión de ilícitos (Delitos informáticos, delitos contra el honor, contra la propiedad intelectual, industrial, etc.).

Un aspecto que vale la pena resaltar es tener absoluta claridad al distinguir una amistad real de una amistad virtual, y desde luego contar con la convicción que a pesar de la cercanía y grado de confianza que se logre entablar, la amistad virtual, difiere en muchos aspectos a un trato personal y continuo, por ello se debe manejar cierto margen de distancia y es aconsejable entablar relaciones de amistad solo con personas conocidas. Todo ello con la finalidad de evitar riesgos e inconvenientes posteriores.

A manera referencial se anota a continuación diversos aspectos que pueden afectar los derechos individuales de los usuarios de redes sociales, entre los que destacan:

Protección de los derechos al honor, a la propia imagen, intimidad y privacidad de los usuarios:

---

<sup>17</sup> **Informe de la Comisión de Protección de Datos Personales.** Agencia de Cooperación Española. 2009 Pág. 33

Protección de los derechos al honor: El honor como bien jurídico tutelado. El honor se define como uno de los componentes inherentes a la persona. Es la propia personalidad entendida como la suma de cualidades físicas, morales, jurídicas, sociales y profesionales, valiosas para la comunidad, atribuibles a las personas. Cuando el que atribuye esas cualidades es el propio interesado se habla de honor subjetivo u honra de la persona. Cuando los que le atribuyen esas cualidades al interesado son los terceros, se habla de honor objetivo o crédito de la persona.

Osorio define el honor: "Cualidad moral que nos lleva al más severo cumplimiento de nuestros deberes respecto del prójimo y de nosotros mismos. El Honor se entiende como la buena reputación que sigue a la virtud, al mérito. Es sinónimo de honestidad y recato."<sup>18</sup>

En lo relativo a los denominados Delitos contra el honor, el bien jurídico tutelado es propiamente el derecho al honor, al buen nombre de la persona, al decoro y la reputación de las personas, es decir todo lo relacionado con su personalidad moral.

Soler expresa que el honor subjetivo puede ser considerado "como una autovaloración, es decir, como el aprecio de la propia dignidad, como el juicio que cada cual tiene de sí mismo en cuanto sujeto de relaciones ético"<sup>19</sup>

---

<sup>18</sup> Osorio Manuel. **Diccionario de Ciencias Jurídicas, Políticas y Sociales** Ob.Cit. Pág. 463

<sup>19</sup> Soler, Sebastián Pág. 202

El honor, como bien jurídico protegido en esta clase de tipos penales, puede ser considerado desde dos puntos de vista; desde un punto de vista subjetivo el honor significa la autovaloración, la propia estimación; es decir, el juicio que cada uno de nosotros se forma de sí mismo sociales.

En consecuencia de un uso indebido de la información que recorre las redes sociales, las personas pueden ser objeto de los siguientes supuestos jurídicos:

Acciones provocadas por injurias/o calumnias ocasionados por medio de redes sociales:

1. La injuria: es la ofensa genérica al honor ajeno; que puede ser a la honra de la persona (honor subjetivo), y en este caso es una lesión al derecho que tienen las personas a que los terceros respeten las cualidades que ellos le asignan a su personalidad. O bien puede ser una ofensa al crédito de la persona (honor objetivo), y en este caso es una lesión al derecho de las personas a que no se perjudique la opinión que sobre su personalidad tengan o puedan tener los terceros. Es la fama o reputación.

2. La calumnia: es una injuria especializada por la naturaleza particular de la imputación hecha por el acusado al ofendido. Mientras en la injuria esa imputación no está tipificada, ya que puede constituir cualquier hecho, calidad o conducta en contra el honor o que obra en desacredito. Por su lado la calumnia es la imputación debe tener por contenido un delito que dé lugar a la acción pública. Al referirse al tema el tratadista

Manuel Osorio define: “Calumnia es la acusación falsa hecha maliciosamente con la finalidad de causar daño.”<sup>20</sup>

En este orden, podemos afirmar que los usuarios que realicen actividades difamatorias mediante la utilización de las redes sociales online, pueden ser sujetos activos de este tipo de delitos.

### **El derecho a la imagen**

En referencia directa con la palabra imagen se entiende y define como la figura, la fisonomía que la persona tiene, como individuo único e irrepetible.

El derecho a la imagen posee varias connotaciones. En un aspecto inicial se hace referencia al derecho que por propia disposición tiene cada persona de captar, reproducir y publicar su propia imagen cómo, dónde y cuándo desee.

En otro aspecto se refiere al derecho que la persona tiene de impedir la obtención, adaptación, reproducción y publicación de su propia figura por terceros, sin su consentimiento.

En este sentido, las redes sociales online son un ámbito susceptible en donde se pueden cometer gran cantidad de infracciones sobre el derecho a la imagen.

---

<sup>20</sup> Osorio Manuel **Ob. Cit.** Pág. 100



Un ejemplo claro lo constituye el hecho que una persona publica una fotografía sin autorización previa, y esta inmediatamente se empieza a distribuir por toda la red de usuarios, llegando a contactos o publicaciones no deseadas por el usuario.

Cabe mencionar que en muchos casos hay actuaciones de los usuarios o de las propias redes que realizan respecto de la imagen y otros datos que se escapan de la propia esfera de la protección de datos, como por ejemplo la cesión ilegal de imágenes con finalidad comercial, sin consentimiento previo e informado del titular.

### **El derecho a la privacidad e intimidad**

El derecho a la intimidad tiene por objeto la protección de la esfera más íntima de la persona, y se encuentra estrechamente ligado a la protección de la dignidad del individuo.

Es por consiguiente el derecho que tiene toda persona humana a que sea respetada su vida privada y familiar, el derecho a no ser objeto de injerencias arbitrarias en la zona espiritual íntima y reservada de una persona o de un grupo, especialmente dentro del núcleo familiar. Se trata de hechos de menos gravedad y que solamente afectan a valores morales de la vida doméstica o de la debida cortesía que impone entre los hombres la convivencia en el seno de la sociedad.

A continuación se hace referencia sobre las posibles situaciones de riesgo para la protección de la intimidad:



1. En el momento del registro de alta como usuario, en la medida en que no sea configurado correctamente el nivel de privacidad del perfil, así como por el hecho de que sea publicada información sensible desde el inicio de la actividad en la red.

2. En el momento de participación en la red como usuario, en el supuesto que el grado de información, datos e imágenes publicados puedan ser excesivos y afectar a la privacidad, tanto personal como de terceros.

3. En relación a la privacidad de terceros: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retiro de forma inmediata.

Es válido resaltar que en la mayoría de ocasiones, las redes sociales permiten a los motores de búsqueda de internet, indexar (deviene del término *índex*, *índice*) en las búsquedas de los perfiles de los usuarios, junto con información de contacto y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de la información en Internet.

Por lo tanto, existen varias posibilidades de infracción a los derechos de intimidad y privacidad en las redes sociales, en virtud que estas pueden ser cometidas por otros usuarios de las redes o por terceros.

### **3.6 Protección de datos personales**

Por lo regular las redes sociales a nivel general cuentan con un nivel de riesgo superior al de las redes de contenido profesional, dado que los usuarios exponen no sólo sus datos de contacto o información profesional (formación, 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 es mayor que en las redes sociales de tipo profesional.

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.

De conformidad con los resultados del estudio sobre la privacidad de los datos personales en las redes sociales on line, realizado por la Agencia Española de Protección de datos, el manejo inadecuado de los datos e información personal puede desencadenar en los siguientes aspectos:

1. 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.
2. Los datos personales pueden ser utilizados por terceros, en medida malintencionada y de forma ilícita.

3. Existe la posibilidad de que traten y publiquen en la Red información falsa o sin autorización del usuario, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho.
4. El hecho de que, a través de las condiciones de registro aceptadas por los usuarios, éstos cedan derechos plenos e ilimitados sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que pueden ser explotados económicamente por parte de la red social.

### **3.7. Derechos de propiedad intelectual en las redes sociales**

La facilidad de reproducción y distribución de contenidos hacen 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.

El modelo de generación de contenidos ha variado en gran medida respecto al existente antes del surgimiento de la Web 2.0, dado que hoy en día los contenidos no son generados por los propios autores en exclusiva, sino que cualquier usuario tiene la capacidad de generar y difundir sus obras de propiedad intelectual, convirtiéndose así en autor y potencial productor y distribuidor.

A manera referencia se puede anotar que algunas redes sociales y, en especial, las plataformas de contenidos multimedia (Youtube, Dalealplay.com, Myspace, Google video, Redkaraoke, etc.), son el mejor ejemplo de las posibilidades que brindan este tipo de plataformas a los autores.

Desde el punto de vista de los posibles riesgos que se pueden producir contra la protección de la propiedad intelectual en Internet, en general, y en los servicios de redes sociales y plataformas en particular, deben diferenciarse dos situaciones en origen:

a) Por una parte se ven afectados 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.

b) De igual manera afectan las implicaciones jurídicas sobre las obras que sean titularidad de los propios usuarios y que éstos deciden compartir o hacer públicas a través de estas redes y plataformas.

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.

La realidad es que en la práctica esto no ocurre de esta manera, ya que los sitios web de redes sociales siguen publicando los contenidos del usuario argumentando que estos deben quedar visibles para los demás usuarios de la red con quien se compartieron en su momento.

### **3.8. Delitos informáticos en las redes sociales**

A continuación se enuncian las modalidades de acción y conductas delictivas que suceden con mayor frecuencia por medio de las redes sociales, siendo estas las siguientes:

1. Pornografía infantil por internet u otros medios electrónicos
2. Delito de trata de personas y explotación sexual
3. Intercepción o captación de comunicaciones electrónicas o telecomunicaciones
4. Acceso a un sistema o dato informático
5. Publicación de una comunicación electrónica
6. Acceso a un banco de datos personales
7. Inserción de datos falsos en un archivo de datos personales
8. Fraude informático
9. Daño o sabotaje informático

En este orden, bastaría solo dejar en claro que de acuerdo a estas modalidades delictivas descritas con anterioridad se logra establecer que, según la situación, pueden



ser cometidas tanto por los mismos usuarios de las redes sociales, o por personas ajenas a esta, o por la misma persona o empresa propietaria del sitio web.

Un reciente estudio reveló que las redes sociales como Facebook, Twitter y MySpace son el blanco preferido de hackers inescrupulosos para llevar a cabo acciones tales como robo de datos personales, robo de información confidencial, estafas, envío de virus o spam.



## CAPÍTULO IV

### **4. Diversas modalidades en la comisión de hechos delictivos a través de las redes sociales y la urgente necesidad de que se incluya en el Código Penal**

#### **4.1 Aspectos considerativos**

Actualmente Guatemala no cuenta con una legislación especializada, efectiva o apropiada para regular lo concerniente a delitos informáticos, así como la diversidad de delitos que atentan contra la indemnidad sexual de las personas, es decir que se hace urgente implementar medidas de amplio alcance que una vez en marcha vigilen y castiguen penalmente, aquellas acciones ilícitas cometidas a través de sistemas que utilicen tecnologías de información y comunicación.

A la presente fecha si bien es cierto ha existido ciertos intentos en el abordaje del tema, también es claro que las escasas iniciativas presentadas a fin de regular dicha problemática se encuentran inactivas, es decir en espera recibir reconocimiento dentro de la agenda legislativa que desde hace algunos años se encuentra en constante estancamiento.

A lo largo del presente capítulo se hará mención de algunos aspectos relacionados con actos delictivos específicamente a delitos de indemnidad sexual y delitos informáticos que se encuentran oportunamente tipificados en el código penal guatemalteco, Así como las novedosas formas operativas que sujetos malintencionados accionan a través de las redes sociales con la finalidad de ocasionar daño material y psicológico a sus víctimas.



## **4.2 Acciones delictivas tipificadas en la legislación penal guatemalteca**

### **4.2.1 Delitos que atentan la indemnidad sexual**

Art. 173 Violación: Quien con violencia física o psicológica, tenga acceso carnal vía vaginal, anal o bucal con otra persona o le introduzca a cualquier parte del cuerpo objetos, por cualquiera de las vías señaladas, u obligue a otra persona a introducirse a sí misma, será sancionado con pena de prisión de ocho a doce años. Siempre que se cometa este delito cuando la víctima sea persona menor de catorce años, o cuando sea persona con incapacidad volitiva o cognitiva, aun cuando no medie violencia física o psicológica. La pena se impondrá sin perjuicio de las penas que puedan corresponder por la comisión de otros delitos.

Art. 173 Bis. Agresión sexual: Quien con violencia física o psicológica, realice actos con fines sexuales o eróticos a otra persona, al agresor o a sí misma, siempre que no constituya delito de violación, será sancionado con prisión de cinco a ocho años.

Cabe mencionar que las penas son agravadas en relación al daño proporcionado a la persona menor de edad así como al número de agresores que participen en la acción delictiva.

Art. 188 Exhibicionismo sexual: Quien ejecute, o hiciere ejecutar a otra persona, actos sexuales frente a personas menores de edad o personas con incapacidad volitiva o cognitiva, será sancionado con pena de tres a cinco años de prisión

Art. 190 Violación a la intimidad sexual: Quien por cualquier medio, sin el consentimiento de la persona, atentare contra su intimidad sexual y se apodere o capte



mensajes, conversaciones, comunicaciones, sonidos, imágenes en general o imágenes de su cuerpo, para afectar su dignidad, será sancionado con prisión de uno a tres años.

Las mismas penas se impondrán al que, sin estar autorizado, se apodere, acceda, utilice o modifique, en perjuicio de tercero, comunicaciones efectuadas por cualquier medio físico o electrónico o datos reservados con contenido sexual de carácter personal, o familiar de otro, que se encuentren registrados en ficheros o soportes informáticos., electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, en perjuicio de la persona titular de los datos o de una tercera persona.

Se impondrá de dos a cuatro años a quien difunda, revele o ceda, a cualquier título, a terceros, los datos o hechos descubiertos o las imágenes captadas a que se refiere este artículo.

#### **4.2.2 Delitos de explotación sexual**

Art. 191 Promoción, facilitación o favorecimiento de prostitución. La explotación de una persona mayor de edad, a través de la promoción, facilitación o favorecimiento de su prostitución, será sancionada con prisión de cinco a diez años, y con multa de mil a cien mil quetzales.

Art. 202 Trata de personas: Constituye delito de trata de personas la captación, el transporte, traslado, retención, acogida o recepción de una o más personas con fines de explotación.

Quien cometa este delito será sancionada con prisión de ocho a dieciocho años y multa de trescientos mil a quinientos mil quetzales.

Es claro que la lista de acciones delictivas es por más extensa, Sin embargo se ha dejado evidencia escrita de los actos más recurrentes e igualmente abordados a través de sistemas de comunicación móvil (teléfonos celulares) o bien por medio de captación de personas por medio de formas por demás engañosas por medio de correos electrónicos, ofreciendo premios por consumo, boletos aéreos, gastos de hospedaje y tramite de visa a Estados Unidos, entre otras, las modalidades varían dependiendo de la tipología del delito y la víctima o grupo objetivo que se persigue, es conocido que Antigua Guatemala , está siendo promocionado como sitio de recreo y turismo sexual, pues investigaciones y numerosas denuncias indican que en dicha localidad hay comercio sexual . El uso de las redes sociales es un canal de comunicación por medio del cual puede ofrecerse toda clase de invitaciones o fotografías de destinos, actividades que en un inicio aparecen como lujosos centros de recreo y Spa, cuando en realidad son paraísos de acciones contrarias a la ley.

#### **4.2.3 Implementación de la ley contra el femicidio y otras formas de violencia contra la mujer**

En respuesta al seguimiento y aplicación de justicia a casos concretos derivados de los altos niveles de violencia que a diario afectan y convierten en víctimas a las

mujeres guatemaltecas, dentro del territorio nacional , se implementó la ley contra el femicidio y otras formas de violencia contra la mujer, de conformidad con los Acuerdos de la Corte Suprema de Justicia No. 30-2012 relacionado con la creación de Juzgados y Tribunales de Primer Instancia Penal de Femicidio y otras formas de violencia contra la mujer.

De igual manera se emitió el Acuerdo de la Corte Suprema de Justicia No. 43-2012 que establece la creación del Juzgado y Tribunal de Primera Instancia Penal de Femicidio y otras formas de violencia contra la mujer y violencia sexual, explotación y trata de personas del departamento de Guatemala.

#### **4.2.4 De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos**

Art. 274: Violación al derecho de autor y derechos conexos: Salvo los casos de excepción contemplados expresamente en las leyes o tratados sobre la materia de los que Guatemala sea parte, será sancionado con prisión de uno a cuatro años y multa de un mil a quinientos mil quetzales, quien realizare cualquiera de los actos siguientes:

- a) La atribución falsa de la calidad de autor y/o titular de un derecho de autor, de artista, intérprete o ejecutante, de productor de fonograma o de un organismo de radiodifusión.



- b) La deformación, mutilación, modificación o cualquier atentado que cause perjuicio a la integridad de la obra o al honor y reputación del autor.
- c) La reproducción de cualquier obra, de una interpretación o ejecución, de un fonograma o de una emisión, sin la autorización del autor o titular del derecho correspondiente.
- d) La adaptación, arreglo o transformación de una obra protegida o de parte de ella, sin autorización del autor o titular del derecho.
- e) La comunicación al público por cualquier medio o procedimiento de una obra protegida o de un fonograma, sin la autorización del titular del derecho correspondiente.
- f) La distribución de reproducciones no autorizadas, totales o parciales, de una obra protegida o de un fonograma, ya sea por medio de la venta, el arrendamiento, el alquiler, el arrendamiento con opción de compra, el préstamo o cualquier otra forma.
- g) La fijación, reproducción o comunicación al público por cualquier medio o procedimiento de una interpretación o ejecución artística, sin la autorización del artista intérprete o ejecutante o del titular del derecho.
- h) La fijación, reproducción o retransmisión de una emisión, transmitida por satélite, radiodifusión por hilo, cable, fibra óptica o cualquier otro procedimiento, sin autorización del titular.
- i) La comunicación al público de una emisión o transmisión efectuada en un lugar al que el público pueda acceder mediante el pago de un derecho de admisión, o bien, para efectos de consumir o adquirir productos o servicios, sin la autorización del titular del derecho correspondiente.

- j) La publicación de una obra protegida con el título cambiado o suprimido, con o sin alteración de la misma.
- k) La decodificación de señales transmitidas por satélite o cualquier otro medio de telecomunicación, portadoras de programas de cualquier tipo sin la autorización del distribuidor legítimo.
- l) La realización de cualquier acto que eluda o pretenda eludir una medida tecnológica implementada por el autor o el titular del respectivo derecho o del titular de un derecho conexo, para evitar la utilización no autorizada de todo tipo de obra, de un fonograma, de una interpretación o ejecución artística o de una emisión protegida.
- m) La realización de cualquier acto que induzca, permita, facilite u oculte una infracción a cualquiera de los derechos exclusivos correspondientes a los autores, a los titulares de un derecho de autor, a los artistas intérpretes o ejecutantes, a los productores de fonogramas o a los organismos de radiodifusión.
- n) La supresión o alteración no autorizada de cualquier información electrónica sobre la gestión colectiva de los derechos de autor o derechos conexos.
- o) La distribución, comercialización, promoción, importación, emisión o comunicación al público sin autorización de obras, interpretaciones o ejecuciones artísticas, producciones fonográficas o emisiones, sabiendo que la información electrónica sobre la gestión colectiva de cualquiera de esos derechos ha sido suprimida o alterada sin autorización.
- p) El transporte, almacenamiento u ocultamiento de reproducciones o ejemplares, en cualquier tipo de soporte material, de obras protegidas, de fonogramas, de interpretaciones o ejecuciones artísticas o de emisiones fabricadas sin el consentimiento del autor o el titular del derecho correspondiente.

- q) La recaudación de beneficios económicos por la utilización de obras, de interpretaciones artísticas o ejecuciones, de fonogramas o de emisiones de organismos de radiodifusión protegidos, o la realización de cualquiera otras actividades propias de una sociedad o gestión colectiva, sin estar facultado para tales efectos
- r) La divulgación de una obra inédita sin el consentimiento del autor o del titular del respectivo derecho.
- s) La traducción, total o parcial, de una obra sin la autorización del autor o titular del derecho correspondiente.
- t) La distribución no autorizada del original o reproducciones legítimas de una obra protegida o de un fonograma, ya sea por medio de la venta, el arrendamiento, el alquiler, el arrendamiento con opción de compra, el préstamo o en cualquier otra forma.
- u) La importación o exportación del original o de reproducciones de toda obra protegida, con fines de explotación comercial, en cualquier tipo de soporte o de fonogramas, sin la autorización del titular del derecho respectivo.

La determinación de los supuestos contenidos en esta norma se hará con base en las disposiciones aplicables de la Ley de Derecho de Autor y Derechos conexos

Art. 274 A: Destrucción de registros informáticos: Será sancionado con prisión de seis meses a cuatro años y multa de doscientos a dos mil quetzales el que destruyere, borrar o de cualquier modo inutilizare registros informáticos: La pena se elevará en un



tercio cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial.

Art. 274 B: Alteración de programas: La misma pena del artículo anterior se aplicara al que alterare, borraré o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

Art. 274 C: Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

Art. 274 D: Registros prohibidos: Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Art. 274 E: Manipulación de información: Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar o alterar los estados contables o la situación patrimonial de una persona física o jurídica



Art. 274 F: Uso de información: Se impondrá prisión de seis meses a dos años y multa e doscientos a mil quetzales al que sin autorización, utilizare los registros informáticos de otro, o ingresare por cualquier medio a su banco de datos o archivos electrónicos.

Art. 274 G: Programas destructivos: Será sancionado con prisión de seis meses a cuatro años y multa de doscientos a mil quetzales al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

Art. 275: Violación a los derechos de propiedad industrial: Sin perjuicio de las responsabilidades civiles que correspondan, será sancionado con prisión de uno a cuatro años y multa de cincuenta mil a quinientos mil quetzales, quien sin el consentimiento del titular del derecho, realice alguno de los siguientes actos:

- a) Introducir al comercio, vender, ofrecer en venta, almacenar o distribuir productos o servicios amparados por un signo distintivo registrado o por una imitación o falsificación de dichos signos, con relación a los productos o servicios iguales o similares a los protegidos por el registro.
- b) Usar en el comercio un nombre comercial, un emblema o una expresión o señal de propaganda protegidos.
- c) Introducir en el comercio, vender, ofrecer en venta, almacenar o distribuir productos o servicios amparados por un signo distintivo registrado, después de haberlo alterado, sustituido o suprimido total o parcialmente.

- d) Usar, ofrecer en venta, almacenar o distribuir productos o servicios que lleven una marca registrada, parecida en grado de confusión a otra registrada, después de que se haya emitido resolución ordenando el cese del uso de dicha marca.
- e) Fabricar etiquetas, envases, envolturas, embalajes u otros materiales análogos que reproduzcan o contengan el signo registrado o una imitación o falsificación del mismo, así como comercializar, almacenar o detentar tales materiales.
- f) Rellenar o volver a usar con cualquier fin envases, envolturas o embalajes que lleven un signo distinto al registrado.
- g) Usar en el comercio etiquetas, envoltorios, envases y demás medios de embalaje o empaque de los productos o de identificación de los servicios de un comerciante o de copias, imitaciones o reproducciones de los mismos que puedan inducir a error o confusión sobre el origen de los productos o servicios.
- h) Usar o explotar un secreto empresarial ajeno, así como cualquier acto de comercialización, divulgación o adquisición indebida de tales secretos.
- i) Revelar a un tercero un secreto empresarial que haya conocido con motivo de su trabajo, puesto, cargo, profesión, relación de negocios o en virtud de una licencia de uso, después de haber sido prevenido sobre la confidencialidad de dicha información.
- j) Apoderarse de un secreto empresarial por cualquier medio, sin la autorización de la persona que lo guarda o de su usuario autorizado.
- k) Fabricar, elaborar, comerciar, ofrecer en venta, poner en circulación, almacenar o detentar productos amparados por una parte ajena.

- l) Emplear un procedimiento amparado por una patente ajena o ejecutar cualquiera de los actos indicados en el literal anterior, respecto a un producto obtenido directamente por ese procedimiento.
- m) Fabricar, elaborar, comercializar, ofrecer en venta, poner en circulación, almacenar o detentar productos que en sí mismos o en su presentación reproduzcan un diseño industrial protegido.
- n) Usar en el comercio, con relación a un producto o servicio, una indicación geográfica falsa o susceptible de engañar al público sobre la procedencia de ese producto o servicio o sobre la identidad del producto de su fabricante o del comerciante que lo distribuye.
- o) Usar en el comercio con relación a un producto una denominación de origen falsa o engañosa, aun cuando se indique el verdadero origen del producto, se emplee una traducción de la denominación o se la use acompañada de expresiones como tipo, género, marca, imitación u otras análogas.

La determinación de los supuestos contenidos en esta norma se hará con base en las disposiciones aplicables de la Ley de Propiedad Industrial.

Art. 275 Bis: Violación de los derechos marcarlos: Será sancionado con prisión de cuatro a seis años y multa de cincuenta mil a cien mil quetzales, quien realizare cualquiera de los actos siguientes:

- a) Usar en el comercio una marca registrada, o una copia servil o imitación fraudulenta de ella, en relación a productos o servicios iguales o similares a los que la marca se aplique.
- b) Usar en el comercio un nombre comercial o un emblema protegido.
- c) Usar en el comercio, en relación con un producto o un servicio, una indicación geográfica falsa o susceptible de engañar al público sobre la procedencia de ese producto, fabricante o comerciante del producto o servicio.
- d) Ofrecer en venta o poner en circulación productos a los que se aplica una marca registrada, después de haber alterado, sustituido o suprimido esta, parcial o totalmente.
- e) Continuar usando una marca no registrada parecida en grado de confusión a otra registrada, después de que se haya emitido resolución ordenando el cese del uso de la marca no registrada.
- f) Ofrecer en venta o poner en circulación los productos o prestar los servicios con las marcas a que se refiere la literal anterior.

Del análisis de los supuestos anteriores es preciso hacer notar algunos aspectos, la norma se aplica en resguardo de los derechos inherentes al derecho de autor sobre su obra, así como su utilización y por ende la comercialización de la misma. Sin embargo es preciso resaltar que en relación a lo que dispone el código penal guatemalteco, en lo relativo a las sanciones aplicables a los delitos informáticos, las sanciones a imponer son más bien insuficientes y hasta incongruentes, con el riesgo y daño perpetrado por medio de una acción maliciosa, causante de un daño tanto a nivel material como económico, deberá ser castigado con la aplicación de una sanción adecuada, más

congruente con el momento actual y con el riesgo e implicación que conlleva la intención de causar daño.

#### **4.3 La era de la tecnología y las comunicaciones dentro del ámbito guatemalteco**

En relación directa con la evolución tecnológica y las novedosas formas de comunicación, recientemente se ha implementado el uso de las redes sociales, que gozan de total respaldo y aceptación dentro del grupo promedio de consumo (jóvenes, adolescentes e incluso menores de edad) provocando una nueva forma de comunicación, cabe mencionar que las comunicaciones virtuales han recibido inmediata aceptación dentro del ámbito guatemalteco.

Lo ideal sería que cada integrante de redes sociales fuese respetuoso tanto de los derechos propios como los de los demás miembros, sin embargo la facilidad para obtener aceptación e ingreso a estas estructuras es inmediata, razón por la cual numerosos estudiantes de nivel medio y preuniversitario en su mayoría comparten datos personales e información clasificada como sensible o privada que no deben compartirse con personas desconocidas. Para nadie es ajeno el hecho que personas adultas malintencionadas utilizan pseudónimos o bien perfiles falsos para obtener la confianza de sus víctimas. A la fecha es numeroso el resultado de denuncias de acoso o bien intimidación, delito de trata de personas, pornografía infantil, todo ello a través de las redes sociales.

Estudios recientes a nivel sociológico han determinado: “Que las personas ingresan a las redes sociales, incluso antes de incorporarse a las diversas actividades diarias, tales como asistir a centros educativos, lugares de trabajo, lugares de recreo etc.

De igual manera se estima que el grupo promedio de seguidores de redes sociales permanecen conectados de manera constante e interactiva por espacios de 3 a 5 horas diarias”, pero obviamente hay personas que sobrepasan dicha estadística, la cual es una gran mayoría.

La tecnología de vanguardia ha encontrado importante número de usuarios y las redes sociales un elevado número de seguidores potenciales, las redes sociales son en el momento actual un medio de comunicación amplia e interactiva que supera los propios sistemas de comunicación convencionales y reconocidos. Grandes movimientos han adquirido mayor de cantidad de presencia y resistencia si el caso lo amerita. Todo ello en virtud que los seguidores de redes se encuentran dando click de manera permanente y repetitiva a cada dato, información de interés o cualquier situación novedosa que acontece. . Las redes sociales brindan un nivel de comunicación ágil, inmediato, interactivo y además económico.

El escenario no puede ser más propicio para que desconocidos se infiltren y de manera insospechada ganen la confianza brindada por medio de una amistad virtual, se inicie con un intercambio de información personal, nuestro país al igual que un alto número de países de Latinoamérica no cuentan con una normativa jurídica que resguarde la privacidad o bien la legalidad en materia de comunicaciones.

Prueba de ello es que diariamente según datos obtenidos en esta investigación e información de estudios especializados demuestran un alto nivel en el delito de robo de aparatos celulares, smartphones y computadoras portátiles, que en oportunidades han tenido finales trágicos como la muerte del propietario por medio de asaltos a mano armada. Cabe mencionar que el alto nivel de este tipo de delitos también evidencia el poco nivel de compromiso que las autoridades tienen en erradicar dicha situación.

#### **4.4 Guatemala supera un índice elevado en el uso de teléfonos móviles**

Puede observarse de manera especial el interés promovido por varios sectores que impulsan la Ley de Registro Móvil para la Prevención y el Combate del Delito. A la presente fecha se estima según estudios estadísticos en el territorio guatemalteco que existe un aproximado de 19.7 millones de teléfonos celulares. Dichos datos obran en el reporte trimestral de la SIT. Superintendencia de Telecomunicaciones. Sin embargo de conformidad con las fuentes consultadas se establece que la cifra del robo de teléfonos celulares es en relación a 315 robos a diario, y 13 celulares por hora.

En atención al delito de extorsión esta tipología del delito ha encontrado auge entre líderes de pandilleros, así como de personas privadas de libertad, que incluso guardando prisión en centros de detención, utilizan aparatos celulares para extorsionar a pequeños empresarios, transportistas y comerciantes y está claro que ante el alto clima de inseguridad y desconfianza imperante, hace que estas personas obtengan altas cantidades bajo esta forma habitual de delinquir.



A manera referencial se define el delito de extorsión el cual se encuentra tipificado en el Artículo 261 del Código Penal Guatemalteco, de la siguiente forma: “Quien, para procurar un lucro injusto, para defraudarlo o exigirle cantidad de dinero alguna con violencia o bajo amenaza directa o encubierta, o por tercera persona y mediante cualquier medio de comunicación obligue a otro a entregar dinero o bienes; igualmente cuando con violencia lo obligare a firmar, suscribir, otorgar, destruir o entregar algún documento, a contraer una obligación o a condonarla o a renunciar a algún derecho, será sancionado con prisión de seis a doce años incommutables”.

Relacionado a este aspecto, es alarmante el nivel de incremento que registra las estadísticas criminales en presencia del delito de extorsión y nada se hace al respecto.

Se espera que legisladores, autoridades de gobierno y operadores de justicia incrementen el nivel de control y aplicación de las medidas correctivas necesarias tanto a los sujetos que resulten responsables por el alto índice de teléfonos celulares robados, así como de los delitos de extorsión y actividades delictivas derivadas del uso indebido en las comunicaciones y por ende se brinde el acompañamiento así como del respaldo legal a las personas quienes resultaren víctimas de dichas acciones.

#### **4.5 Forma de comisión de los delitos a través de las redes sociales**

##### **4.5.1 El Modus operandi de los delincuentes informáticos**

Esencialmente no existe mucha diferencia entre las conductas antijurídicas punibles y tradicionales, con aquellas que se comenten a través de medios informáticos. Es



justamente la adjetivación del delito informático, la que convierte al delincuente en algo apartado de la tradición y envuelve el hecho de unas connotaciones que lo dotan de cierta autonomía conceptual. “El ordenador se convierte en un instrumento del delito, no por sí solo, sino por la conexión a una red interna (intranet) o a una red externa (Internet) por donde circulan usuarios, estudiantes, empresarios, profesionales, pederastas, grandes sumas de dinero encriptados, estafadores, saboteadores, jóvenes, niños y terroristas.”

#### **4.5.2 Presupuestos del ciber crimen en la red**

Predominantemente existen dos formas de comunicación a través del Internet:

El correo electrónico por medio de la World Wide Web www y las redes sociales, ambas funcionan como un sistema de hipertexto que funciona sobre Internet, a través del cual y con la ayuda de una aplicación informática destinada al efecto, el navegador web extrae información (documentos o páginas web) y se muestran en la pantalla del usuario. Al darle continuidad al enlace, el usuario puede tener acceso inmediato a múltiples páginas con diversidad de contenidos, temas e información. Dichas páginas se encuentran hospedadas en servidores donde se almacena la información en discos duros.

A nivel participativo son tres o cuatro sujetos como mínimo los que participan en el fenómeno del ciber crimen.

El sujeto activo del delito es quien inicia con la conducta punible, (ya sea enviando contenidos a un servidor, sea descargando archivos prohibidos o bien enviando e-mails

difamatorios o abusivos) Los sujetos coadyuvantes sin cuya intervención el ciberdelincuente tendría escasos medios técnicos para desarrollar su conducta criminal (el servidor de acceso que posibilita la conexión a la red y el servidor de contenidos en cuyos discos duros se alberga la información delictiva que más tarde causa perjuicios).

Un detalle importante es que por medio del Internet, la comunicación puede ir focalizada a varias personas, ya que el ciberdelincuente conocedor de las ventajas de la World Wide Web, utiliza la tela de araña para que los efectos de su acción se multipliquen y perjudiquen a multitud de personas.

Adicionalmente debe considerarse la inmediatez y versatilidad con la que el ciberdelincuente cuenta para enviar un mensaje, todo ello en virtud de que en solo una fracción de segundos puede lograr el envío de un e-mail intimidatorio, o bien la ejecución de un fraude, por otro lado cualquier persona con escasos medios técnicos y financieros puede entrar al circuito y utilizar la red.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de estos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de esta área. Desde el punto de vista de la legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener el resultado esperado sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.

#### 4.5.3 Ley de Registro móvil para la prevención y el combate del delito

“Con fecha martes 18 de septiembre del año 2013, el Congreso de la República de Guatemala aprobó en sesión ordinaria el Decreto No. 8-2013 denominado: Ley de registro móvil para la prevención y el combate del delito”<sup>21</sup>. La cual se encuentra contenida en 34 artículos, en los que se regula y penaliza de manera determinante las siguientes acciones:

- Activaciones ilegales de teléfonos celulares
- Clonación y adulteración de equipos móviles
- Comercialización de equipos terminales móviles sin registro ni autorización.
- Uso de terminales móviles en centros de detención.

Es preciso anotar de manera adicional que con la aplicación de esta ley se espera poner freno al robo desmedido de aparatos celulares, así como a la reactivación de los mismos, por lo que por medio de la referida normativa se establecen penas de seis años de prisión a veinte años de prisión y multas que van desde diez mil a doscientos mil quetzales,(Q.10,000.00 a Q.200,000.00) la finalidad primordial es y suprimir y/o disminuir las estadísticas actuales que presentan creciente aumento en los delitos tales como extorsiones, secuestros y amenazas. Cabe mencionar que la referida ley fue aprobada en sesión ordinaria y fue promulgada de urgencia nacional con una totalidad de: 117 votos a favor y 8 en contra.

---

<sup>21</sup> [www.congreso.gob.gt](http://www.congreso.gob.gt) Consultada el 18/10/13



## 4.6 Las nuevas modalidades delictivas a través de las redes sociales

### 4.6.1 Delito de trata de personas y los nuevos avances tecnológicos

“La trata de personas es una violación a los derechos humanos, por el cual niños, niñas, adolescentes, mujeres y hombres son captados, trasladados y privados de su libertad para ser explotados. La captación puede ser mediante secuestro, amenazas y engaño.”<sup>22</sup>

Actualmente los medios de comunicación como el Internet a través de chats, blogs, las redes sociales y los teléfonos móviles son espacios donde delincuentes contactan a sus posibles víctimas para ganar su confianza, engañarlas y finalmente aprovecharse de ellas.

Por dicha razón es de gran importancia estar al tanto de las nuevas modalidades que personas inescrupulosas utilizan para el (aparente) reclutamiento de personal, anuncios o avisos de casting para captación de modelos preadolescentes y adolescentes con fines artísticos y publicitarios etc.

A continuación se hace mención de algunas modalidades por medio de las que las redes sociales son un elemento básico en la nueva forma de captación de menores, mujeres, y hombres en edad laboralmente activa.

---

<sup>22</sup> Lic. De León Duque, Jorge Eduardo **Informe Circunstanciado del Procurador de Derechos Humanos de Guatemala**. pag 134

Los espacios cibernéticos y los teléfonos móviles han creado nuevas formas de comunicación e inter relación que pueden en determinado momento poner en riesgo derechos como la libertad, la privacidad y la indemnidad sexual.

1. **Perfiles Falsos:** Estos actos ilícitos consisten en la creación de perfiles simulados con datos reales o empresariales, a efecto de obtener o manipular a los usuarios. Las ofertas o mejoras económicas se realizan bajo el trasfondo de ser una entidad internacional, que ofrece contratación inmediata, pago de salario en moneda extranjera (Dólares, Euros, etc.) Tramite de visas y permisos laborales, gastos de hospedaje, boleto aéreo, etc. Cabe mencionar que el alto índice de desempleo y falta de oportunidades es propicio para el uso de esta modalidad.
2. **Pornografía infantil:** Los numerosos casos de pornografía infantil on line que han y están ocurriendo en el país y a nivel internacional, demuestran que el Internet se ha convertido en el medio principal para que pedófilos intercambien archivos y fotografías de menores. Las redes sociales son espacios donde es posible encontrar atraer y seducir menores de edad.
3. **Robo de información:** Es uno de los delitos cibernéticos más populares y olvidados por los usuarios de las redes, quienes han descuidado la forma en que publican información personal en lugares como blogs, foros o redes sociales. La excesiva confianza y negligencia de los usuarios en las redes los lleva a compartir información privada o sensible. Los delincuentes informáticos aprovechan este espacio para desarrollar los siguientes actos ilícitos: Robo de información para

extorsión del usuario, para robos presénciales, secuestros virtuales, secuestros reales, entre otros.

4. Sexting: Esta modalidad consiste en enviar mensajes de texto a través de teléfonos móviles, o bien por medio de redes sociales (comentarios, sugerencias, imágenes) o Internet que contienen fotografías, videos con contenido sexual. Las personas menores de edad que envían sexting, lo hacen porque alguien se los solicita o bien por simple diversión, con la finalidad de quedar bien o con el deseo de recibir admiración, aceptación y afecto.
5. Cyberbullying o ciber-acoso: Se entiende por el hostigamiento de un menor hacia otro menor, en forma de insultos, vejaciones, amenazas, chantajes, utilizando para ello un canal tecnológico Dentro de la sociedad norteamericana, este aspecto se relaciona con el hecho de poner en la red o en aplicaciones como Youtube, videos que abiertamente contengan escenas de riñas, golpes, insultos y demás situaciones que afectan directamente el entorno de jóvenes, esta situación puede darse dentro de las instituciones educativas, centros de recreo e incluso en áreas residenciales.

Un aspecto que se ve altamente evidenciado es la postura incomoda del menor ante la humillación pública, pues estas personas utilizan las imágenes para burlarse, hacer comentarios públicos, lo cual es una situación abiertamente difícil para la víctima.

6. Sextorsion: Esta figura aparece cuando una persona es advertida del riesgo de hacer público el contenido de imágenes, fotografías o videos en las que participe de

manera directa o indirectamente. Es decir que la conducta delictiva aparece con el ánimo de apropiarse de cierta cantidad de dinero o a sostener relaciones sexuales sin su voluntad, a cambio de la NO publicación del material referido, es sin lugar a duda una forma de extorsión o chantaje.

7. Grooming: Se define como el conjunto de maniobras que una persona adulta desarrolla para ganarse la confianza del menor o la víctima, a través de internet, con el fin último de obtener concesiones de índole sexual, pero también es un medio por el que los tratantes engañan a niños, niñas y adolescentes. Relacionado al mismo aspecto se debe tener cuidado de no consignar direcciones exactas, o fotografías del entorno familiar, pues esta es una forma de agilizar la búsqueda, ubicación y posterior localización del menor y su familia.

Es preciso hacer valer que a la presente fecha el delito de trata de personas no sea exclusivo de menores de edad, al contrario, cada vez es más frecuente el caso de personas en edad laboral que en espera de lograr el sueño americano, resultan víctimas de explotación laboral.

#### **4.7 Institucionalización del día internacional contra el delito de trata de personas**

Como resultado de la incidencia de este delito, se institucionalizó el día 23 de septiembre de cada año, como: El día en contra del delito de trata de personas.

En la actualidad existen esfuerzos combinados tanto de entidades nacionales así como de organismos internacionales con la finalidad de erradicar completamente las secuelas de esta indignante acción delictiva.

#### **4.8. Sumario de acontecimientos relacionados con el uso inapropiado de las redes sociales**

##### **4.8.1. Caso FACEBOOK**

Antecedentes: A manera referencial se anota algunos datos relacionados con el denominado CASO FACEBOOK, que es un claro ejemplo de la acción delictiva de personas inescrupulosas con el objetivo primordial de causar daño a jóvenes inexpertas a través de las redes sociales. Las acciones fueron perpetradas por un individuo que adoptó el nombre de El Vaquero Indomable. Quien en el mes de septiembre del año 2011 invito a dos jovencitas residentes del departamento de Escuintla, el nexos causal fue la supuesta confianza y amistad que surgió a raíz del intercambio de constantes mensajes vía Facebook. El sujeto en cuestión estableció relación de amistad con ambas y aprovechando los datos personales compartidos, la táctica utilizada fue muy simple, en principio enviaba constantes y numerosos mensajes que hacían reconocer el alto nivel de interés por parte de él, en formar parte del grupo de amigos y conocidos, y mejor aún reunirse, para estrechar vínculos y dejar que la amistad on line, pasara a una fase más próxima es decir, una verdadera amistad basada en la confianza, momentos de diversión y armonía propias de la juventud. Al sentir seguridad sobre su decisión invito a ambas jovencitas a reunirse con él. Y desde luego ellas aceptaron inmediatamente. Acto seguido cometió el delito secuestro.



Posteriormente exigió pago por el derecho de rescate a los padres de las menores, estos accedieron depositando una fuerte suma de dinero y pese a ello, al no encontrarse satisfecho por obtener un pago parcial, posteriormente dio muerte ambas adolescentes.

Caso Facebook llega a sentencia: “El proceso penal en el Caso Facebook, concluyo con la lectura que un Tribunal de Sentencia emitió el día 12 de octubre de 2013, en el que se impuso una sentencia condenatoria consistente en 200 años de prisión”<sup>23</sup> que deberá aplicarse a: Saúl Eleazar Arreaga (alias el vaquero indomable) y a Eduardo Chen García (alias El Crazy), ambos son sindicados por el delito de doble secuestro y asesinato de dos jovencitas guatemaltecas, residentes del departamento de Escuintla.

Cabe mencionar que con la aplicación de esta sentencia, se marca un precedente histórico en la sociedad guatemalteca, enviando un mensaje de alerta a aquellos infractores de la ley.

#### **4.8.2 Caso de sexting y acoso sexual en el departamento de Jalapa**

Este caso sucedió particularmente en el departamento de Jalapa, localidad en la cual hace algunos meses, una joven adolescente al salir de su casa y dirigirse al centro de estudios, inicialmente fue víctima de miradas acusadoras pues la veían con desprecio. No comprendía la razón hasta que se enteró de que alguien había distribuido por celular un video donde ella supuestamente sostiene una relación sexual.

---

<sup>23</sup> [www.elperiodico.com.gt](http://www.elperiodico.com.gt). Consultada el 12/03/14

La joven es víctima de la acción delictiva denominada sexting, un término que fusiona dos palabras del inglés, sex y texting, para hacer alusión a la generación y envío, por medio de teléfono celular, de contenidos pornográficos, un fenómeno del que ya se reportan casos en Guatemala.

“Nuestra familia ha sido afectada porque hicieron un video horrible y usaron un montaje de mi hermana pequeña, de 14 años, quien sufre de acoso e insultos cuando sale a la calle”, relata la mayor de las hijas de una familia afectada, cuyo nombre se omite por razones de seguridad. Existe una denuncia de este caso en la Procuraduría de los Derechos Humanos (PDH). “Alguien fabricó ese montaje y la gente lo cree real”, explica Cecilia Aguirre, auxiliar de la PDH.

De hecho, en Jalapa se han denunciado dos casos de ese tipo, por lo que Aguirre califica la situación de “grave”, porque evidencia un deterioro en las relaciones humanas y sociales. Aunque se ha sabido de otros videos, las víctimas no acuden a las autoridades para denunciar, por vergüenza.

#### **4.9 Influencia negativa**

La difusión de materiales pornográficos a través de internet ha distorsionado la mentalidad de numerosos jóvenes, quienes filman el momento en que sostienen una relación sexual durante el noviazgo, pero cuando este finaliza distribuyen el video entre sus amigos, a manera de venganza.

“La sociedad no se ha dado cuenta de la gravedad del problema”, opina Aguirre, quien sugiere a los padres y maestros que aborden el tema de la sexualidad, el noviazgo y las consecuencias de la pornografía.

De hecho, en Jalapa la PDH impulsa la campaña “No contamines tu celular, no contamines tu mente”, para contrarrestar el problema. La medida básicamente consiste en que los jóvenes rechacen este tipo de contenidos en su móvil, lo cual certifican con un llavero que obsequian. “Los jóvenes deben tener el valor de hacer lo correcto”, expone Aguirre.

#### **4.10 Víctimas de sociópatas**

Víctor López, del Centro de Investigaciones para la Salud, de la Universidad de San Carlos, comentó que el envío de contenido sexual por teléfono se originó en USA, pero ahora con la disponibilidad de teléfonos móviles que captan video, se han dado casos en algunos departamentos. Advierte que a menudo esos mensajes empiezan como una broma, aunque hay casos de jóvenes que son drogadas o embriagadas para ser grabadas. En cualquiera de los casos, se trata de una distorsión del verdadero sentido de la sexualidad y de un daño moral irreparable.

Aída Castro Conde, Profesional de la Psicología Forense, asegura que quienes filman y distribuyen ese material son sociópatas; es decir que carecen de sentido de



responsabilidad, son egocéntricos y no les importa hacer daño a alguien. “Por ello los jóvenes deben fijarse bien con quién se relacionan”<sup>24</sup>, enfatizó.

A manera referencial se adjunta a continuación los datos de algunas de las instituciones que velan por la persecución penal así como el resguardo de los derechos humanos, pero particularmente que persiguen de oficio acciones en contra de jóvenes, mujeres y niños que resultaren víctimas acciones delictivas.

- Procuraduría General de la Nación PGN

15 Ave. 9-69 zona 13 PBX 22483229

Página web [www.pgn.org.gt](http://www.pgn.org.gt)

- Procuraduría de los Derechos Humanos PDH

PBX 24241717 Denuncias 1555

Página web [www.pdh.org.gt](http://www.pdh.org.gt)

- Ministerio Público

15 Ave. 15-16 zona 1 Barrio Gerona

PBX 24118181 24119191

Página web [www.mp.org.gt](http://www.mp.org.gt)

- Policía Nacional Civil PNC

Denuncias Call Center 122

<sup>24</sup>[www.prensalibre.com.gt](http://www.prensalibre.com.gt) consultada 19/05/14



La autora de la presente tesis promueve a través de la labor investigativa, evidenciar con datos reales que surgen como respuesta de la presente labor investigativa la inmediata necesidad de modificar o bien reformar la legislación penal existente, así como brindar por medio del presente, un aporte documental en relación con la reconocida problemática del uso de las redes sociales como herramienta para la realización de actos delictivos. Pues de conformidad con los datos que obran en los registros de denuncias propias de la unidad de Procuraduría de Derechos Humanos, Ministerio Público, Policía Nacional Civil y otras entidades afines encaminadas a este delito y sus secuelas, cada día aumenta la cifra de denuncias de actos delictivos perpetrados por medio de uso de celulares y más directamente por medio del uso abusivo e inapropiado de las redes sociales.

Por lo que se considera que como medida correctiva se aplique la inclusión de estas acciones delictivas dentro del código penal guatemalteco y por consiguiente la persecución y enjuiciamiento penal de quienes resultaren responsables por el uso inadecuado de las redes sociales.

Es urgente implementar un patrón de control y vigilancia en la red de las comunicaciones, en un inicio a nivel nacional, pero está claro que esta medida posteriormente deberá realizarse a nivel de la región centroamericana, pues en recientes fechas los medios de comunicación escrita, hablada y televisiva, han demostrado públicamente que las estructuras criminales sobrepasan las fronteras, especialmente en delitos de extorsión y trata de personas así como de explotación sexual en menores de edad.



Por tal razón se debe tomar conciencia sobre el indignante proceder de los sujetos que actúan en completa impunidad haciendo su (modus vivendi) o medio de vida la ejecución habitual de acciones delictivas así como la obtención de altos dividendos que se generan a través de la extorsión y delitos conexos.





## **CONCLUSIONES**

- 1. La implementación de las comunicaciones virtuales y la versatilidad y costo económico del Internet, ha permitido que muchos usuarios prefieran el uso de un sistema interactivo, a bajo costo y con disponibilidad inmediata, siendo los consumidores jóvenes y adultos jóvenes, quienes navegan por la red en un promedio de 3 a 4 horas diarias.**
- 2. De conformidad con los datos provenientes de la encuesta que fue utilizada como instrumento de consulta se logró establecer, que los miembros de redes sociales, utilizan esta modalidad con dos propósitos: a) como medio de comunicación y; b) como medio de información.**
- 3. El uso inadecuado de la telefonía celular y el uso desmedido de redes sociales, puede convertir un hábito cotidiano a un cuadro de adicción, que se inicia con una fase leve hasta llegar a sobrepasar un descontrol inconsciente del mismo e incluso convertirse en una herramienta para la facilitación y ejecución de hechos delictivos.**
- 4. Los datos estadísticos establecen que los delitos de robo de teléfonos celulares crecen a un ritmo acelerado en el territorio Guatemalteco, provocando más inseguridad y violencia.**
- 5. Grupos delictivos compuestos por miembros de pandillas y personas privadas de libertad, hacen uso de teléfonos móviles para llevar a cabo diversos delitos.**



## RECOMENDACIONES

1. El Congreso de la República debe implementar de manera urgente la tipificación y la penalización del el uso inadecuado de las redes sociales, mediante el establecimiento de un marco jurídico relativo a los sistema que utilicen tecnología de la información logrando con esto la protección integral de la persona, sus bienes y sus derechos así como la prevención del delito.
2. El Congreso de la República de Guatemala legisle en cuanto a la protección al usuario del uso de las redes sociales, creando normas jurídicas pertinentes y adecuadas, que permitan uso seguro de la comunicación y de la información en dichas herramientas informáticas.
3. Es necesario que los padres de familia en general tomen el control del uso de teléfono celular y equipo de cómputo por parte de sus hijos, es decir, mantener vigilancia en cuanto a las redes sociales a las cuales se conectan, así como el tiempo de permanencia en ellas, y hacerles conciencia del riesgo que conlleva el uso inadecuado dichas redes.
4. Los jueces deben aplicar la pena prisión, sin privilegio alguno, a toda aquella persona que cometa el delito de robo de terminales móviles porque de esa manera disminuiría tal delito.

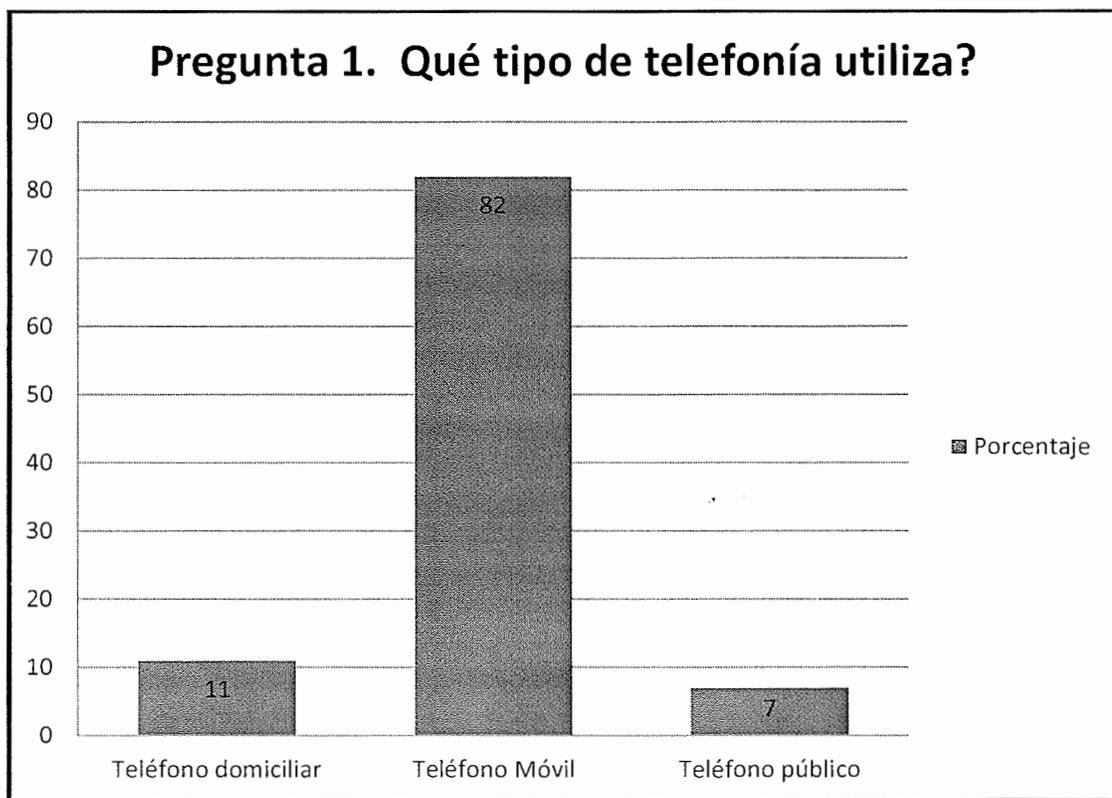


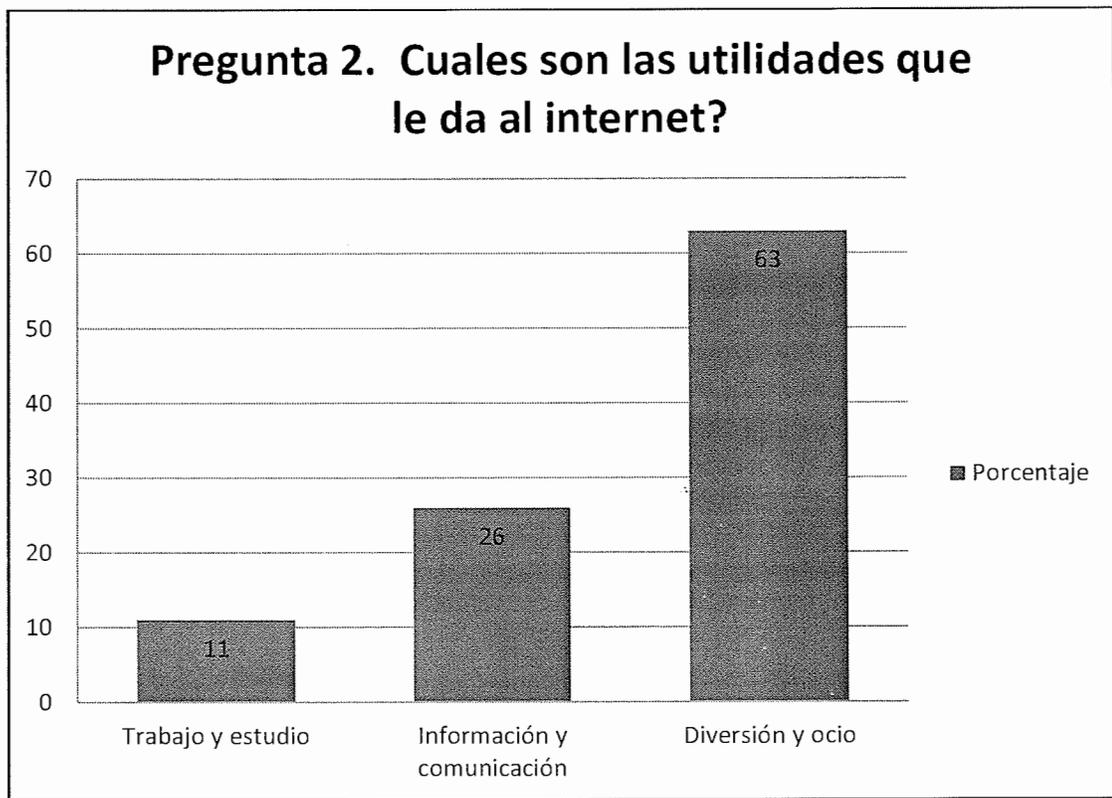


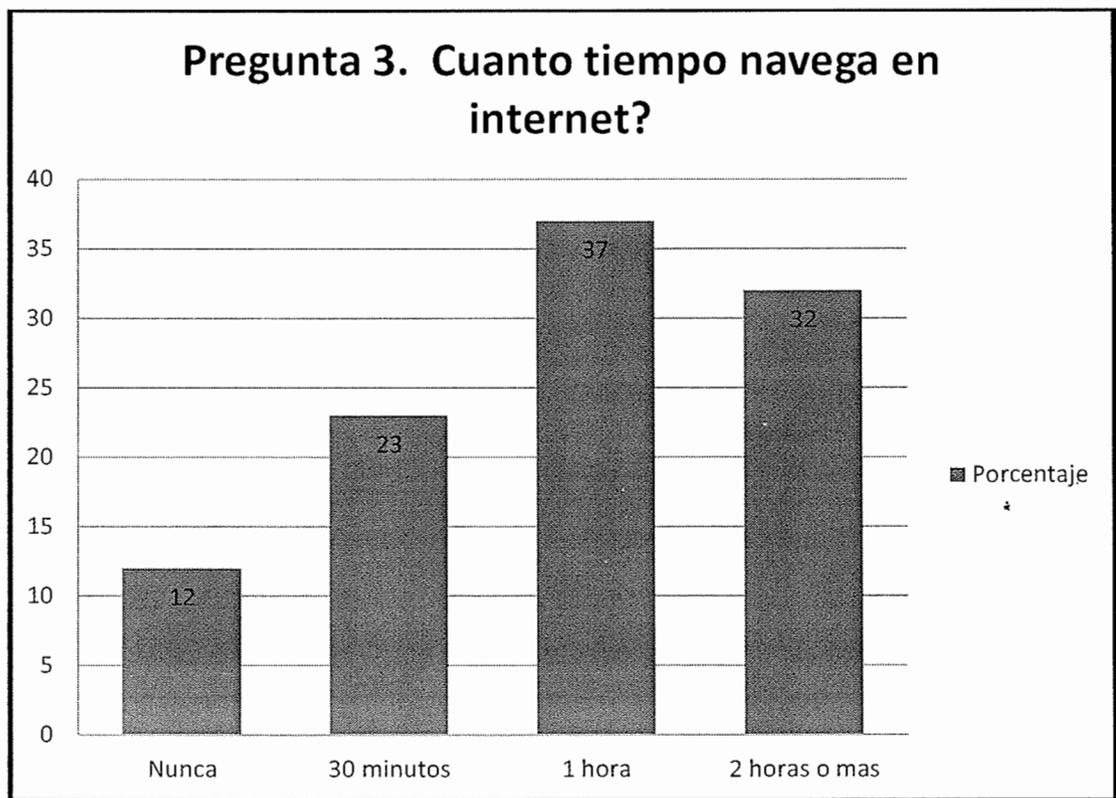
## ANEXOS

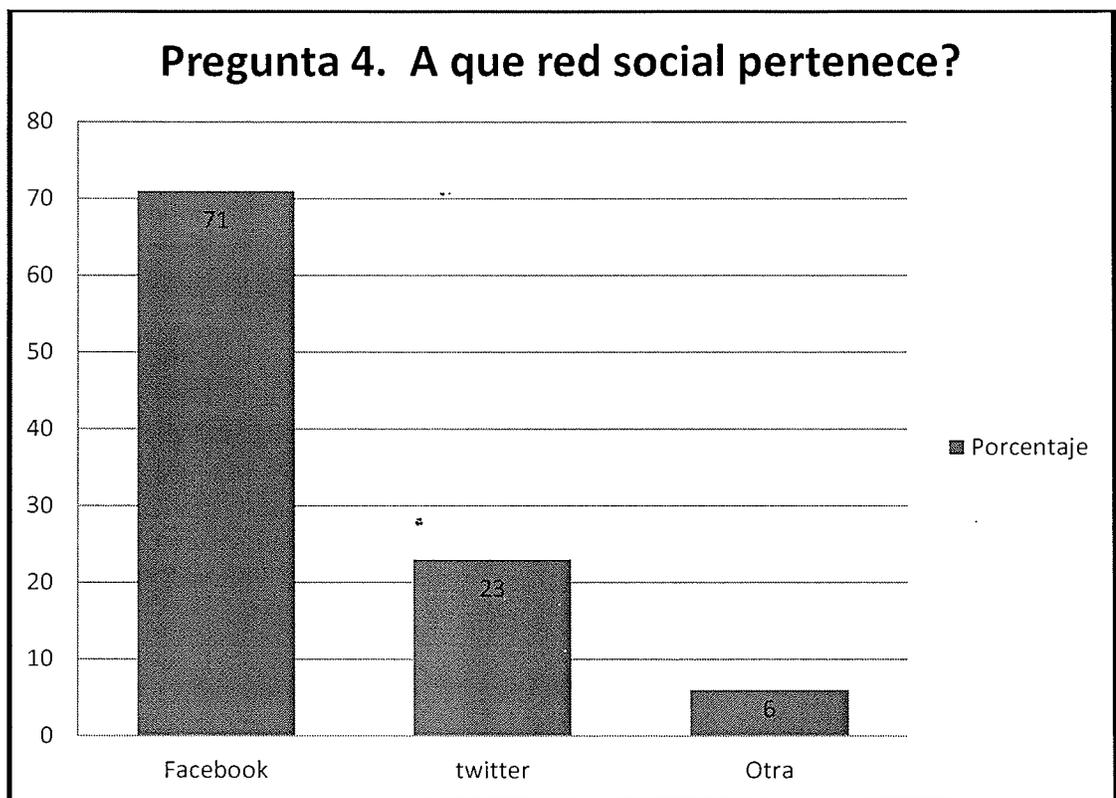


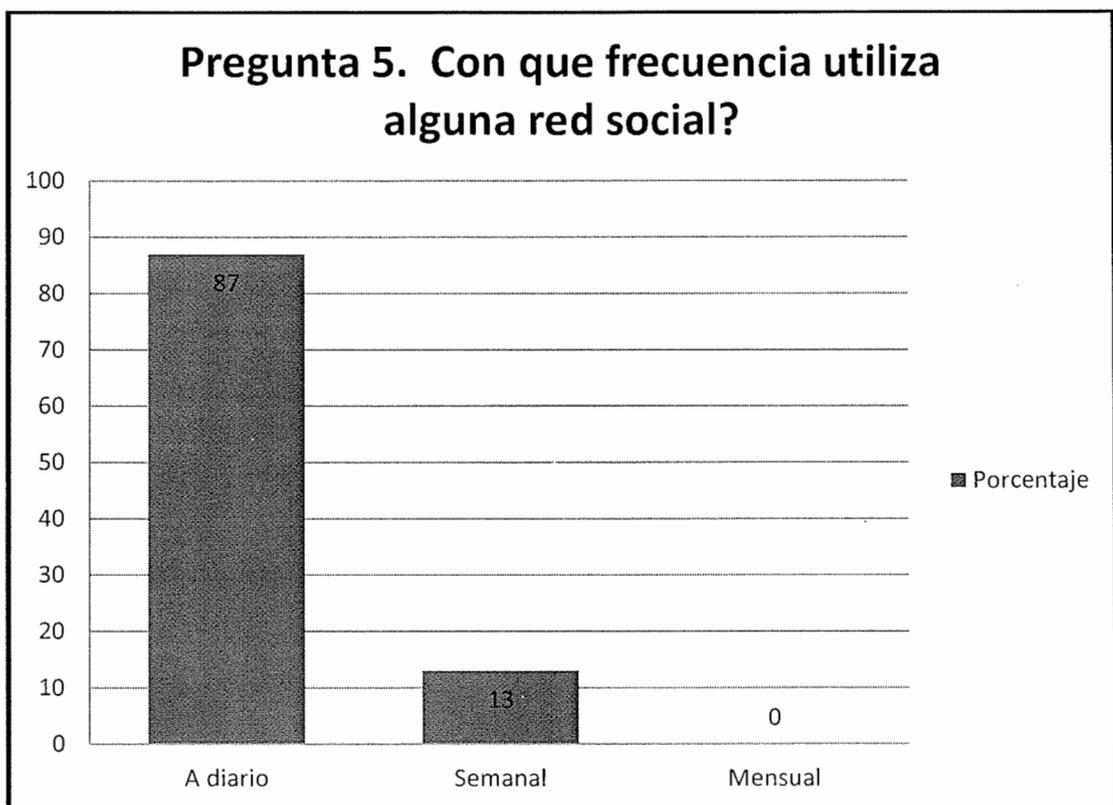
## ANEXOS

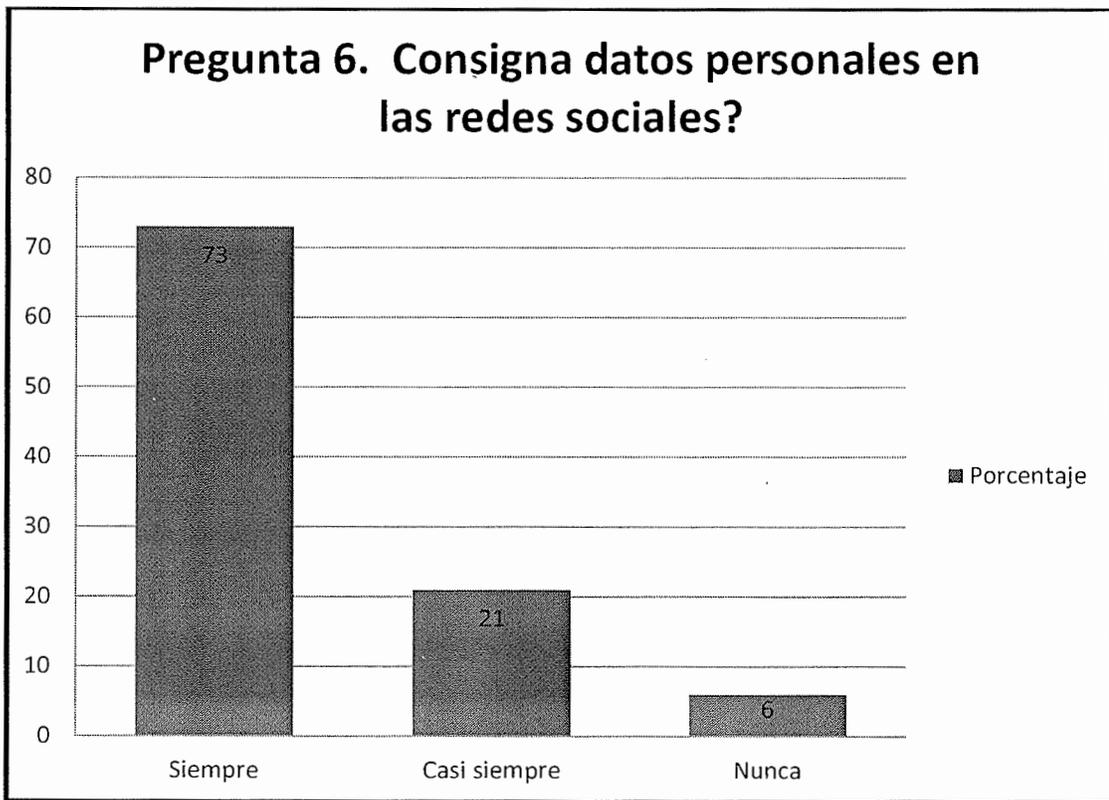


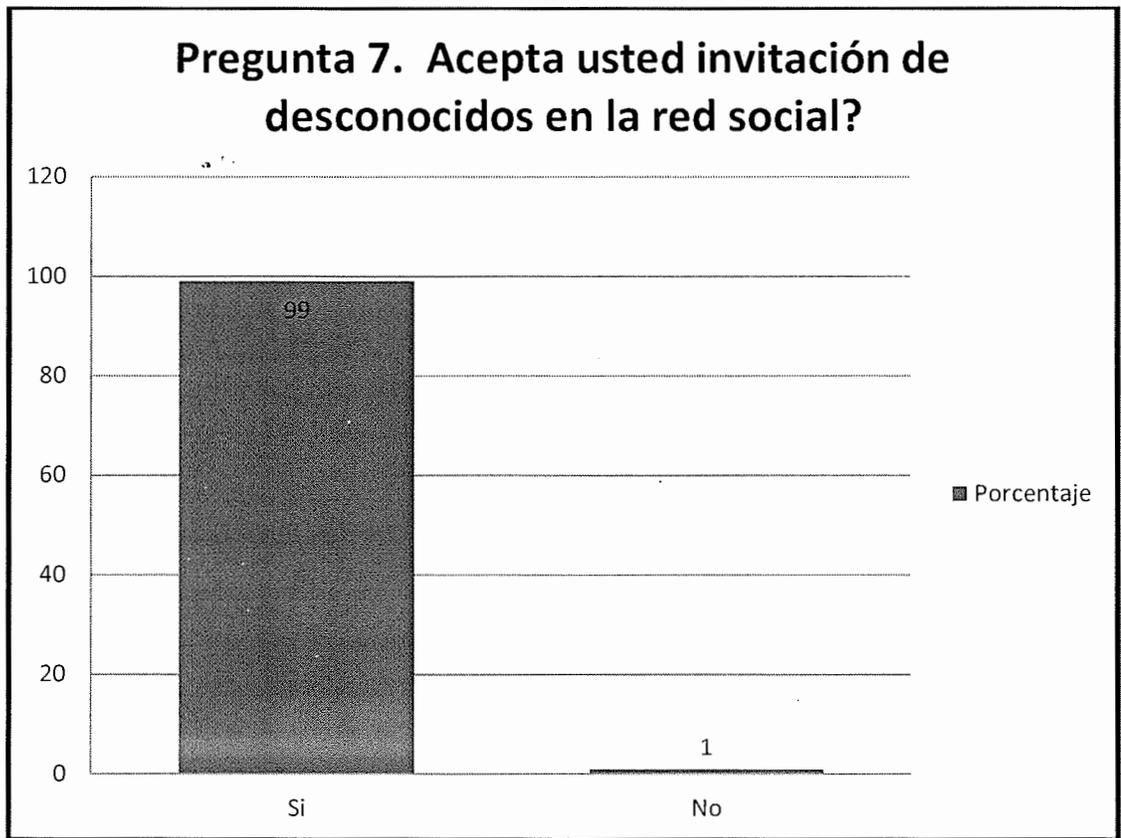


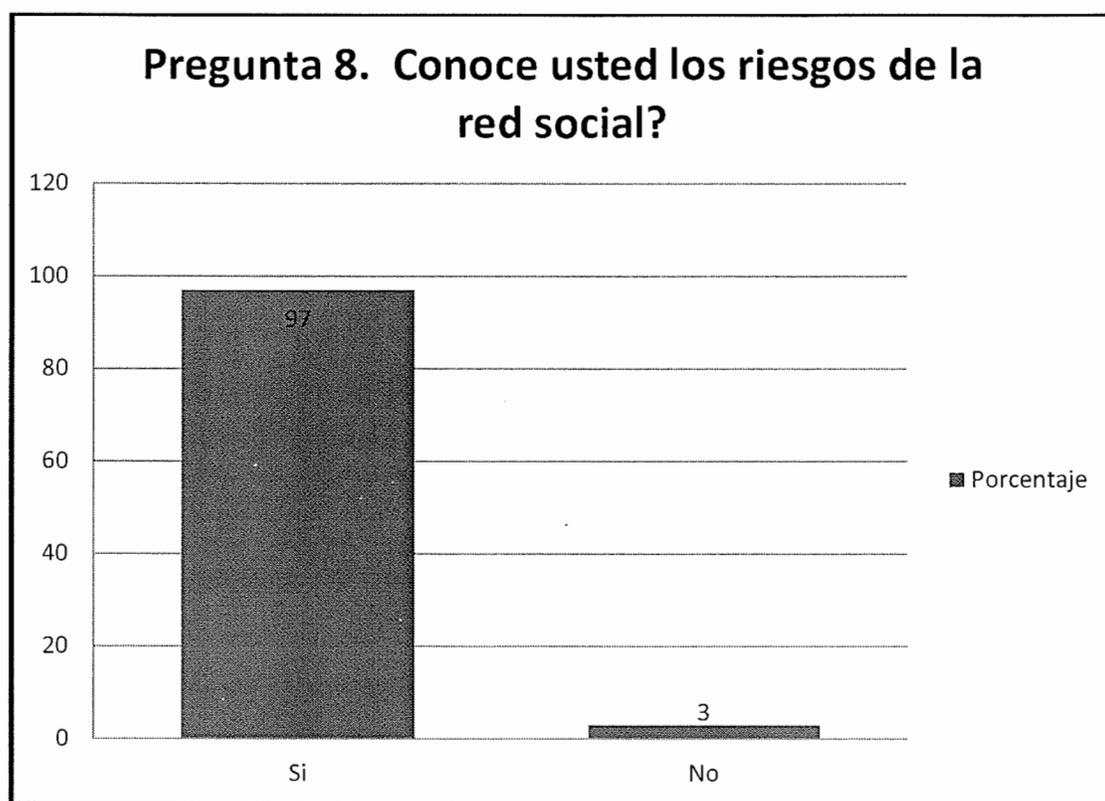




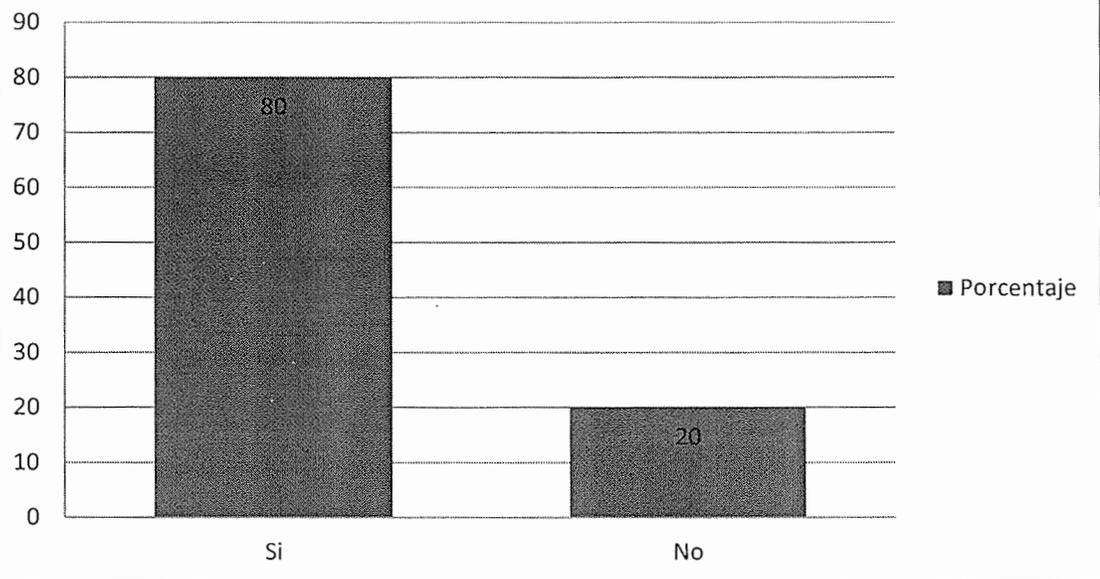


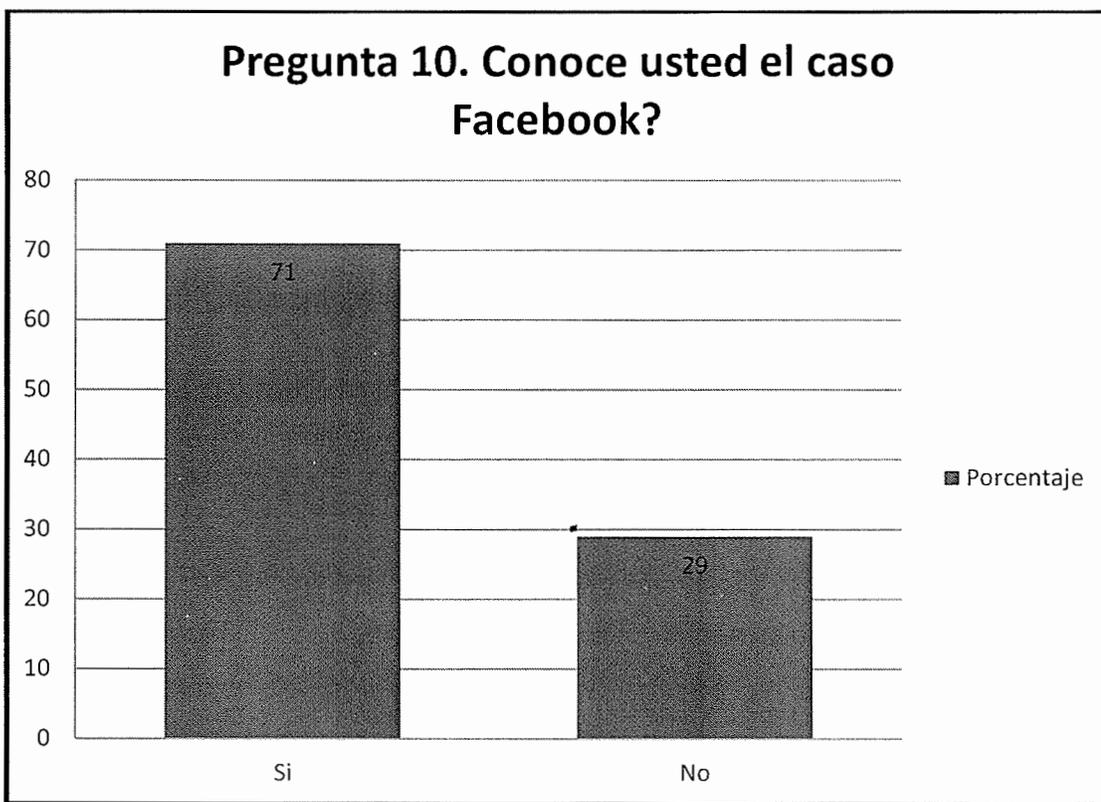






### Pregunta 9. Considera usted que la red social se utiliza como herramienta para cometer delitos?







## BIBLIOGRAFÍA

- BACIGALUPO, Enrique. **Manual de derecho penal**. Santa Fe. Colombia 1994.
- BLOSSIERS MAZZINI, Juan José. **Descubriendo los delitos informáticos**. Lima Perú.2003.
- BORJA JIMENEZ, Emiliano. **Derecho penal y paz social**. Revista Ciencias Penales. Costa Rica Año 1999.
- BUSTAMANTE ALSINA, Jorge. **La informática y la protección del secreto de la vida privada**. 1987.
- CARRARA, Francisco. **Derecho penal**. Bibliotecas Clásicas Volumen I México DF 1999.
- CORREA, Carlos María. **El derecho informático en América Latina**. Bogotá Themis 1990.
- DE LEON DUQUE, Jorge Eduardo. **Informe circunstanciado del Procurador de Derechos Humanos de Guatemala** (s.e). 2012.
- HULSMAN Louk **Sistema penal y seguridad ciudadana**. Universidad Católica de Barcelona España Ed. Bella Tierra. 1994.
- Informe de la **Comisión de protección de datos personales**. Agencia de Cooperación España 2009.
- JIMENEZ DE ASUA, Luis **Lecciones de derecho penal**. México DF Revista UNAM 1983.
- KELSEN Hans. **La teoría penal del delito**. Ediciones Nacionales México DF 1981.
- LOEVINGER, Lee. **Minnesota law review**. Volumen 34 (s.e), (s.f).
- LOZANO, Mario. **Sociología del delito**. (s.e),1990.
- MUÑOZ CONDE, Francisco. **Introducción al derecho penal**. Barcelona Bosch 1985.
- MUÑOZ CONDE, Francisco. **Teoría general del delito**. (s.e), (s.f).
- NIEVES, Ricardo. **Teoría del delito contemporáneo**. Revista del Ministerio Público República Dominicana 2008.

NORIEGA SALAZAR, Aarón Hans. **Delitos informáticos**. Instituto de la Defensa Pública Penal. Guatemala (s.e), (s.f).

OSSORIO, Manuel. **Diccionario jurídico penal político y social**. Database 2009.

Real Academia Española. **Diccionario de la real academia española**. Edición Electrónica, España 2007.

RUSCONNI, Maximiliano. **Las fronteras del derecho penal**. Buenos Aires Argentina (s.e), 2003.

SOLER, Sebastián. **Tratado de derecho penal argentino**. Tomo III (s.e), 1992.

TELLEZ VALDEZ, Julio A. **Derecho informático**. México Mc Graw Hill (s,e), 2008.

TIEDEMANN, Klaus. **Poder económico y delito**. Barcelona Ariel. 1985.

WEINER, Norbert **Cibernética, control y comunicación**. Barcelona (s.e). 1985

[www.congreso.gob.gt](http://www.congreso.gob.gt) (consultado: octubre 2013).

[www.cooperacionespañola.es](http://www.cooperacionespañola.es) (consultado: marzo 2014).

[www.ilifebelt.com](http://www.ilifebelt.com) (consultado: febrero 2014).

[www.oj.org.gt](http://www.oj.org.gt) (consultado: julio 2014).

[www.pdh.org.gt](http://www.pdh.org.gt) (consultado: octubre 2014).

[www.pgn.org.gt](http://www.pgn.org.gt) (consultado: septiembre 2014).

[www.publinews.gt](http://www.publinews.gt) (consultada 15/06/14).

[www.sit.org.gt](http://www.sit.org.gt) (consultado: septiembre 2014).

[www.transformarse.ar](http://www.transformarse.ar) (consultado: enero 2015).

[www.unam.mx](http://www.unam.mx) (consultado: abril 2014).

[www.wikipedia.com](http://www.wikipedia.com) (consultado: agosto 2014).

ZAFFARONI, Eugenio Raúl **Tratado de derecho penal**. Buenos Aires, Ediar. 1999.

ZAFFARONI, Eugenio Raúl. **Derecho penal**. Buenos Aires. Nuevo Offset. 2002.



## **Legislación:**

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

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

**Código Procesal Penal.** Decreto 51-92 del Congreso de la República, 1992.

**Ley de Acceso a la Información Pública.** Decreto 57-2008 del Congreso de la República, 2008.

**Ley de Derechos de Autor y derechos conexos.** Decreto 33-98 del Congreso de la República. 1998.

**Ley Contra la Violencia Sexual, Explotación y Trata de Personas.** Decreto 09-2009 del Congreso de la República. 2009.