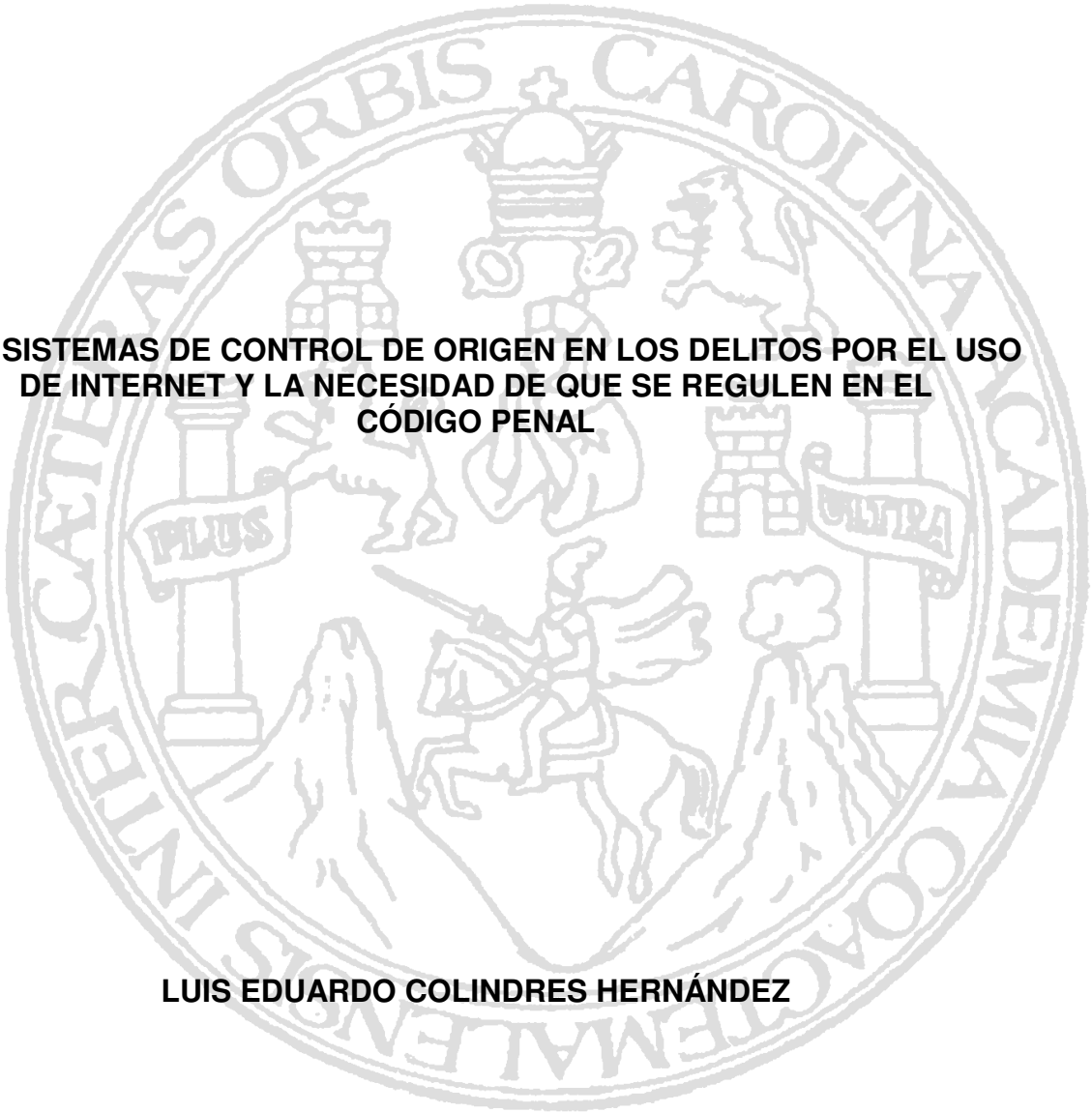
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL

LUIS EDUARDO COLINDRES HERNÁNDEZ

GUATEMALA, NOVIEMBRE DE 2010

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

LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

LUIS EDUARDO COLINDRES HERNÁNDEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, noviembre de 2010

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

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. César Landelino Franco López
VOCAL II:	Lic. Gustavo Bonilla
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Mario Estuardo León Alegría
VOCAL V:	Br. Luis Gustavo Ciraiz Estrada
SECRETARIO:	Lic. Avidán Ortiz Orellana

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).

Bufete Jurídico
Carlos Antulio Salazar Urizar
Abogado y Notario

Guatemala, 03 de agosto de 2009

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
01 SET. 2009
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guateala
Su Despacho.

Respetuosamente me dirijo a usted, de la manera más atenta, con el objeto de emitir dictamen sobre la tesis del bachiller LUIS EDUARDO COLINDRES HERNÁNDEZ, de su trabajo de tesis intitulado: **"LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL".** Después de la asesoría encomendada, dictamino:

1. El contenido científico y técnico de la tesis es el adecuado y para su obtención, el sustentante empleó la doctrina y legislación correcta, redactándola y utilizando un lenguaje apropiado y además desarrolló de manera sucesiva; los distintos pasos del proceso de investigación.

2. Los métodos de investigación empleados, fueron los siguientes: analítico, con el que se señaló la importancia del derecho penal; el sintético, dio a conocer la incorrecta utilización de los medios electrónicos; el inductivo, señaló los delitos electrónicos y el deductivo, dio a conocer su regulación legal. Las técnicas de investigación utilizadas fueron: fichas bibliográficas y documental, con las cuales se recolectó la información actual y suficiente.

3. La redacción empleada es la correcta y se ajusta perfectamente al desarrollo de la tesis. La hipótesis comprobó que existen actividades delictivas que se realizan por medio de estructuras electrónicas, que van ligadas a herramientas delictivas que buscan infringir y dañar todo lo que encuadre en el ámbito informático.

4. El contenido técnico y científico de la tesis, señala con datos actuales la importancia de estudiar la los delitos informáticos. Los objetivos se determinaron y establecieron que no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento de ellos, por parte de individuos irresponsables de los datos que dichos sistemas contienen.

Bufete Jurídico
Carlos Antulio Salazar Urizar
Abogado y Notario

5. La tesis contribuye de manera científica a la sociedad guatemalteca y es de útil consulta para profesionales y para estudiantes, y en la misma el ponente señala un amplio contenido que se relaciona con la importancia de sancionar; a quienes destruyan ordenadores y alteren medios electrónicos en Guatemala.

6. Las conclusiones y recomendaciones fueron redactadas de manera sencilla y constituyen supuestos certeros que definen que los sistemas informáticos abarcan aspectos de importancia, relacionados con el desarrollo y el funcionamiento de diversas actividades en Guatemala.

7. La bibliografía utilizada es la adecuada y de actualidad. Al sustentante le sugerí diversas enmiendas a su introducción, citas bibliográficas y capítulos; encontrándose conforme en llevar a cabo las modificaciones sugeridas.

La tesis desarrollada por el sustentante cumple efectivamente con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que emito **DICTAMEN FAVORABLE,** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Sin otro particular me suscribo de usted, atentamente.

Licenciado Carlos Antulio Salazar Urizar
8ª. avenida 20-22 zona 1
Tel: 22381390
Colegiado 6279
Asesor de Tesis

LIC. CARLOS ANTULIO SALAZAR URIZAR
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, veinticinco de septiembre de dos mil nueve.

Atentamente, pase al (a la) LICENCIADO (A) GLADYS ELIZABETH MONTERROSO VELÁSQUEZ, para que proceda a revisar el trabajo de tesis del (de la) estudiante LUIS EDUARDO COLINDRES HERNÁNDEZ, Intitulado: "LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL".

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. 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, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".

LIC. CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD ASESORÍA DE TESIS

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

cc.Unidad de Tesis
CMCM/sllh.

CORPORACIÓN DE ABOGADOS Y NOTARIOS ESPECIALIZADOS

12 calle 1-25 zona 10 local 312 3er. Nivel Edificio Géminis Diez

Tels: 23380330-23380331-23380349-23380350

Corporación_profesional@yahoo.es

Guatemala 09 de octubre de 2009

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
12 ENE. 2010
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su Despacho

Respetable Licenciado Castro:

Me honra informarle que en cumplimiento de la designación recaída sobre mi persona como revisora de tesis, según resolución proferida por la Unidad de Asesoría de Tesis a su digno cargo de fecha veinticinco de septiembre del año dos mil nueve, del bachiller LUIS EDUARDO COLINDRES HERNÁNDEZ, quien elaboró el trabajo de tesis intitulado: **"LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL";** le doy a conocer que la tesis abarca:

1. Un contenido científico y técnico del tema investigado, además se consultaron la doctrina y legislación adecuadas, utilizando una redacción y terminología jurídica acorde, clara y precisa, habiendo desarrollado sucesivamente los diversos pasos del proceso investigativo y dividiendo la misma en cuatro capítulos.

2. El sustentante, en el análisis realizado, señala la importancia de que se analicen los distintos sistemas de control de origen en los delitos informáticos.

3. Se emplearon los métodos apropiados, siendo los utilizados los siguientes: el método inductivo, se utilizó para determinar los sistemas de control; el método deductivo, dio a conocer las características de los mismos; el método analítico, señaló el inadecuado uso del internet y el método sintético, estableció lo esencial de la regulación de los delitos electrónicos.

4. La contribución científica del trabajo de tesis llevado a cabo, muestra con datos actuales que el internet es el medio masivo de comunicación imprescindible, para el desarrollo económico global. Los objetivos generales y específicos, fueron alcanzados al ser determinantes en señalar la importancia de que la legislación penal guatemalteca, sancione a los responsables de la comisión de delitos electrónicos. También, la hipótesis se comprobó, al indicar la misma, lo esencial de analizar toda conducta que revista características antijurídicas y culpables que atentan contra el soporte lógico de un sistema de procesamiento de información,

CORPORACIÓN DE ABOGADOS Y NOTARIOS ESPECIALIZADOS
12 calle 1-25 zona 10 local 312 3er. Nivel Edificio Géminis Diez
Tels: 23380330-23380331-23380349-23380350
Corporación_profesional@yahoo.es

sea sobre programas o datos relevantes; a través del empleo de las tecnologías de la información.

5. Las técnicas que se emplearon fueron la documental y de fichas bibliográficas, con las cuales se recolectó ordenadamente la bibliografía necesaria y actualizada relacionada con el tema.

6. La introducción, conclusiones y recomendaciones fueron redactadas en forma clara y sencilla, constituyendo supuestos válidos que dan a conocer la realidad nacional.

7. Le sugerí la necesidad de llevar a cabo algunas correcciones a los capítulos de su tesis, introducción y bibliografía, encontrándose conforme en su realización para una debida estructuración del tema investigado.

La tesis desarrollada por el sustentante cumple efectivamente con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que emito **DICTAMEN FAVORABLE,** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Sin otro particular, me suscribo de usted, deferentemente.

Licenciada Gladys Elizabeth Monterroso Velásquez
Abogada y Notaria
Colegiada 5956

Gladys Elizabeth Monterroso
Velasquez de Morales
Abogada y Notaria

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

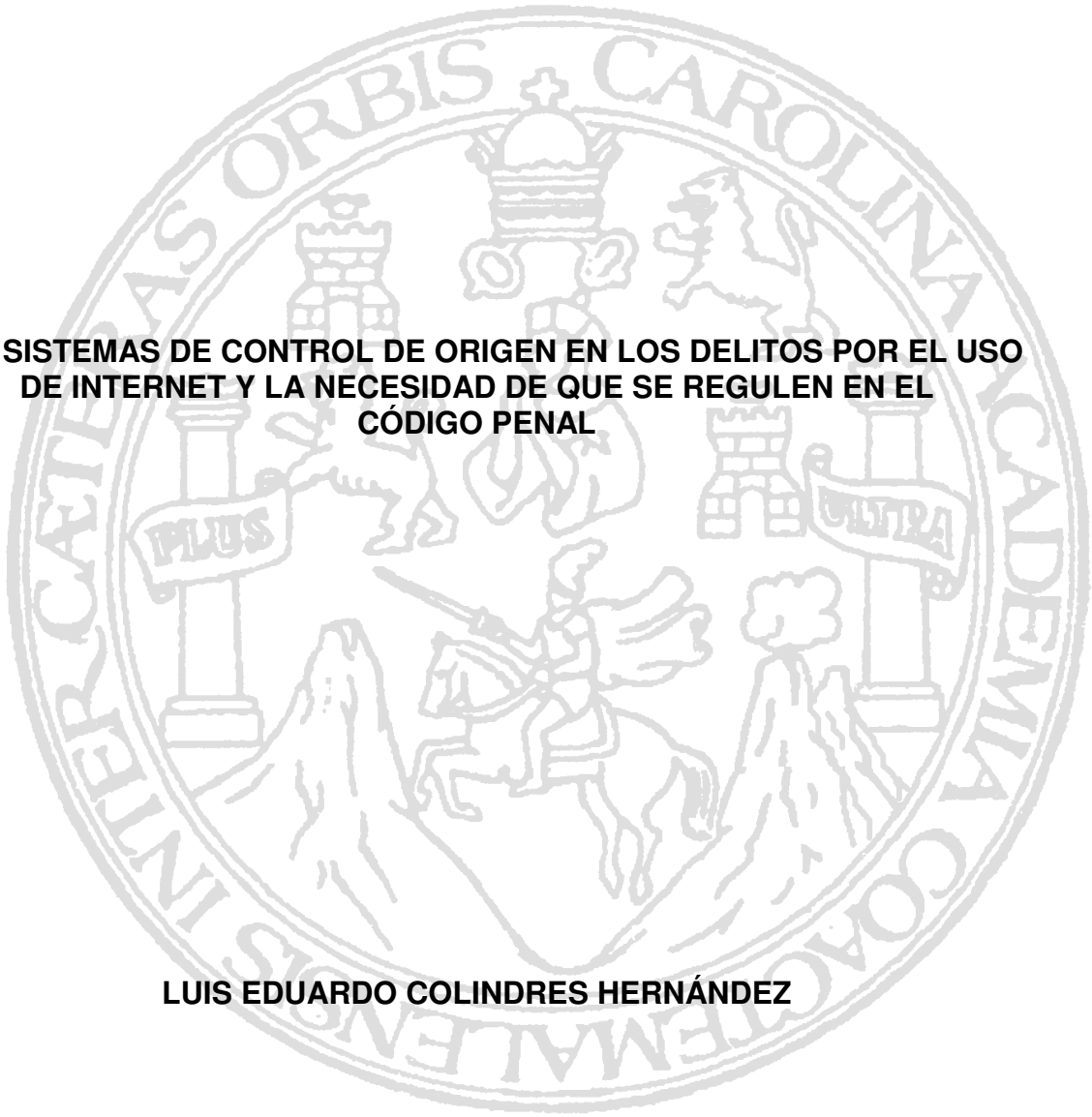
Ciudad Universitaria, zona 12
Guatemala, C. A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, cinco de octubre del año dos mil diez.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante LUIS EDUARDO COLINDRES HERNÁNDEZ, Titulado LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO 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.-

MTCL/sllh.

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



LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL

LUIS EDUARDO COLINDRES HERNÁNDEZ

GUATEMALA, NOVIEMBRE DE 2010

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

LOS SISTEMAS DE CONTROL DE ORIGEN EN LOS DELITOS POR EL USO DE INTERNET Y LA NECESIDAD DE QUE SE REGULEN EN EL CÓDIGO PENAL

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

LUIS EDUARDO COLINDRES HERNÁNDEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, noviembre de 2010

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

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. César Landelino Franco López
VOCAL II:	Lic. Gustavo Bonilla
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Mario Estuardo León Alegría
VOCAL V:	Br. Luis Gustavo Ciraiz Estrada
SECRETARIO:	Lic. Avidán Ortiz Orellana

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).

DEDICATORIA

A DIOS: Por bendecir diariamente mi vida, permitir alcanzar mis metas, y que en los momentos de adversidad, siempre me cobijo y nunca me desamparó.

A MIS PADRES: Maria y Miguel Colindres (Q.E.P.D.) dos grandes pilares en mi vida.

A MI ESPOSA: Ingrid Elizabeth de Paz Pérez, por ser parte de mi vida, su apoyo ha sido fundamental en el triunfo de mi carrera.

A MIS HIJOS: Christopher Alexander, Mildred Adriana, por la inmensa felicidad que me dan cada día y por quienes daré mi mejor esfuerzo para alcanzar el éxito.

A LOS PROFESIONALES: Licenciados: Gladis Elizabeth Monterroso Velásquez, Carlos Antulio Salazar Urizar y a cada uno de los que formaron parte de mi formación profesional.

A MIS AMIGOS: Estuardo Ulises, Erika Gonzáles, Marta Hernández, Danilo Picon, Héctor Pozuelos, por los momentos de solidaridad y muestras de compañerismo.

A: La gloriosa y tricentenaria Universidad de San Carlos de Guatemala y en especial a la Facultad de Ciencias Jurídicas y Sociales.

ÍNDICE

Pág.

Pág.

INTRODUCCIÓN

El tema de la tesis se eligió, debido a que el crecimiento del uso del Internet y de los distintos programas informáticos ha generado que muchas personas se conecten a las redes de Internet, lo cual les puede hacer vulnerables a los distintos ilícitos que se generan con el uso de la computación o bien a través de los software o programas; que permiten estar vinculados a las redes digitales.

Los objetivos dieron a conocer que en el Código Penal se regulan ilícitos vinculados a este tipo de actividades informáticas, especialmente en lo relacionado con los sujetos activos de los delitos; y en lo relativo a la jurisdicción y competencia vinculados a estos hechos penales.

En general, lo que se pretende analizar son los conflictos de jurisdicción en los delitos que se cometan a través del uso de la red, o del Internet. Un sistema global y abierto como Internet, lleva implícita la relación con personas que físicamente pueden encontrarse a miles de kilómetros y sujetos a leyes muy distintas a otras. El problema radica en que debe definirse la jurisdicción y competencia en el caso de los delitos informáticos, especialmente en el ámbito internacional, por cuenta a cometerse un hecho delictivo; éste debe definir el control de origen para que sea perseguido y juzgado. Existe conflicto de jurisdicción en el tema de los delitos informáticos, circunstancia que se encuentra regulada en el Código Penal, por lo que en el país debe establecerse jurisdicción y competencia en el juzgamiento. Es esencial el establecimiento de un análisis jurídico y doctrinario de la figura de los metatags y de la forma en como se emplean en el uso del Internet, así como la afectación que producen en las marcas y en los registros afectando la propiedad industrial, intelectual, inclusive derechos de autor, lo cual tiene que responsabilizarse penalmente, incluyéndose como figura delictiva en el Código Penal; como parte de los delitos informáticos. A través de la problemática planteada, es esencial buscar una solución a efecto de que se regulen en el Código Penal, los ilícitos a que pueden estar afectas las personas que violenten los sistemas de control o de seguridad en el uso del Internet y para ello, se tiene que establecer un marco normativo adecuado, técnico, acorde a esa realidad.

Para una mayor comprensión, el trabajo se clasificó, organizó y relacionó en cuatro capítulos, estando el primero organizado a partir de explicar los elementos definitorios del derecho penal, la teoría del delito y los factores que determinan los bienes jurídicos tutelados; el segundo, se redactó a partir de explicar el derecho informático, las características que hacen de esta rama del derecho una ciencia jurídica autónoma, así como la importancia que el mismo tiene para comprender el avance de la informática en el derecho; el tercero, se analiza los delitos informáticos, los elementos doctrinarios característicos de cada uno de ellos, especificando el bien jurídico tutelado, el sujeto activo y pasivo, así como la penalización que le corresponde de acuerdo a la gravedad del ilícito y del daño ocasionado. Por último, en el cuarto se hace una relación doctrinaria y legal acerca de los sistemas de control de origen en los delitos cometidos por el uso del Internet en el caso de los metatags, la necesidad de su regulación y la restricción de acceso a los prestadores de servicios.

Los métodos que se utilizaron fueron: el analítico, que permitió todo el conocimiento en partes, en relación a lo que establece la legislación nacional respecto a lo contenido en la doctrina, la realidad y las leyes; al aplicar el método de la síntesis, se permitió analizar separadamente los fenómenos objeto del estudio, para descubrir la esencia del problema y del fenómeno estudiado en cuanto a las repercusiones que tiene el fenómeno estudiado; así también el fenómeno en estudio y la necesidad de su adecuación jurídico legal. Dentro de las principales técnicas se aplicaron la bibliográfica y la documental, en cuanto al material que se recopiló para el desarrollo de la investigación, utilización de la tecnología como el Internet y otros. También se empleó por la naturaleza del trabajo, la aplicación de las técnicas para la interpretación de la legislación.

A partir de lo estudiado se puede argumentar que resulta fundamental la regulación de los procedimientos para el control de los sistemas automatizados que contribuyen a la comisión del hecho delictivo, por el uso de los metatags en el Internet; con lo cual se le garantiza seguridad jurídica a los usuarios de la tecnología cibernética.

CAPÍTULO I

1. El derecho penal

La ciencia del derecho es muy amplia, y una especialidad, es el derecho penal, se encuentra constituido por un conjunto de normas jurídicas, leyes, instituciones, principios, etc. El autor Luis Repolles; "para poder establecer la definición del derecho penal hace una relación de este concepto material y lo divide en cuanto al orden social en el control social, el control social penal, y se refiere a que un orden social cualquiera que éste sea, no se logra a través de un simple acuerdo sobre sus contenidos. Exige una profunda integración de muy diferentes instituciones sociales, sean de naturaleza primaria como la familia, la escuela, la comunidad local… sean de naturaleza secundaria como la opinión pública, los tribunales, la policía…Todas ellas aportan su colaboración para asegurar que los comportamientos de los ciudadanos sean socialmente correctos, ésto es, respetuosos con los contenidos del orden social acordados. "[1]

Los elementos fundamentales del sistema de control social en su conjunto, al igual que de los diferentes subsistemas en que aquél se descompone, son tres: la norma, la sanción y el procedimiento de verificación de la infracción de la norma, de determinación de la sanción a imponer y de cumplimiento de ésta.

Con respecto al control social penal, se refiere a que el derecho penal viene a ser un subsistema más dentro del sistema de control social, que, como todos los restantes, persigue sus mismos fines de aseguramiento del orden social y se sirve de idénticos instrumentos fundamentales, ésto es, normas, sanciones y proceso.

"Es el que establece y regula la represión y castigo de los crímenes o delitos por medio

[1] Repolles, José Luis. **Manual de derecho penal guatemalteco.** Pág. 3 a 5.

de la imposición de las penas."[2]

Sigue manifestando el autor; "lo primero que ha de hacer es fijar los bienes jurídicos que han de ser protegidos penalmente y sobre esos principios variables en el tiempo y en el espacio, configurar específicamente los delitos y establecer la pena que a cada uno de ellos corresponde."[3]

Continua manifestando José Luis Repolles; "respecto a la definición formal de las leyes que significa la definición de la norma jurídico penal, se refiere a la protección de bienes por el mismo derecho que se realiza a través del instrumento que constituyen las normas jurídico penales."[4]

Éstas pueden ser de dos clases: Prohibitivas o mandatos. Mediante las primeras el derecho penal prohíbe las acciones dirigidas a lesionar o poner en peligro los bienes jurídicos. A través de las segundas ordena realizar determinadas acciones para evitar la lesión o puesta en peligro de los mismos. En todo caso, en la medida en que van dirigidas a conseguir la omisión (objeto de prohibiciones) o la realización (objeto de mandatos) de acciones son normas de determinación, y no meras normas que valoran comportamientos.

El tratadista Eugenio Cuello Calón establece que; "es el conjunto de normas jurídicas que determina los delitos, las penas, y las medidas de seguridad que el Estado impone a los delincuentes y las medidas de seguridad que él mismo establece." [5]

Los juristas De León Velasco y De Mata Vela lo definen; "El derecho penal sustantivo o material. La parte del derecho compuesto por un conjunto de normas establecidas por

[2] Ossorio, Manuel**. Diccionario de ciencias jurídicas, políticas y sociales**. Pág. 345.
[3] **Ibid.** Pág. 345.
[4] **Ibid.** Pág. 17.
[5] José Francisco De Mata Vela y Héctor Aníbal De León Velasco. **Derecho penal guatemalteco.** Pág.6.

el Estado que determinan los delitos, las penas y/o las medidas de seguridad que han de aplicarse a quienes los cometen."[6]

De las anteriores definiciones, se puede concluir al respecto que el derecho que se encuentra conformado por un conjunto de normas jurídicas, instituciones, principios, creadas por el Estado para determinar los delitos, las penas y las medidas de seguridad, en este caso, también la ciencia comprende el estudio del derecho al que tiene como fin el mantenimiento del orden jurídico previamente establecido, ser preventivo, rehabilitador y se encuentra investido de una serie de principios fundamentales.

1.1. Naturaleza jurídica

Para que sea posible la convivencia entre los hombres se precisa una serie de normas positivas que establezcan las bases de coexistencia. El conjunto de estas normas constituye el derecho. Entre ellas, hay unas que a sus destinatarios imponen prohibiciones o mandatos de hacer u omitir determinadas conductas, amenazan con sanciones penales a quines los infrinjan y tienen como fin principal la lucha contra el crimen, que constituye el más importante factor que puede definirse como el sector de ordenamiento jurídico que tutela los valores fundamentales de la vida comunitaria, atribuyendo a un poder transpersonalista superior la facultad de exigir a los individuos comportarse de acuerdo con las normas, y de imponer penas o medidas de seguridad a quienes atenten contra aquéllos valores.

Para constituir la naturaleza, se tendría que plantear sus orígenes y la conformación actual, para entender los distintos criterios que la definen. Por un lado se ha determinado que esta ley es de carácter público, porque corresponde al Estado en ejercicio del poder punitivo sancionar a los ciudadanos que cometen infracciones a las

[6] **Ibid.** Pág.6.

normas penales, por otro lado, se ha establecido que esta misma es considerada como una ciencia, otros lo consideran como una disciplina jurídica, a juicio del sustentante, se razona ambos aspectos, toda vez, que constituye una ciencia, porque contiene elementos integrantes de la misma, toda vez que implica, un estudio científico, de averiguación que conlleva la experimentación, el ser efectiva y de aplicabilidad en la sociedad en el espacio y época determinada, con respecto a buscar la redefinición de los fines de la misma, en cuanto al ejercicio del poder punitivo del Estado que conlleva la facultad de juzgar y sancionar, tomando como base garantizar los derechos fundamentales individuales y colectivos.

No cabe duda que, para la existencia misma del derecho penal, como un conjunto de normas jurídicas que regulan la prohibición de determinadas conductas humanas, y que si se infringe con ello, el sujeto activo se hace acreedor de una sanción. Como afirma Rodríguez Devesa; "respecto a la intervención del Estado y al origen del derecho penal, éste necesariamente debe basarse precisamente en el principio de legalidad y de las garantías que de él se derivan, se halla en el anhelo de seguridad jurídica y en la lucha para excluir la arbitrariedad en el derecho punitivo."[7]

Pretende entonces, a través del ejercicio del derecho penal, como una disciplina jurídica, limitar ese poder punitivo del Estado, evitando excesos y arbitrariedades en contra de la sociedad.

1.2. Las fuentes del derecho penal guatemalteco

Al haber revisado una serie de libros de derecho penal, se ha podido corroborar que existen varias descripciones de las distintas fuentes del mismo. Al hacer un análisis de cada una de ellas, sea considerado que las que ha señalado el jurista de Mata Vela; "es la que se adecua más a la realidad nacional, específicamente al ordenamiento

[7] **Ibid.** Pág. 463.
[8] Ibid. Pág. 87.

jurídico penal guatemalteco, las describe como fuentes reales o materiales, refiriéndose a las que también en la doctrina se denominan substanciales, y que tienen su fundamento en la realidad social de los hombres y los pueblos y se refieren a los hechos naturales, a las expresiones humanas o a los actos sociales que determinan el contenido de las normas jurídicas, es decir, son las expresiones y manifestaciones socio- naturales previas a la formación de una ley punitiva, por cuanto que son los fenómenos naturales o sociales los que constituyen y plantean las necesidades de regulación penal por parte del Estado con el objeto de brindar protección a bienes jurídicos, que en un momento determinado se consideran amenazados por efecto de los fenómenos indicados."[8]

Con relación a las fuentes formales indican que son aquéllas que se identifican con el proceso de creación jurídica de las normas penales y los órganos del Estado técnicamente destinados a este proceso, de acuerdo a la organización política que corresponde al Organismo Legislativo a través del Congreso de la República.

En cuanto a las fuentes directas o inmediatas, indica que son aquéllas que por si mismas tienen la posibilidad de emanar directa e inmediatamente del derecho penal, es decir, las normas imperativo-atributivas que describen delitos, penas y medidas de seguridad. Agrega que las fuentes directas del derecho penal suelen dividirse en directas de producción y directas de cognición, las de producción se refieren al poder que dicta las normas o la autoridad que declara el derecho, que no es más que el Estado a través del Organismo Legislativo, representado por el Congreso de la República, que es el lugar donde por excelencia se producen las leyes, y las fuentes de cognición se refieren a la forma que el derecho objetivo asume en la vida social y en la cual se manifiesta la expresión de la voluntad del legislador, es decir, los códigos y las leyes penales.

[8] **Ibid**, pág. 88.

En cuanto a las indirectas o inmediatas, indica el tratadista que son aquéllas que por si mismas no tienen la virtud de crear normas jurídicas con carácter obligatorio, empero si pueden influir y coadyuvar en forma indirecta y mediata en la creación y proyección de nuevas normas jurídico penales, además que pueden ser de mucha utilidad en la interpretación, valoración y aplicación de la ley penal cuando se trata de resolver casos concretos. Éstas pueden ser la costumbre, los principios generales del derecho, los tratados internacionales y la jurisprudencia. El tratadista Edgar Maldonado Juárez; en su trabajo de tesis, describe la siguiente clasificación:

a. Reales o materiales: Hechos naturales o actos sociales que se manifiestan en una sociedad, previo a la elaboración de la ley penal.

b. Formales: El proceso de creación de la ley penal y los órganos que intervienen en su elaboración (Congreso y Ejecutivo).

c. Directas: Son aquéllas de donde emana directamente el derecho penal. La ley suele ser la única fuente directa para crear normas que contengan figuras delictivas, se subdividen en:

    - Fuentes directas de producción: Es la autoridad, el Estado, quien se manifiesta en el Organismo Legislativo.
    - Fuentes directas de cognición: La ley a saber, es decir, el código penal, que refleja la expresión de la voluntad del legislador.

d. Fuentes indirectas: Pueden coadyuvar a la formación de nuevas normas penales e incluso pueden ayudar en la interpretación y en la sanción de la ley penal. Pero no puede ser fuente de derecho. Carecen por si solas, de eficacia para obligar:

    - La costumbre: Conjunto de normas jurídicas no escritas, antes se aceptaba como fuente de derecho, hoy no.

- La jurisprudencia: Criterio constante y uniforme de aplicar la ley mostrando en las sentencias de los tribunales de la nación. La jurisprudencia es de mucha importancia para interpretar las leyes penales, pero no es fuente independiente ni productora de derecho. existen países en que sí.
- La doctrina: El derecho científico, conjunto de teorías, opiniones y especulaciones de los juristas, es tan solo una fuente de derecho indirecta.
- Los principios generales de derecho: Son los valores máximos a que aspiran las ciencias jurídicas, la justicia, la equidad y el bien común.

1.3. Los fines principales de la ciencia del derecho penal en la sociedad guatemalteca

" Los fines inmediatos que pretende la aplicación del derecho penal en la sociedad, es mantener ese control por parte del Estado a través del ejercicio del poder punitivo, y la sanción efectiva que amerita al infractor de normas prohibitivas e imperativas que se rigen en los códigos penales, permitiendo a la vez, mantener la armonía entre los ciudadanos que necesitan además de que se les prohíba la conducta que puedan afectar bienes jurídicos tutelados por el Estado, como lo son la vida, la seguridad, la libertad, proteger a los ciudadanos de los infractores o los que lesionen éstos bienes jurídicos."[9]

Ahora bien, tomando en consideración que el derecho penal, se constituye en el ámbito del ordenamiento jurídico y que se ocupa de la determinación de los delitos y faltas, de las penas, procede entonces, imponer a los delincuentes y de las medidas de seguridad establecidas por el Estado para la prevención de la delincuencia, el contenido de éste son:

[9] Maldonado, Juárez Edgar. **Análisis jurídico crítico del juzgamiento por analogía en los casos de la participación en el delito.** Pág. 7.

a. Los delitos
b. Las penas
c. Las medidas de seguridad y corrección

Al respecto, el tratadista Edgar Maldonado Juárez hace referencia; "El derecho penal criminal, tiene un fin único, que se mantiene tradicionalmente, el mantenimiento del orden jurídico previamente establecido, y su restauración a través de la imposición o ejecución de la pena cuando es afectado o menoscabado por un delito. Sin embargo, a lo anterior, hay que agregar que con el derecho penal moderno, se adiciona a las discutidas medidas de seguridad, un fin último: La objetiva prevención del delito y la efectiva rehabilitación del delincuente." [10]

1.4. La ley penal

"El término ley o lex proviene del verbo latino "lego (are)" que significa leer. La importancia de la ley escrita es que, en combinación con su carácter impersonal y abstracto, satisface el ideal de un "Estado de derecho." Sólo por la palabra escrita puede garantizarse los derechos ciudadanos (libertad, seguridad jurídica e igualdad ante la ley), estableciendo, así, un sistema de competencias para los gobernantes, en donde no existan situaciones jurídicas de excepción."[11]

Palacios Motta lo entiende en sentido amplio (lato sensu) e indica que es el conjunto de normas que definen los delitos y las faltas, determinándose las responsabilidades o las excepciones y establecen las penas o medidas de seguridad que corresponden a las figuras delictivas. Y en sentido estricto, como la ley penal es una norma de carácter general que asocia una sanción, pena o medida de seguridad, a una conducta prohibida por ella, es decir, el delito o la falta.

[10] **Ibid.** Pág. 10.
[11] Repolles. **Ob. Cit.** Pág. 246.

La ley penal, única fuente capaz de crear delitos y penas, estados peligrosos y medidas de seguridad, ha de reunir los requisitos materiales y formales exigibles a toda ley. En toda norma jurídica, existe un precepto o presupuesto y una sanción o consecuencia jurídica. La norma penal establece un presupuesto (la descripción de un delito, falta o estado peligroso, cuando se refiere a la posibilidad de imposición de una medida de seguridad) y le vincula una consecuencia imperativa (pena o medida de seguridad). Esto ocurre en los tipos penales que integran la llamada parte especial (delitos en particular) de los códigos penales, sin que se pueda extender esta técnica a la parte general de los textos penales, formada para evitar repeticiones de la norma penal.

La ley penal expresa el pensamiento del legislador e implica siempre un juicio de valor imperativo y desfavorable- sobre determinada conducta que desaprueba y castiga con una pena. La función que desempeña es castigar determinadas conductas, implicando indirectamente la prohibición de las mismas o estableciendo mediatamente una norma de conducta. Las normas que describen delitos o faltas y establecen penas se dirigen a todos los ciudadanos que integran la sociedad y también a los órganos judiciales encargados de su aplicación, mientras que estos órganos del Estado son los únicos destinatarios de las normas que describen estados peligrosos y establecen medidas de seguridad.

1.5. Características de la ley penal

Dentro de las principales características de la ley penal, las siguientes:

- "Generalidad, obligatoriedad e igualdad: Significa que una norma va dirigida a todos, a la general, sin distinción de ninguna naturaleza o criterio, por lo que se vuelve obligatoria para todo ciudadano, lo que consecuentemente trae una igualdad en la aplicación de la misma. La inmunidad o el antejuicio no afectan lo escrito, puesto que lo único que constituyen es un trámite especial para quien detenta este privilegio, sin embargo, es ley obligatoria para todos.

- Exclusividad: Es la exclusividad de la ley penal para hacer el derecho penal nadie puede ser penado por delitos o faltas que no estén contenidos en la ley, y a nadie se le puede aplicar penas que no sea previamente establecidas por la ley. Sólo la ley penal puede establecer ilícitos y solo ella puede imponer o asociar una sanción.

- Contiene normas prohibitivas e imperativas, así como son normas permanentes e ineludibles: Se establece que la ley penal contiene conductas que son prohibidas para la sociedad, porque protegen bienes jurídicos tutelados, además, de ser prohibitivas son imperativas, porque constituyen mandatos que de no cumplirse generan consecuencias jurídicas, no como lo que sucede con las normas morales, que aunque son prohibitivas de determinadas conductas, no son imperativas, porque es facultad del sujeto pasivo acatarlas o no, porque las consecuencias no son jurídicas, sino más bien morales." [12]

Son permanentes, porque se necesita de un proceso para que sean abolidas, y mientras este vigente la ley es ineludible.

1.6. Formas de la ley penal

La ley penal tiene un ámbito temporal y una eficacia espacial, así como una vigencia en relación con las personas. En este último sentido debemos proclamar que el principio de igualdad ante la ley (Artículo 4 de la Constitución) no admite excepciones en la norma penal.

El Artículo 3. Código Penal establece: "Ley excepcional o temporal. La ley excepcional o temporaria se aplicará a los hechos cometidos bajo su vigencia, aún cuando ésta hubiere cesado al tiempo de dictarse el fallo, salvo lo dispuesto en el Artículo 2. Que dice: Extractividad, si la ley vigente al tiempo, en que fue cometido el delito fuere distinta

[12] **Ibid.** Pág. 12.

de cualquier ley posterior, se aplicará aquella cuyas disposiciones sean favorables al reo, aún cuando haya recaído sentencia firme y aquél se halle cumpliendo su condena."

El ámbito temporal de la ley penal debe estudiarse teniendo en cuenta su vigencia o validez formal (desde su entrada en vigor hasta su derogación expresa o tácita) y eficacia o vigencia material (la ley penal se aplica a los hechos cometidos bajo su vigencia).

La regla general es el principio de irretroactividad y la excepción es la retroactividad de la ley penal favorable. Con carácter general se formula el principio de irretroactividad en la Constitución Política de la República de Guatemala, que dice en el Artículo l5. "Irretroactividad de la ley. La ley no tiene efecto retroactivo, salvo en materia penal cuando favorezca al reo."

Ostenta el jurista Edgar Maldonado Juárez al respecto; "que existen formas de la ley penal de manera formal y material. La ley penal formal se establece en tanto que ella nace del órgano técnicamente facultado para hacerlo, es decir: El Congreso de la República, en el caso de la ley penal material, es cuando nace la ley de un órgano que no es el que constitucionalmente esta establecido para crearla. Tal el caso de los decretos leyes que se emiten en un Estado de hecho, por no haber congreso." [13]

1.6.1. Especies de la ley penal

La ley penal es única, sin embargo, dentro del marco jurídico existen leyes generales, especiales y las que provienen de los tratados internacionales especialmente lo que se relacionan a los derechos humanos.

[13] **Ibid.** Pág.14.

“Las leyes que aparte de la principal, como el código penal, se convierten en especies son:

- Leyes penales especiales: Que rigen para personas de un fuero determinado: el Código Penal Militar, el Código de Aduanas, Ley de Contrabando y Defraudación, etc.

- Convenios internacionales: Tal es el caso del Código de Bustamante, Código de Derecho Internacional Privado. Cuando una ley interna los convierte en legislación del Estado, por ser países signatarios.

- Los decretos leyes: Son aquéllas leyes que emanan del Organismo Ejecutivo, toda vez que no existe congreso de la República por cualquier motivo, tal el caso de los gobiernos de factos y los Estados de emergencia. La ley de Protección al Consumidor, por ejemplo, que nace por emergencia y en un gobierno de facto.”

1.6.2. Leyes penales en blanco o abiertas

Entre las formas de aparición de la norma penal destacan las leyes penales incompletas, en blanco o necesitadas de complemento, en las que la propia ley penal se remite a otra fuente del derecho para integrar del precepto o la sanción, que pueden aparecer incluso en mandatos distintos. Así, la remisión puede hacerse a otra disposición de la misma ley penal, a otra ley distinta o a una disposición de rango reglamentario. En este último supuesto ley penal en blanco en sentido propio la delegación del legislativo en la administración debe restringirse al máximo y sólo es aconsejable que, por su propia naturaleza, son imposibles de determinar en las leyes penales.

“Son aquéllas normas penales en las que aparece muy bien definida la sanción que deberá imponerse al infractor de las mismas, pero para saber con precisión a que se

refiere la conducta delictiva que amenaza la pena descrita, debe consultarse otra ley o reglamento de autoridad competente. Son diferentes las leyes penales incompletas, puesto que se trata de normas que su interpretación requiere de un análisis extensivo y pueden provocar una laguna de ley, pero las primeras no."

1.7. El delito

"Según Rafael de Pina, es un acto u omisión constitutivo de una infracción de la ley penal. En el derecho penal, es la acción u omisión ilícita y culpable expresamente descrita por la ley bajo amenaza de una persona o sanción criminal."[14]

"Es la acción u omisión que sanciona la ley penal, nadie podrá ser sancionado penalmente por una acción u omisión, sí esta no se haya expresamente prevista como delito por la ley vigente cuando se cometieron o si la sanción no se encuentra establecida en ella."[15]

Para que exista un delito es necesariamente en primer término que la voluntad humana se manifiesta exteriormente en una acción u omisión, además de toda una serie de elementos positivos del delito que se analizarán como parte de la teoría general de delito a continuación.

1.7.1 La acción

La acción consiste en un actuar o hacer, es un hecho positivo el cual implica que el agente o sujeto activo, lleve acabo uno o varios movimientos corporales por si mismo, por medio de instrumentos, por medio de animales, mecanismos e incluso mediante personas.

---

[14] **Ibid.** Pág. 28.
[15] **Ibid.** Pág. 32.

1.7.2. La omisión

En caso contrario de la acción, la omisión consiste en realizar la conducta típica con abstención de actuar, esto no hacer, dejar de hacer, constituye el modo en forma negativa del comportamiento.

1.7.3. Tipos de omisión.

Existen distintos tipos de omisión en la doctrina. Puede ser omisión simple u omisión propia, que consiste en no hacer lo que se deba hacer ya sea voluntario o imprudencia con la cual se procede un delito, que no haya resultado de modo que se infringe una norma preceptiva, como por ejemplo, la portación de armas.

También está la omisión de comisión por omisión, que también es conocida como omisión impropia, y quiere decir, que es un no hacer voluntario imprudencia cuya atención produce en resultado material y se infringe una norma preceptiva y otra prohibitiva, como por ejemplo, en materia de alimentos, el incumplimiento de deberes de asistencia.

1.7.4. Tipicidad

La tipicidad no es más que el encuadramiento de la conducta a la norma previamente establecida, es la adecuación del hecho a la norma. Su fundamento se encuentra en los Artículos 6, l3 y l7 de la Constitución. El Artículo l7 establece que no hay delito ni pena sin ley anterior, hace preservar el principio de legalidad. El Artículo 6 se refiere de la detención legal, y el Artículo 13 a los motivos para auto de prisión.

1.7.5. Antijurícidad

Es un juicio de valor que se hace a través de la realización de la conducta y que se encuadra a la norma que contiene supuestos y prohibiciones, así como consecuencias,

que son las sanciones o las penas. Su fundamento se encuentra contenido en el Artículo 2, 17 de la Constitución Política de la República de Guatemala. El Artículo 2 se refiere a los deberes del Estado y el Artículo l7 al principio de legalidad, cuando establece que no hay delito ni pena sin ley anterior.

1.7.6. Punibilidad

La palabra punible proviene de pena, y es que en el derecho penal, la punibilidad es la facultad que tiene el Estado que al crear los delitos, también, establezca la pena que corresponde a cada uno de éstos delitos, graduándola en un mínimo y máximo, para que los jueces, la fijen de conformidad con las circunstancias atenuantes o agravantes que puedan modificar la responsabilidad penal.

1.7.7. Culpabilidad

Es el reproche que se hace al autor de un hecho que constituye delito, para ver si le es exigible que debió cumplir con la norma, de que debió haber observado la norma prohibitiva y que por no haberlo hecho, le es aplicable una sanción, una consecuencia. Su fundamento se encuentra en los Artículos 2, 4, 5, l7 de la Constitución Política de la República de Guatemala. Se distingue entre los delitos culposos y dolosos que regula el código penal. El Artículo 2 de la Constitución se refiere a los deberes del Estado, el 4 al principio de libertad e igualdad, el 5 a la libertad de acción y el l7 al principio de legalidad.

1.8. Clasificación del delito

Existen distintas clasificaciones que hacen doctrinarios y estudiosos de la teoría general del delito, sin embargo, para efectos de la realización del presente trabajo, únicamente, se mencionará las distintas formas de la comisión de los delitos y su ubicación.

Así, atendiendo a la manifestación de voluntad, se distingue entre: delitos de acción,

delitos de omisión y delitos de comisión por omisión. Observando el resultado, se diferencia entre delitos materiales, que exigen un resultado para su consumación; delitos formales, que se consuman con la simple manifestación de voluntad, y también entre delitos de lesión, que son aquéllos que dañan materialmente el bien jurídicamente protegido, y delitos de peligro, que lo hacen idealmente al determinar la puesta en situación de riesgo de dichos bienes. Contemplando el grado de su perfección, se clasifican en intentados, frustrados y consumados; con las subespecies de los delitos agotados e imposibles. Atendiendo a la forma de culpabilidad se distingue entre dolosos e imprudentes.

Si bien estas últimas clasificaciones tienen su base en el articulado del código penal, la clasificación legal que aparece en el código penal específicamente, en delitos dolosos y culposos, aunque hace también una diferenciación entre delito consumado, la tentativa, la tentativa imposible, los cambios de comisión, el caso fortuito.

1.9. El ente que realiza la persecución de los delitos

De conformidad con las reformas a la Constitución Política de la República, en el Artículo 251 Constitucional existe el fundamento de la creación del Ministerio Público, como una institución auxiliar de la administración pública y de los tribunales, con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país. Su organización y funcionamiento se rige por la Ley Orgánica del Ministerio Público contenida en el Decreto 40-92 del Congreso de la República.

El Ministerio Publico entonces es el ente que se encarga de la investigación y persecución de los delitos el cual se auxilia de Policía que está bajo su autoridad y mando inmediato, haciéndose mención que no es la única institución de la cual se auxilia, porque de conformidad con la ley, específicamente su Ley Orgánica y el código procesal penal, también, puede requerir información y colaboración a otras instituciones estatales afines.

La palabra Ministerio proviene del latín "Ministerium" que significa cargo que ejerce, empleo, oficio, u ocupación especialmente noble y elevado. Por cuanto a la expresión "público", está también se deriva del latín "Públicus" "Pópulos", Pueblo indicando lo que es notorio, visto o sabido por todos, aplíquese a la potestad o derecho de carácter general y que afecta en la relación social como tal perteneciente a todo el pueblo. Por lo tanto en su aceptación gramatical el Ministerio Público significa; "cargo que ejerce en relación al pueblo."[16]

Por lo que con las nuevas reformas que ha sufrido la legislación en materia penal se puede definir al Ministerio Publico como el encargado de investigar y perseguir el delito, abatir la impunidad y procurar la justicia, proporcionando el auxilio médico de manera inmediata que requiere la víctima del delito, así como la asesoría jurídica necesaria para la reparación del daño, salvaguardar las garantías individuales de los implicados en la comisión del delito, tutelar los derechos de personas incapaces o menores de edad, en todo proceso judicial velando por el Estado de derecho en su carácter de representante de sociedad por lo que el Ministerio Publico debe realizarse esencialmente en los principios de buena fe, lealtad a la sociedad, objetividad, imparcialidad, legalidad y respeto a los derechos humanos.

[16] Ossorio. **Ob. Cit.** Pág. 48.

CAPÍTULO II

2. El derecho informático y el uso del internet respecto a los denominados metatags

Para muchas personas cuando escuchan la palabra internet, automáticamente la asocian con las computadoras. Es precisamente a través del uso de una computadora, en que se puede acceder al internet, entendiéndose como una forma de comunicación que fue inventada recientemente y que ha producido gran impacto en la vida social en los distintos ámbitos, y en el caso de Guatemala, que hasta hace poco tiempo, aproximadamente en los años setenta, se empezó a utilizar esta forma de uso principalmente para facilitar la tarea laboral, en el caso de las impresiones, estudios, casos, guardar información, etc. y qué con el aparecimiento de esta forma de redes de comunicación, se ha incrementado enormemente su uso, siendo que en la actualidad, cualquier persona que adquiera una computadora, puede tener acceso al internet, como se verá más adelante.

Cabe agregar también, que aunado a las ventajas que podrían representar para la sociedad el uso del internet, en el ámbito de criminalidad, también lo simbolizó y personificó en la actualidad, porque el Estado como el ente rector de la paz y de quien es el llamado para sancionar conductas ilícitas a través del derecho penal, como se vio en el capítulo anterior, no ha estado a la vanguardia de estos avances, que han generado la violación a derechos fundamentales de las personas, pero que no son sancionadas estas conductas ni mucho menos perseguidas, por cuanto no se encuentran reguladas en el código penal como figuras delictivas, como se verá más adelante.

Es increíble imaginarse la gran gama de figuras ilícitas que se cometen a diario con el uso del internet y que esas conductas, aunque sean dañinas para las personas a quienes se les afecta, no se pueden sancionar, por una serie de circunstancias que

también se analizarán más adelante, pero fundamentalmente, una de ellas, es la falta de regulación en la ley. En este caso también se encuentran los denominados metatags que son las palabras del lenguaje HTML que pueden ser leídas solamente por los motores de búsqueda de la red y describen el contenido del sitio en el que se encuentran, de forma que pueden ser localizados y obtenidos por los usuarios interesados.

Si su empleo se realiza con el propósito de conducir a los usuarios a las páginas de los competidores, entonces constituye un acto de carácter ilícito provocando así un riesgo de asociación o confusión, en cuyo caso resultan de aplicación las normas de competencia desleal y que por esa situación a juicio de quien escribe, tal como se describen, deben ser regulados como delito en el código penal guatemalteco.

2.1. Definiciones

La información acerca del internet como tal, no se encuentra aún en libros del derecho. El internet es; "un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial."[17]

Derecho informático: entonces, es aquel conjunto de normas jurídicas, principios, instituciones que tienen relación directa con el uso de las tecnologías a través del internet y que facilitan las comunicaciones, previendo un marco regulatorio con el fin de evitar los abusos a que puedan estar expuestos los usuarios del mismo, como un deber del Estado.

Los metatags son; "etiquetas html que se incorporan en el encabezado de una página

[17] Sandoval Ramirez, Luis. **La computación en el siglo veinte.** Pág. 24.

web y que resultan invisibles para un visitante normal, pero de gran utilidad para navegadores u otros programas que puedan valerse de esta información.

Su propósito es el de incluir información (metadatos) de referencia sobre la página: autor, título, fecha, palabras clave, descripción, etc.

Esta información podría ser utilizada por los robots de búsqueda para incluirla en las bases de datos de sus buscadores y mostrarla en el resumen de búsquedas o tenerla en cuenta durante las mismas y será invisible para un visitante normal.

Estas etiquetas también se usan para especificar cierta información técnica de la cual pueden valerse los navegadores para mostrar la página, como el grupo de caracteres usando, tiempo de expiración del contenido, posibilidad de dejar la página en cache o calificar el contenido del sitio ("para adultos", "violento"…).

Estas etiquetas se incorporan en el código fuente entre las paginas web."[18]

Entonces, como se señaló los metatags son las palabras del lenguaje html que pueden ser leídas solamente por los motores de búsqueda de la red y describen el contenido, del sitio en el que se encuentran, de forma que pueden ser localizados y obtenidos por los usuarios interesados.

Si su empleo se realiza con el propósito de conducir a los usuarios a las páginas de los competidores, entonces constituye un acto de carácter ilícito provocando así un riesgo de asociación o confusión, en cuyo caso resultan de aplicación las normas de competencia desleal.

[18] Repolles. **Ob. Cit.** Pág. 53.

Estos actos ilícitos se pueden resumir en los siguientes supuestos básicos:

- Uso de signos registrados sin notoriedad. Se debe atender al principio de la especialidad, si son utilizados para páginas que no guardan relación de identidad o similitud, entonces no se produce una situación de infracción.

- Uso de los signos notorios o renombrados. Cuando la finalidad es atraer clientes aprovechando la reputación ajena para una actividad diferente, por la "curiosidad inicial de quien buscando una cosa encuentra otra." En estos casos se produce un deterioro de la imagen de marca y como resultado de la protección que se dispensa a los titulares de marcas notorias, se exceptúa la aplicación del principio de especialidad y, por tanto, se produce un acto claro de competencia desleal.

2.2. Breves antecedentes históricos del aparecimiento del internet a nivel mundial.

Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como arpanet entre tres universidades en California y una en Utah, Estados Unidos. Uno de los servicios que más éxito ha tenido en internet ha sido la World wide web (w w w, o "la web"), hasta tal punto que es habitual la confusión entre ambos términos. La w w w es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en internet, aparte de la web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VOIP), televisión (IPTV), los boletines

electrónicos (NNTP), el acceso remoto a otras máquinas (SSH y Telnet) o los juegos en línea.

En el mes de julio de 1961 Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

La primera red interconectada nace el 21 de noviembre de 1969, cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, y gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde 1959 (ver arpanet). El mito de que Arpanet, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, éste no fue el único motivo. Si bien es cierto que Arpanet fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables, tal y como se atestigua en la siguiente cita:

A raíz de un estudio, se extendió el falso rumor de que Arpanet fue diseñada para resistir un ataque nuclear. Ésto nunca fue cierto, solamente un estudio no relacionado con Arpanet, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores enfatizaron la robustez y capacidad de supervivencia de grandes porciones de las redes subyacentes. (Internet Society, A Brief History of the Internet)

En 1972. Se realizó la primera demostración pública de Arpanet, una nueva red de

comunicaciones financiada por la DARPA que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva arquitectura sirvió para que, en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

En 1983; el 1 de enero, ARPANET cambió el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a internet. Por otra parte, se centró la función de asignación de identificadores en la IANA que, más tarde, delegó parte de sus funciones en el internet registry que, a su vez, proporciona servicios a los DNS.

En 1986; la NSF comenzó el desarrollo de NSFNET que se convirtió en la principal red en árbol de internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de internet.

En 1989; con la integración de los protocolos OSI en la arquitectura de internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En el CERN de Ginebra, un grupo de físicos encabezado por Tim Berners-Lee creó el lenguaje HTML, basado en el SGML. En 1990 el mismo equipo construyó el primer cliente Web, llamado World Wide Web (W W W), y el primer servidor web.

En 2006, el 3 de enero, internet alcanzó los mil cien millones de usuarios. Se preve que en diez años, la cantidad de navegantes de la red aumentará a 2.000 millones.

Internet tiene un impacto profundo en el trabajo, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo de ésto es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) por ejemplo GNU, Linux, Mozilla y OpenOffice.org.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los weblogs, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de internet y las nuevas tecnologías es muy limitada para las personas.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería imposible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante.

Muchos utilizan el internet para descargar música, películas y otros trabajos. Hay fuentes que cobran por su uso y otras gratuitas, usando los servidores centralizados y distribuidos, las tecnologías de P2P. Otros utilizan la red para tener acceso a las noticias y el estado del tiempo.

La mensajería instantánea o Chat y el correo electrónico son algunos de los servicios de uso más extendido. En muchas ocasiones los proveedores de dichos servicios brindan a sus afiliados servicios adicionales como la creación de espacios y perfiles públicos en donde los internautas tienen la posibilidad de colocar en la red fotografías y comentarios personales. Se especula actualmente si tales sistemas de comunicación fomentan o restringen el contacto de persona a persona entre los seres humanos.

En tiempos más recientes han cobrado auge sitios como Youtube, en donde los usuarios pueden tener acceso a una gran variedad de videos sobre prácticamente cualquier tema.

La pornografía representa buena parte del tráfico en internet, siendo a menudo un aspecto controversial de la red por las implicaciones morales que le acompañan. Proporciona a menudo una fuente significativa del rédito de publicidad para otros sitios. Muchos gobiernos han procurado sin éxito poner restricciones en el uso de ambas industrias en internet. Un área principal del ocio en la Internet es el sistema Multi jugador."[19]

[19] Sandoval Ramírez. **Ob. Cit.** Pág. 23

A través de la información que se pudo recibir de qué es lo que significa y la historia o evolución que ha tenido esta forma de comunicación a nivel mundial, ha representado no solo beneficios, sino también perjuicios. Cabría señalar entonces, que el Estado en este caso, determinará los perjuicios para contrarrestarlos en beneficio precisamente de la población guatemalteca.

A pesar de que desde sus inicios, el internet, sirvió para navegar, como se ha señalado, respecto a algo muy concreto, como buscar información didáctica, información para ampliar nuestros conocimientos acerca de determinado tema, en la actualidad, la oportunidad de escritores de publicar a través de este sistema sus ideas, obras, etc., venderlas, comercializar productos, objetos, bienes, etc., también ha significado el interés de los criminales para provocar perjuicios con fines lucrativos en contra de la sociedad que utiliza este servicio.

A pesar de que su existencia es relativamente reciente, como se ha observado en el análisis histórico, la incorporación de tantas personas a la red hace que este fenómeno se vea en incremento a través del tiempo, tan es así, que se ha reducido el uso del teléfono, del manuscrito para hacer cartas a los parientes, amigos, etc., y que resulta mucho más cómodo que desde sus hogares, de sus trabajos, puedan comunicarse de un país muy lejano al otro y viceversa.

Como toda gran revolución, el internet augura una nueva era de diferentes métodos de resolución de problemas. Algunos sienten que produce la sensación que todos hemos sentido alguna vez, produce la esperanza que necesitamos cuando queremos conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios genera una sensación de cercanía, empatía, comprensión, y a la vez de confusión, discusión, lucha y conflictos que ellos mismos denominan como la vida misma.

Con la aparición de internet y de las conexiones de alta velocidad disponibles al público, ha alterado de manera significativa la manera de trabajar de algunas personas al poder hacerlo desde sus respectivos hogares. Internet ha permitido a estas personas mayor flexibilidad en términos de horarios y de localización, contrariamente a la jornada laboral tradicional de 9 a 5 en la cual los empleados se desplazan al lugar de trabajo.

"Un experto contable asentado en un país puede revisar los libros de una compañía en otro país, en un servidor situado en un tercer país que sea mantenido remotamente por los especialistas en un cuarto. Internet y sobre todo los blogs han dado a los trabajadores un foro en el cual expresar sus opiniones sobre sus empleos, jefes y compañeros, creando una cantidad masiva de información y de datos sobre el trabajo que está siendo recogido actualmente por el colegio de abogados de Harvard.

Internet ha impulsado el fenómeno de la globalización y junto con la llamada desmaterialización de la economía ha dado lugar al nacimiento de una nueva economía caracterizada por la utilización de la red en todos los procesos de incremento de valor de la empresa."[20]

Respecto al acceso a internet, incluye aproximadamente, "5000 redes en todo el mundo y más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red. Los servicios disponibles en la red mundial de PC, han avanzado mucho gracias a las nuevas tecnologías de transmisión de alta velocidad, como DSL y Wireless, se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite (ver tu casa desde el cielo), observar el mundo por webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego Multi jugadores en 3D, un buen libro PDF, o álbumes y películas para descargar.

[20] Ayau, Manuel. **Como mejorar el nivel de vida**. Pág. 8.

El método de acceso a internet vigente hace algunos años, la telefonía básica, ha venido siendo sustituida gradualmente por conexiones más veloces y estables, entre ellas el (ADSL), Cable Módems, o el (RDSI). También han aparecido formas de acceso a través de la red eléctrica, e incluso por satélite (generalmente, sólo para descarga, aunque existe la posibilidad de doble vía, utilizando el protocolo (DVB-RS).

Internet también está disponible en muchos lugares públicos tales como bibliotecas, hoteles o ciber cafés y hasta en shopping's. Una nueva forma de acceder sin necesidad de un puesto fijo son las redes inalámbricas, hoy presentes en aeropuertos, subterráneos, universidades o poblaciones enteras."[21]

2.3. Los metatags y su regularización en la legislación comparada

De conformidad con la naturaleza jurídica de los denominados metatags, tiene mucha relación con el ámbito en que se ha regulado en diversos países dirigido al derecho de marcas.

La pregunta que se debe hacer la sociedad mundial respecto a los metatags, es ¿cómo ha impactado el uso de redes informáticas como internet al derecho de marcas y qué tipos de conflictos pueden plantearse? Los conflictos derivados de la utilización de las marcas en internet pueden tomar diversas modalidades. Desde luego que la primera pregunta que habrá de responderse es: ¿qué constituye uso de marca en internet? La respuesta es casi tan variada como países existentes en el planeta.

"La cuestión radica en determinar las circunstancias bajo las cuales la reproducción y aparición de un signo de marca en internet constituye uso de marca en los distintos territorios en los que dicho signo es perceptible, por ejemplo, a través de una pantalla

[21] Córdova, Marco Antonio. **Delitos monetarios y reserva de ley orgánica.** Pág. 16.

de computadora. Simultáneamente, habrá que precisar si la persona responsable de uso de la marca en internet en un sitio queda sujeta a la jurisdicción de los tribunales de un país en la que la página y las informaciones en la misma son accesibles en ese país."[22] Específicamente, ¿mantener un sitio de internet que contenga una marca infractora conferirá jurisdicción personal sobre un demandado extranjero por cualquier tribunal donde el hecho ilícito pueda ser visto?

Para contestar esta pregunta, muchos tribunales a lo largo y ancho del globo han seguido el criterio de la naturaleza de los sitios de internet, desarrollado en el caso Zippo, donde el tribunal estableció una escala para determinar si era o no competente para conocer de controversias derivadas de contratos de internet de un asunto contra un individuo no residente en la jurisdicción. En un lado del espectro están los sitios activos donde el demandado claramente hace negocios en el internet. Al lado contrario se encuentran los sitios pasivos donde el demandado simplemente ha colocado información en un sitio que es accesible a usuarios extranjeros de otras jurisdicciones. En medio de ambos se encuentran los sitios interactivos donde el usuario puede intercambiar información con la computadora anfitriona o host.

Como una regla general, mantener un sitio pasivo implica que simplemente se provée información que no sea tendiente a ofrecer algo o a realizar transacciones comerciales, lo cual no es suficiente para establecer la jurisdicción personal. Los sitios interactivos son aquéllos que no son puramente informativos, sino que por ejemplo, permite a los usuarios intercambiar información, siendo relevante el nivel de interactividad y la naturaleza comercial de dichos intercambios. En los sitios activos, el responsable realiza negocios o actividades comerciales, aunque sea el simple ofrecimiento y no se lleguen a concretar transacciones específicas.

[22] **Ibid,** Pág. 18.

La postura que han adoptado los tribunales en Francia es ilustrativa de la línea de pensamiento contraria, la cual entiende que las autoridades de un país pueden conocer de las reclamaciones que ahí se plantean por el dueño de una marca registrada en ese país, por el solo hecho que la marca registrada aparece en una pantalla ubicada en el territorio del país de registro sin que dicha aparición esté autorizada por quien tiene la marca registrada en ese país. De esta manera, los tribunales franceses consideran que son competentes para conocer de estas controversias y que el derecho francés es aplicable desde el momento en que el signo en litigio aparece en una pantalla localizada dentro de su territorio. En apoyo de esta postura, se ha invocado el texto del Artículo 46, línea 3 del Código de Procedimientos Civiles de ese país, de acuerdo con el cual el actor puede escoger entre tres opciones en cuestión de jurisdicción:

1. En razón del lugar de residencia del demandado
2. En razón del hecho generador de daño
3. En razón del lugar donde ha ocurrido el daño

Como ejemplo de lo anterior, el 13 de octubre de 1997 los tribunales franceses decidieron un caso en el que la empresa alemana Brokat.Informations Systeme, Gmbh utilizaba la marca de servicios "PAYLINE", en el sitio www.brokat.de misma que fue demandada por este. SG2, la cual era la titular de dicha marca en el país galo. En el procedimiento quedó establecido que la empresa alemana ofrecía en Alemania el servicio en cuestión bajo la aludida marca y que dicho servicio se anunciaba en internet. El tribunal francés sostuvo que tenía jurisdicción para conocer del asunto por considerar que "la difusión de la internet es de naturaleza mundial y accesible en Francia, por lo cual el daño había tenido lugar en territorio francés". En el caso en cuestión, la empresa alemana fue condenada a "suprimir toda referencia a la denominación 'PAYLINE' en cualquiera forma, incluyendo en internet dentro de la 72 horas siguientes a la orden de apercibimiento, bajo el riesgo de pagar 5000 francos por cada día de retraso."

En otro caso disputado; “en 1996 donde los hechos eran similares, sólo que se desarrolló en una corte del distrito sur de Nueva York, el juzgador fue más cauto y realizó una ponderación mayor de la naturaleza internacional de los hechos del caso. La actora era la empresa Play boy Enter prises, Inc., la editora de la conocida revista de entretenimiento masculino. El demandado era el editor de una revista italiana conocida como Playmen, quien había abierto un sitio en internet en un servidor ubicado en Italia, donde era el titular de la marca, y en la cual se utilizaba la marca “playmen".

El sitio permitía diversos tipos de acceso, incluyendo fotos. Play boy aducía que dicho uso violaba una orden judicial emitida en 1981 que le impedía a la editorial italiana distribuir o vender sus revistas en los Estados Unidos y pedían que la empresa italiana impusiera claves y filtros a las tarjetas de crédito emitidas en los Estados Unidos, así como en general, impedir el acceso a ciudadanos de los Estados Unidos. Sin embargo, con respecto al uso de la empresa italiana de la marca “playmen" en las páginas de internet para servicio en Italia, lo cual estaba prohibido en los Estados Unidos, la corte sostuvo que a nadie le debe ser impedido instalar un sitio de internet bajo un nombre en particular por el simple hecho que el mismo es accesible desde un país en el cual la venta de dichos productos a través de internet esta prohibido. ”[23]

Además de los conflictos derivados del uso de marcas en internet, comenzaron a surgir conflictos por la incorporación en los nombres de dominio, de marcas idénticas o similares a otras cuyo titular también llevó su inconformidad antes los tribunales, a mediados de los noventas, y al no existir una regulación al respecto, los particulares intentaron llevar sus controversias ante los tribunales, alegando violaciones a sus derechos como legítimos titulares de marcas comerciales. Irónicamente, los que impulsaron esta evolución legislativa propiciada en algunos países, fueron precisamente aquéllos arriesgados hombres de negocios que caminaban una fina línea entre la intrepidez y la violación a los derechos de marca.

[23] Maldonado. **Ob. Cit.** Pág. 59.

Con respecto a la colisión que se presenta entre internet y nombres de dominio; y las marcas y otros signos distintivos, los casos que han surgido pueden clasificarse de la siguiente manera, de acuerdo al tipo de controversia a que se refieren:

- Cybersquatting o Domain-Grabbing, lo cual consiste en el registro de uno o varios nombres de dominio con el propósito de impedir su uso a los titulares de las marcas o de procurar su transmisión posterior a cambio de una remuneración.

- Cuando dos o más titulares de marcas idénticas o similares desean obtener el mismo nombre de dominio

- Cuando un signo distintivo es idéntico al nombre de una persona física o moral

- Uso de marcas famosas o notoriamente conocidas en los sitios de internet

Los primeros casos llegaron a los tribunales en Estados Unidos y Europa en 1995 y comenzaron a ser resueltos a partir de 1996. Dos de los casos más famosos tuvieron como demandado al mismo individuo, un hombre de negocios de apellido Toeppen, quien vivía en la ciudad de Champaign, en Illinois, Estados Unidos y quien operaba una empresa proveedora de servicios de internet o ISP y que al momento de la disputa ya había registrado más de 240 nombres de dominio de compañías famosas y quien admitió haber registrado dichos nombres de dominio con el propósito de re-venderlos o licenciarlos a los titulares de las marcas famosas. En el primer caso, el Sr. Toeppen sostenía que debido a que lo registró primero el nombre de dominio www.intermatic.com ante Network Solutions, Inc. éste le pertenecía. La parte actora, en cambio, sostenía que eso era una violación a sus derechos como titular de una marca que además estaba registrada y era famosa en aquel país. La corte concluyó que: (1) intermatic era una marca famosa; (2) el Sr. Toeppen realizaba un uso comercial de la

marca al ofrecer el nombre de dominio para su venta; (3) la utilización de la marca que el Sr. Toeppen hacía en la internet era considerada comercial; y finalmente (4) que el Sr. Toeppen estaba violando los derechos del titular de la marca, con base en el estatuto Anti-dilución o contra agresiones que importen la pérdida distintiva de la marca, por lo que se le ordenó a Toeppen que se abstuviera de utilizar el nombre de dominio y no impidiera que la empresa intermatic procurara obtener dicho nombre de dominio.

El mismo resultado legal se alcanzó dos años después en otro caso contra el mismo Sr. Toeppen, pero donde en esta ocasión la parte actora era la conocida empresa Panavision. La única diferencia relevante en los hechos de este caso fue que el demandado alegaba que hacía un uso válido del sitio www.panavision.com al desplegar un mapa del pequeño pueblo de Pana, en el Estado de Illinois, Estados Unidos, lo que de acuerdo a su ingenioso argumento, no constituía una violación a los derechos del titular de la marca porque el sitio mostraba la "visión" de "pana" y por lo tanto, era válido su uso del sitio www.panavision.com. A la postre, la corte que conoció del caso, no estuvo de acuerdo con ese argumento.

Otros importantes casos siguieron surgiendo en las cortes norteamericanas, destacándose uno que se refería al uso de una marca en el sitio de Internet, pero no como parte del nombre de dominio. En 1998 donde una señora de apellido Wells utilizaba la palabra "Play boy" para describir un hecho cierto en su sitio de internet con respecto a su identidad, que había sido la "Play mate del año 1981". Además, la demandada utilizaba la palabra "Play boy" en los metatags, donde había usado dicha palabra para indicar el contenido del sitio de internet. La corte del caso determinó que el uso de la Sra. Wells de la marca "Play boy" era simplemente para identificar el contenido del sitio hacer referencia legítima a su propia identidad y pasado profesional.

Del mismo modo, en Europa comenzaron a surgir las controversias en torno al uso de marcas en nombres de dominio o en los sitios de internet, siendo el Bundesgerichtshof (BGH) el que ha marcado la pauta a los demás tribunales europeos decidiendo al

menos cinco importantes casos en torno a las problemáticas más frecuentes e importantes. Dentro de las controversias importantes más trascendentes puede mencionarse la que sostuvo el consorcio petrolero Shell GMBH y un nacional alemán de apellido Shell, misma que fue decidida en revisión por el BGH.

El consorcio Alemán pidió que el demandado se abstuviese de utilizar el nombre de dominio WWW.shell.de y que este fuera transferido al titular de la marca. Al realizar un equilibrio de intereses entre la protección a los derechos del titular de la marca y la "protección al nombre" de las personas consagrada en el derecho alemán, la corte determinó que el usuario de internet que ingresa a la dirección www.shell.de espera encontrarse con la página del consorcio petrolero, quien posee un importante interés económico en dicho nombre de dominio, y no de un ciudadano Alemán. El tribunal concluyó que al utilizar la persona de apellido Shell dicho nombre de dominio para fines personales, la parte actora tenía prioridad para utilizar el nombre de dominio controvertido.

La respuesta a las controversias antes descritas y otras muchas suscitadas en buena parte del mundo desarrollado, trajo como consecuencia que la OMPI preparara un informe final sobre el primer proceso relativo a los nombres de dominio de internet, el cual estuvo disponible el 30 de abril de 1999 y fue entregado a ICANN. Dicho reporte fue la base para intensas negociaciones que dieron como resultado el diseño de una política uniforme para la resolución de conflictos referentes a nombres de dominio, (UDRP, por sus siglas en Inglés) misma que fue adoptada el 26 de agosto de 1999 por ICANN, fueron aprobados los documentos de implementación el 24 de octubre y se implementó el 1 de diciembre del mismo año. Al día siguiente, la primera demanda conforme a la UDRP fue recibida electrónicamente en el Centro de Mediación y Arbitraje de la OMPI y fue promovida por la World Wrestling Federation en contra de un ciudadano norteamericano por el registro del nombre de dominio worldwrestlingfederation.com.

El 28 de junio de 2000, a instancias del Ministerio de Comunicaciones, Información y Tecnología de Australia, a nombre de su gobierno y el de otros 19 países, solicitaron a la OMPI que iniciara un Segundo Proceso de la OMPI relativo a los nombres de dominio de Internet a fin de analizar aspectos que no se consideraron para el diseño de la UDRP. Este proceso dio como resultado el envío de un segundo reporte en 2001 y un segundo grupo de recomendaciones a ICANN en el 2002, mismas que aún no se han visto reflejadas en la UDRP.

La mencionada política uniforme UDRP está diseñada para ser aplicada en procedimientos totalmente en línea, donde la parte demandante escoge el proveedor de servicios arbitrales y las partes someten todas sus promociones electrónicamente. La UDRP se aplica en forma simultánea a cualquier procedimiento legal de carácter jurisdiccional que se encuentre disponible para el actor, si es el caso que la legislación doméstica contempla algún recurso o remedio ante los tribunales.

Ahora bien, un titular de una marca que sienta afectados sus derechos y que recurra a la UDRP buscará que uno de los siguientes remedios sean pronunciados por el árbitro o panelistas: cancelación o transferencia del nombre de dominio. El procedimiento se seguirá contra el que registró el nombre de dominio en disputa o aún ante la rebeldía de éste, bajo un procedimiento muy similar al conocido como In Rem, es decir, contra la cosa, utilizado por la legislación norteamericana. Para lograr lo anterior, debe demostrar todas y cada una de las siguientes circunstancias:

- Que el nombre de dominio en disputa es idéntico o semejante en grado de confusión a la marca de la parte actora;
- Que el demandado no tiene derecho alguno o interés legítimo sobre el nombre de dominio en disputa; y finalmente
- Que el nombre de dominio en disputa fue registrado o ha sido usado de mala fe.

Para demostrar la existencia de derecho alguno o interés legítimo que asista al demandado, éste deberá proveer evidencia de cualquiera de los siguientes supuestos:

- Que antes de la notificación de la demanda se hizo uso o se hicieron preparativos demostrables para el uso del nombre de dominio, en relación con el ofrecimiento de bienes o servicios de buena fe;

- Que la empresa o individuo demandado ha sido comúnmente conocido con ese nombre de dominio, aún cuando no sea el titular de la marca; o

- Que se está haciendo un uso no comercial o de conformidad con la libertad de expresión o de publicidad comparativa del demandado, sin intención alguna de obtener una ganancia comercial de clientes o manchar la reputación de la marca de la cual el actor es titular.

Debe aclararse que los procedimientos arbitrales conforme a la UDRP son ejercitados por titulares de las marcas conforme a la legislación interna del lugar de residencia de la parte actora, pero si ambas partes se encuentran en la misma jurisdicción, puede además invocarse la legislación nacional del país donde se trate. También debe aclararse que la simple falta de uso es evidencia en contra de la existencia de un derecho o interés legítimo. De la misma manera, evidencia de una oferta para vender o transferir el nombre de dominio o disponibilidad para cancelar el nombre de dominio es indicativo de la falta de derecho o interés legítimo, así como la adopción de una marca famosa o notoriamente conocida con la cual el demandado no tenga conexión alguna. Dada la dificultad de comprobar la mala fe, y más en un procedimiento a distancia, la misma UDRP provee una lista no exhaustiva de circunstancias que serán evidencia de dicha mala fe.

- La retención de un nombre de dominio con el propósito de ofrecerlo para su venta al titular por un precio mayor al de los costos directos en relación a la adquisición y mantenimiento del nombre de dominio.

- El registro de un nombre de dominio con el propósito de impedir el uso del mismo al titular de la marca, lo cual puede establecerse si el demandado se ha comportado de esa manera antes.

- Registrar el nombre de domino con el objetivo principal de trastornar el negocio de un competidor.

- Utilización del nombre de dominio para atraer o desviar clientes a sitios de terceros, con la intención de obtener una ganancia comercial y mediante la creación de condiciones que permitan la posibilidad de confusión.

Desde luego que es posible para el demandado oponer defensas y excepciones. También puede el demandado demostrar fehacientemente que en efecto tiene un derecho o interés legítimo en el nombre de dominio, ya sea porque es su nombre, denominación legal, apellido o por que igualmente posee un registro de marca o los derechos correspondientes a ésta.

También puede demostrar el demandado que ha hecho “preparaciones demostrables” para usar el nombre de dominio en disputa. De la misma manera puede demostrar que ha sido conocido ordinariamente mediante el nombre de dominio en disputa o que ha hecho un uso legítimo o en ejercicio de su libertad de expresión o realizar actividades que constituyan publicidad comparativa. El simple uso nominativo de una marca en tal forma que no cree confusión normalmente no constituye evidencia de mala fe.

La política aplica para disputas relativas a nombres de dominio genéricos, es decir, todos los que terminan en .com, .net y .org. También ha sido adoptada voluntariamente por los administradores de CCTLD como es el caso de los .nu, .tv y .ws. Los administradores de nombres de dominio de otros países, sin embargo, han decidido desarrollar sus propias políticas de resolución de conflictos, que en general son muy similares a la política uniforme ya comentada.

Por lo tanto, la UDRP se aplicará, y de hecho se ha aplicado, contra residentes en México que posean un nombre de dominio .com, .net, .org., .nu, .tv o .ws. Por cualquier individuo o compañía en cualquier parte del mundo. De la misma forma, podrá ser invocada por residentes en México, y si ambas partes residen en México, se aplicará además la Ley de Propiedad Industrial o la Ley Federal del Derecho de Autor en lo que se refiere a reservas de derechos. La UDRP ha sido aplicada en más de 6,000 disputas referentes a nombres de dominio, involucrando partes de más de 119 países y más de 11,000 nombres de dominio.

Por su parte, NIC México, el administrador del CCTLD .mx, adoptó las llamadas "Políticas Generales de Nombres de Dominio", así como las "Políticas de Solución de Controversias en Materia de Nombres de Dominio para .mx" (conocida comúnmente como LDRP) así como su reglamento el 11 de julio de 2003. Todas estas disposiciones fueron incorporadas por referencias a los contratos de los poseedores existentes de nombres de dominio a partir del 1 de junio de 2004, así como a los de aquéllos que adquirieron nombres de dominio .mx a partir de dicha fecha. De su revisión, es claro que la LDRP es en general similar a la UDRP. También el Reglamento de la Política de Solución de Controversias en materia de Nombres de Dominio para .mx es virtualmente una traducción literal de las Reglas para la Política Uniforme para la Resolución de Conflictos referentes a Nombres de Dominio. No obstante, pueden advertirse las siguientes diferencias:

- NIC México solo reconoce un proveedor de servicios arbitrales o de solución de controversias: El Centro de Mediación y Arbitraje de la OMPI.

- La LDRP se aplica no solo a marcas, en estricto sentido sino a marcas de productos o servicios, aviso comercial, denominaciones de origen o reservas de derechos.

- La LDRP puede ser invocada en caso de marcas y avisos comerciales, solo cuando éstos se encuentren registrados.

- La LDRP puede ser invocada en caso de denominaciones de origen y reservas de derechos cuando "el promovente tenga los derechos".

Al respecto conviene aclarar que es bastante impreciso el texto de la resolución en lo que se refiere a denominaciones de origen y reservas de derecho. Conforme a la legislación mexicana y a diferencia de lo que pasa en la gran mayoría de los países de Europa, el titular de las denominaciones de origen no son las asociaciones, cámaras, cooperativas o uniones de productores o fabricantes, sino el Estado mexicano, de acuerdo al Artículo 167 de la Ley de Propiedad Industrial, y es el Estado a través del Instituto Mexicano de la Propiedad Industrial (IMPI) el que autoriza a los particulares la utilización de determinada denominación de origen en relación con sus productos.

De este régimen tan particular surgen situaciones donde más de un individuo o empresa está en igualdad de circunstancias para obtener la titularidad del nombre de dominio, y la política no parece contener mecanismo alguno que lidie con dichos casos. Como ejemplo, pensemos en la denominación de origen "tequila", cuyo titular es el Estado mexicano, pero respecto de la cual existen diversas empresas autorizadas en los términos del Artículo 169 de la Ley de Propiedad Industrial. Luego entonces, surge la pregunta ¿quién tiene el mejor derecho para ser el titular del nombre de dominio

tequila.com.mx? ¿El primero en registrarlo? O ¿Todos por igual? O ¿Será titular el Estado mexicano?, en cuyo caso ¿Quién administrará el sitio?, etc. Ninguna de estas cuestiones es prevista por la LDRP ni su reglamento.

Por otro lado, en lo que respecta a las reservas de derechos, la LDRP señala que toda persona que estime afectados sus "derechos", debe mostrar que tiene los "derechos" sobre la "reserva de derechos". Además de lo criticable de la redacción, la LDRP omite reconocer claramente que la única forma de ser el titular de la reserva de derechos es mediante el "certificado" expedido por el Instituto Nacional del Derecho de Autor (INDAUTOR), mismo que no es otra cosa más que la representación del "registro" o "inscripción" que el propio instituto realiza.

Por tanto, en nuestra opinión, hubiera sido más claro hacer referencia a que podrá ser invocada la LDRP cuando la reserva de derechos "se encuentre registrada" al igual que el lenguaje utilizado para las marcas y avisos comerciales, contribuyendo así a la claridad con respecto de quienes pueden invocar la política para resolver conflictos .mx.

Cabe mencionar que se excluye por completo de la LDRP a los nombres comerciales, que a pesar de ser protegidos conforme a la Ley de Propiedad Industrial, no son tutelados por dicha política. Tampoco queda claro si las marcas colectivas se encuentran protegidas por la LDRP, aunque en caso de que ambas partes tuvieran su residencia en México, pudiera aplicarse la Ley de Propiedad Industrial mediante la invocación de la cláusula 19 del reglamento de la LDRP, tal y como sucede con la disposición equivalente de la UDRP.

La LDRP ha sido utilizada para resolver solamente 6 casos en 2004, ordenándose en todos ello la transferencia del nombre de domino a la parte actora. Otros 10 casos referentes a nombres de dominio .mx fueron resueltos conforme a la UDRP, en donde el resultado fue que en 6 de ellos se ordenó la transferencia de los nombres de dominio

involucrados, en un caso se ordenó la cancelación, en uno de ellos el demandado conservó el sitio, y los 2 procedimientos restantes no fueron concluidos.

Finalmente recordemos que a pesar de la importancia de la LDRP no podemos hablar que éste constituya un avance legislativo en estricto sentido, toda vez que no es una ley ni tratado internacional, ni ha pasado por el proceso legislativo. Por el contrario, constituyen una serie de disposiciones o estipulaciones contractuales que son incorporados por referencia a los contratos de registro de nombres de dominio, en uso de la libertad contractual de los adquirentes. La LDRP, aunque muy importante, no le debe ningún mérito a las autoridades administrativas, ni al congreso de la unión, ni es aplicada por los tribunales federales. Es producto, al igual que la UDRP de un mecanismo ingenioso e intrincado en su diseño, pero sencillo en su implementación y efectivo para resolver controversias por la vía privada, es decir, del arbitraje.

Como hemos visto hasta ahora, tanto la UDRP como la LDRP son generalmente vistas como adelantos legales excepcionales. La UDRP con sus distintas adecuaciones en las políticas implementadas en diferentes países se ha convertido en un mecanismo exitoso para dirimir controversias relativas a nombres de dominio, que resuelve muy bien las problemáticas de la jurisdicción, la notificación al demandado, la territorialidad, el espacio y los costos. Además de eso, algunos textos que se proponen para el Tratado de Libre Comercio de América, han revelado que se planea incluir a la UDRP como política para la resolución de nombres de dominio en todos los países de América, lo que en la práctica se ha adelantado.

No obstante, para muchos autores la UDRP dista mucho de ser perfecta, y otros más señalan airadamente las inconsistencias. Kieren McCarthy, identifica las siguientes:

- No se especifica en quien recae la carga de la prueba
- No especifica que debe probarse para comprobar la inocencia o culpabilidad

- Impone plazos muy cortos
- No se requiere un contacto entre el actor y el demandado antes de someter el asunto a arbitraje
- La parte actora elige el proveedor de servicios arbitrales
- No existe un proceso de apelación
- Los árbitros, frecuentemente usan como fundamento áreas del derecho sobre las cuales no tienen facultad para pronunciarse
- Muchos árbitros han ignorado consideraciones para probar interés legítimo más allá de la propiedad intelectual
- Las defensa de “mala fe” es insignificante
- Nadie monitorea las reglas contenidas en la propia UDRP

Aunque el análisis de cada uno de estos temas requerirían ser abordados con mayor profundidad de la que requiere un trabajo de esta extensión, el autor arriba citado esgrime convincentes argumentos para sostener su posición y de forma preliminar, podemos apuntar que coincidimos con varias de las consideraciones de su postura.

Otros estudiosos apuntan que la UDRP presenta las siguientes desventajas:

1. Definitividad: Las partes son libres de llevar su asunto ante los tribunales antes, durante o después del procedimiento arbitral y los tribunales, en muchos países, no están obligados por el leudo del panel arbitral.
2. Daños y perjuicios: Al panel arbitral no le es permitido pronunciarse con respecto a los daños y perjuicios que el actor que prevalezca en sus pretensiones debe obtener, limitándose a decidir sobre la cancelación o transferencia del nombre de dominio.

3. Tratamiento completo: Si el demandado ha incurrido en otros actos ilícitos, tales como diluir la fuerza distintiva de la marca, publicidad engañosa o competencia desleal, el titular de la marca quisiera litigar todos estos asuntos y reclamar todas las acciones en un mismo procedimiento, en vez de ir por partes.
4. Pruebas: Las decisiones del panel arbitral son tomadas con base en la demanda, la contestación, y en el caso de ciertos proveedores de servicios arbitrales, también con base en las réplicas y contrarréplicas. Si el titular de la marca desea ofrecer pruebas adicionales o la mala fe del demandado no queda claramente asentada en los documentos antes mencionados, no hay posibilidad de alegatos ni pruebas adicionales.

Por otro lado, como lo demuestra en su excelente estudio Keith Blackman, las críticas que actualmente se hacen a la UDRP tienen un gran sustento, sobre todo en lo que se refiere al abuso de la política para beneficiar los intereses de grandes compañías y suprimir para librar batallas en Internet contra los críticos de algunos productos o servicios.

En efecto, la UDRP ha servido para que muchas compañías y particulares suspendan el uso de nombres de dominio, sin tener que probar siquiera la violación a sus derechos de propiedad intelectual, lo cual es permitido por la política, ya que una vez admitida la demanda, el sitio es suspendido en lo que se resuelve el asunto. Esta práctica es conocida como reverse hijacking la cual es definida como “utilizar la política de mala fe para intentar despojar o impedir el uso, así como para causar molestia al nombre de dominio a su titular”.

Otra consecuencia de la aplicación de la política han sido las limitaciones a la libertad de expresión, derecho fundamental que es reconocido por la mayoría de las constituciones del mundo occidental. La cláusula 4 (c) de la UDRP establece que el demandado que no haga un uso comercial del sitio o que sea conocido ordinariamente

por medio del nombre de dominio, solo puede demostrar un interés legítimo si utiliza el sitio en forma no comercial o en ejercicio de su libertad de expresión o de realizar actividades que constituyan publicidad comparativa que, sin intención de atraer o desviar clientes a sitios de terceros o manchar la reputación de la marca de la cual el actor es titular.

El lenguaje utilizado en la cláusula citada encuentra su fundamento en el Federal Trademark Dilution Act, y al igual que éste busca combatir las conductas que dañen el buen prestigio ganado por las marcas, pero en la práctica, dicha definición ha sido ampliada por los panelistas al aplicar la UDRP. Lo anterior ha tenido el indeseable propósito de afectar la libertad de expresión de muchos ciudadanos que legítimamente quieren mostrar en el ciberespacio sus puntos de vista.

La UDRP representa un sorprendente avance en la protección de marcas en un ámbito completamente nuevo: el ciberespacio. Hasta ahora, muy pocos países han adoptado o promulgado leyes que permitan a los titulares de marcas y otros derechos de propiedad intelectual acudir a los tribunales para buscar la tutela de sus derechos y de sus intereses. En Latinoamérica, pocos países han reformado sus legislaciones, y ni siquiera se encuentran actualmente discutiendo alguna ley que permita lidiar con esta nueva problemática, ni sus tribunales se han visto dispuestos a aplicar las reglas generales del derecho civil o de la legislación especializada de propiedad intelectual para proteger los signos distintivos. En muchos otros casos, tampoco los particulares se han visto motivados para llevar sus controversias a los tribunales nacionales mediante un procedimiento jurisdiccional a fin de procurar un cambio legislativo a través de precedentes judiciales.

El panorama anterior nos deja con la visión de que la UDRP, y las demás políticas adoptadas por los administradores de dominios nacionales, han sido el único medio eficaz para dirimir controversias relativas a conflictos derivados del uso de marcas en nombres de dominio. Dicho sistema ha mostrado que una solución privada, sin la

intervención de la administración pública, de los respectivos parlamentos de los países, ni de un tratado internacional, puede resultar exitosa y puede ser implementada en forma notablemente rápida. También ha demostrado que la privatización de la justicia en determinadas controversias especializadas puede resultar tan eficaz (o incluso más) que los procedimientos jurisdiccionales nacionales; y que la inclusión de cláusulas por referencia mediante anexos a contratos privados mediante el uso del sacrosanto principio de la libertad contractual puede ser un recurso extremadamente flexible y ágil para crear todo un nuevo sistema normativo.

La aplicación tanto de la UDRP como de la LDRP resulta de la voluntad de las partes, mediante una cláusula arbitral y mediante la incorporación por referencia, en el propio contrato, del texto de dichas políticas de resolución de conflictos. Debido a que el registro de nombres de dominio se hace completamente en línea, su contratación se realiza mediante lo que la doctrina mexicana denomina contratos de adhesión. El contrato de adhesión o por adhesión se encuentra regulado en México por la Ley Federal de Protección al Consumidor (LPC) y puede definirse como aquel en el cual una de las partes establece un contenido prefijado del mismo para ser utilizado en todas las transacciones de determinado tipo, para la realización de actos en masa y con respecto de los cuales, su clausulado solo puede ser pura y simplemente aceptado. A pesar de que algunos los consideran como simples actos jurídicos unilaterales o los critican por propiciar los abusos por parte de las empresas, la jurisprudencia mexicana ha dicho que la característica de que una de las partes fije su contenido “no afecta su validez, ya que no implica la ausencia de la alternativa de aceptarlo o rechazarlo en forma total o parcial por quien no interviene en su elaboración”.

La LPC la define como “el documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato.” Ahora bien, con base en este análisis, es claro que los contratos de registro de nombres de dominio son contratos de

adhesión, debido a que son celebrados en línea, sin la posibilidad de modificar sus cláusulas y expresando la voluntad mediante la simple aceptación del contrato en su totalidad.

Con respecto a la forma del consentimiento otorgado por medios electrónicos, es claro que éste es válido y se equipara al consentimiento otorgado en forma expresa. Ahora bien, la siguiente cuestión será determinar la validez del contenido del mismo. Al respecto, la misma LPC establece que no son válidas y se tendrán por no puestas las cláusulas que se consideren abusivas. Las cláusulas a las cuales se refiere la LPC se encuentran contenidas en su Artículo 90 y son las siguientes:

- Las que permiten al proveedor modificar unilateralmente el contrato o sustraerse de sus obligaciones.
- Las que liberen de su responsabilidad civil al proveedor, excepto cuando el consumidor incumpla el contrato.
- Las que trasladen la responsabilidad civil del proveedor al consumidor o un tercero.
- Las que prevengan términos de prescripción inferiores a los legales.
- Las que prescriban el cumplimiento de ciertas formalidades para la procedencia de las acciones que se promuevan contra el proveedor.
- Los que sometan al consumidor a la competencia de tribunales extranjeros.
- Deberán celebrarse por escrito, en idioma Español y sus caracteres deben ser legibles a simple vista.

Creemos que para nuestro estudio, resulta relevante la fracción VI, toda vez que respecto al idioma utilizado en los contratos de adhesión relacionados con el registro de nombres de dominio, pueden darse dos situaciones: (1) que se registre un nombre de dominio .mx; o (2) que se registre un nombre de dominio de cualquier otra CCTLD,

siendo el más usual los GTLD, es decir, .com, .net, .org, entre otros. En el primero de los casos se trataría de un contrato celebrado en idioma Español, mientras que en el segundo caso, se trataría casi siempre de contratos en otro idioma, principalmente Inglés, lo cual es de suyo importante ya que pudiera afectar la validez del contrato y consecuentemente, la validez de la cláusula arbitral.

Las consecuencias de la nulidad prescrita por la LPC son particularmente enérgicas. En efecto, la regla general del derecho mexicano es que los actos nulos siempre producirán provisionalmente sus efectos, mientras no se decrete la nulidad por la autoridad judicial. Pero esa regla no se aplica cuando se trata de cláusulas cuya nulidad prevé el Artículo 90 de la LPC, sino que se tienen por no escritas. Es decir, su nulidad no necesita ser declarada por la autoridad judicial.

También resulta relevante la fracción VII del Artículo 90 de la LPC, ya que la misma invalidaría, una cláusula que sometiera a la competencia de un tribunal extranjero a quien registre un nombre de dominio. Sin embargo, coincidimos con Javier Arce Gargollo en el sentido de que "no es claro que esta disposición comprenda la cláusula de arbitraje, aunque parece que no cabe otra cláusula de arbitraje que no sea el regulado por la LPC..." Por lo que también coincidimos que "una cláusula que estipulara un arbitraje diferente llevaría el riesgo de ser considerada como una forma de someterse al consumidor al cumplimiento de ciertas formalidades para el ejercicio de sus acciones", pero solo cuando el arbitraje sea el único medio de defensa permitido por el contrato de adhesión, y en el caso de los contratos de registro de nombres de dominio, el procedimiento arbitral no excluye la posibilidad de recurrir a los procedimientos jurisdiccionales.

CAPÍTULO III

3. De los delitos informáticos

El autor mexicano Julio Téllez Valdez; señala que los delitos informáticos son: "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)." [24]

Por su parte, el tratadista penal italiano Carlos Sarzana; sostiene que los delitos informáticos son: "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo." [25]

De conformidad con lo anterior, se puede determinar que los delitos informáticos, en general, son aquéllos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible -o el considerablemente más efectivo-, y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos y cuyas conductas ilícitas se encuentren previamente establecidas en el país en donde se produjo la afectación o el daño.

En términos generales, entonces, se debe comprender que estos delitos se cometen utilizando los medios tecnológicos o son el método o medio comisivo, o el fin de la conducta delictiva.

[24] Téllez Valdéz, Julio. **Los delitos informáticos**. Pág. 246.
[25] **Ibid.** Pág. 246.

Por lo anterior, es comprensible que los delitos informáticos se manifiesten en dos sentidos: como delitos de resultado y como delitos de medio. En el primer caso, porque las conductas que vulneran los sistemas que utilizan tecnologías de información, lesionan el bien jurídico constituido por la información que los sistemas contienen, procesan, resguardan y transmiten, puesto que la información no es más que el bien que subyace en ellos.

En el segundo caso, porque recoge las conductas que se valen del uso de las tecnologías de información para atentar contra bienes jurídicos distintos de la información contenida y tratada en sistemas automatizados, ésto es, bienes como la propiedad, la privacidad de las personas o el orden económico. Lo que distingue a este grupo de delitos informáticos es la utilización de las tecnologías de información como único medio de comisión posible -o como medio extremadamente ventajoso en relación con cualquier otro- para vulnerar el bien jurídico objeto de protección penal.

Según el autor al cual se referirá en este trabajo, que ha sido uno de los máximos exponentes en esta materia, Téllez Valdez, este tipo de acciones presentan las siguientes características principales:

- 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) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- 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.
- Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquéllos que las realizan.

- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto, por su mismo carácter técnico.
- En su mayoría son imprudencia les y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- 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.

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

a) Como instrumento o medio

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, 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.

b) Como un fin u objetivo: este tipo de delitos, esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- 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.).

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones. Por otro lado, la red internet permite dar soporte para la comisión de otro tipo de delitos como:
- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

3.1. Sujetos activos y pasivos de los delitos informáticos

"Las personas que cometen los "delitos informáticos" son aquéllas que poseen ciertas características que no presentan el denominador común de los delincuentes, ésto es,

los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como “delitos de cuello blanco”, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las “violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros”.

Asimismo, este criminólogo estadounidense dice que tanto la definición de los “delitos informáticos” como la de los “delitos de cuello blanco” no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.”[26]

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos “respetables” otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en

[26] Repolles. **Ob. Cit.** Pág. 235.

consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos, a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

En lo que se refiere a delitos informáticos, Olivier Hance:"considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a. Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.
b. Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).
c. Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos

Informáticos; señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a. Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
a. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
b. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
c. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
d. Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
e. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional." [27]

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la inter conexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países como la Argentina, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país,

[27] **Ibid.** Pág. 236.

como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Ahora bien, el sujeto pasivo en el caso de los delitos informáticos, puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

3.2. Los delitos informáticos en la legislación penal guatemalteca

Antes de señalar los delitos que se regulan en el Código Penal respecto al uso del internet o medios informáticos, es importante describir algunas figuras delictivas que a juicio de quien escribe, se circunscriben no necesariamente a la figura típica tal como se regula, sino que éstas se pueden cometer a través del uso de las computadoras y por ende del internet, sin qué en el Código Penal se encuentren reguladas como tal, siendo que a la fecha, podría ser que los jueces, que son quienes juzgan y sancionan, se encuentren en dificultades principalmente porque son figuras delictivas atípicas y porque los medios de prueba también son sui géneris que no sólo se debe tener conocimiento de la ley sino de cómo funciona el internet, a lo cual, podría ser que no todos los jueces se encuentren preparados para ello, tomando en cuenta que

recientemente se encuentra funcionando estas formas o redes de comunicación.

Dentro de las figuras delictivas que no solamente se cometen tal como lo regulan las normas, pueden hacerse a través del uso del internet y que no se regulan, se encuentran entre las más importantes, las siguientes:

La coacción y amenazas.

Artículo 214. Quien, sin estar legítimamente autorizado mediante procedimiento violento, intimidatorio o que en cualquier forma compela a otro, obligue a éste para que haga o deje de hacer lo que la ley no le prohíbe, efectúe o consienta lo que no quiere o que tolere que otra persona lo haga, sea justo o no, será sancionado con prisión de seis meses a dos años.

Amenazas.

Artículo 215. Quien amenazare a otro con causar el mismo o a sus parientes, dentro de los grados de ley, en su persona, honra o propiedad, un mal que constituya o no delito, será sancionado con prisión de seis meses a tres años.

Coacción contra la libertad política.

Artículo 216. Quien fuera de los casos previstos en las leyes especiales respectivas, por medio de violencia o amenazas impidiere o coartare el ejercicio de cualquier derecho político, será sancionado con prisión de seis meses a tres años.

De conformidad con las normas anteriores, resulta evidente de que por medio de los correos electrónicos, por medio de las comunicaciones como se les denomina Chat, se pueden realizar estos actos que deben estar prohibidos por la ley y que en caso se cometan se deben aplicar las figuras genéricas como las que se describen, pero que no es lo ideal, y que en este caso, la justicia podría estar desequilibrada al respecto en perjuicio de la sociedad.

3.3. De la violación y revelación de secretos.

Violación de correspondencia y papeles privados.

Artículo 217. Quién, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónico o de otra naturaleza, que no le estén dirigidos a quién, sin abrirlos, se impusiere de su contenido, será sancionado con multa de cien a un mil quetzales.

Sustracción, desvío o supresión de correspondencia.

Artículo 218. Quién, indebidamente, se apoderare de correspondencia, pliego o despachos, a que se refiere el artículo anterior o de otro papel privado, aunque no estén cerrados o quien los suprimiere o desviare de su destino, será sancionado con multa de cien a un mil quetzales.

Intercepción y reproducción de comunicaciones.

Artículo 219. Quién, valiéndose de medios fraudulentos interceptare, copiare o grabare comunicaciones televisadas, radiales, telegráficas, telefónicas u otras semejantes o de igual naturaleza, o las impida o interrumpa, será sancionado con multa de cien a un mil quetzales.

Agravación especifica.

Artículo 220. Las sanciones señaladas para los hechos delictuosos definidos en los tres artículos que preceden, serán de prisión de seis meses a tres años, en los siguientes casos: 1o. Si el autor se aprovechare de su calidad de funcionario o empleado de la dependencia, empresa o entidad respectivas. 2o. Si se tratare de asuntos oficiales. 3o. Si la información obtenida, el autor la hiciere pública, por cualquier medio.

Publicidad indebida.

Artículo 222. Quién, hallándose legítimamente en posesión de correspondencia, de papeles o de grabaciones, fotografías no destinadas a la publicidad, los hiciere públicos, sin la debida autorización, aunque le hubieren sido dirigidos, cuando el hecho cause o pudiere causar perjuicio, será sancionado con multa de doscientos a dos mil quetzales.

Revelación de secreto profesional.

Artículo 223. Quién, sin justa causa, revelare o empleare en provecho propio o ajeno un secreto del que se ha enterado por razón de su estado, oficio, empleo, profesión o arte, sin que con ello ocasionare o pudiere ocasionar perjuicio, será sancionado con prisión de seis meses a dos años o multa de cien a un mil quetzales.

Usurpación de estado civil.

Artículo 241. Quién, usurpare el estado civil de otro, será sancionado con prisión de dos a cinco años.

Cualquiera de las figuras delictivas preestablecidas en el Código Penal que se han señalado pueden ser cometidas a través del uso del internet y ocasionar un grave perjuicio al sujeto pasivo. Adicionalmente, en estos casos se atenta contra el estado civil de las personas y su derecho a la intimidad.

3.4. De los delitos contra el patrimonio.

Hurto.

Artículo 246. Quien tomare, sin la debida autorización, cosa, mueble, total o parcialmente ajena, será sancionado con prisión de 1 a 6 años.

Hurto agravado.

Artículo 247. Es hurto agravado: 1o. El cometido por doméstico o interviniendo grave abuso de confianza. 2o. Cuando fuere cometido aprovechándose de calamidad pública o privada, o de peligro común. 3o. Cuando se cometiere en el interior de casa, habitación o morada o para ejecutarlo el agente se quedare subrepticiamente en edificio o lugar destinado a habitación. Esta circunstancia agravante no se aplicará cuando el hurto concursare con el de allanamiento de morada. 4o. Cuando se cometiere usando ganzúa, llave falsa u otro instrumento semejante o llave verdadera que hubiere sido sustraída, hallado o retenida. 5o. Cuando participaren en su comisión dos o más personas; una o varias fingiéndose autoridad o jefes o empleados de un servicio público. 6o. Cuando el hurto fuere de objetos o dinero de viajeros y se realizare en cualquier clase de vehículos o en estaciones, muelles, hoteles, pensiones o casas de huéspedes. 7o. Cuando fuere de cosas religiosas o militares, de valor científico, artístico o histórico o destinadas al uso u ornato públicos. 8o. Si el hurto fuere de armas de fuego. 9o. Si el hurto fuere de ganado. 10. Cuando los bienes hurtados fueren productos separados del suelo, máquinas, accesorios o instrumentos de trabajo, dejados en el campo, o de alambre u otros elementos de los cercos. 11. Cuando el hurto fuere de vehículos dejados en la vía pública o en lugares de acceso público. Si los vehículos hurtados fueren llevados y aceptados en predios, talleres, estacionamientos o lugares de venta de repuestos, con destino a su venta, realización o desarme, serán solidariamente responsables con los autores del hurto, los propietarios de los negocios antes mencionados, sus gerentes, administradores o representantes legales, quienes en todo caso, están obligados a verificar la legítima procedencia de los vehículos

recibidos para su comercialización. Al responsable de hurto agravado se le sancionará con prisión de 2 a 10 años.

Hurto de uso.

Artículo 248. Quién, sin la debida autorización, tomare una cosa mueble, total o parcialmente ajena, con el solo propósito de usarla y efectuare su restitución en circunstancias que claramente lo indiquen o se dedujere de la naturaleza del hecho, dejare la cosa en condiciones y lugar que permitan su fácil y pronta recuperación, será sancionado con multa de doscientos a tres mil quetzales, sin perjuicio de las responsabilidades resultantes de los daños causados a la cosa. Cuando el hurto de uso se cometiere para efectuar plagio o secuestro o con fines o propósitos subversivos, se impondrá al responsable prisión de dos a cinco años, sin perjuicio de las sanciones que correspondan al otro delito.

Hurto de fluidos.

Artículo 249. Quién, ilícitamente, sustrajere energía eléctrica, agua, gas, fuerza de una instalación o cualquier otro fluido ajeno, será sancionado con multas de doscientos a tres mil quetzales.

3.5. Robo.

Artículo 251. Quién sin la debida autorización y con violencia anterior, simultánea o posterior a la aprehensión, tomare cosa mueble, total o parcialmente ajena, será sancionado con prisión de 3 a 12 años.

Robo agravado.

Artículo 252. Es robo agravado: 1o. Cuando se cometiere en despoblado o en cuadrilla

2o. Cuando se empleare violencia, en cualquier forma, para entrar al lugar del hecho. 3o. Si los delincuentes llevaren armas o narcóticos, aun cuando no hicieren uso de ellos. 4o. Si los efectuaren con simulación de autoridad o usando disfraz. 5o. Si se cometiere contra oficina bancaria, recaudatoria, industrial, comercial o mercantil u otra en que se conserven caudales o cuando la violencia se ejerciere sobre sus custodios. 6o. Cuando el delito se cometiere asaltando ferrocarril, buque, nave, aeronave, automóvil u otro vehículo. 7o. Cuando concurriere alguna de las circunstancias contenidas en los incisos 1o., 2o., 3o., 6o., 7o., 8o., 9o., 10 y 11 del Artículo 247 de este Código. El responsable de robo agravado será sancionado con prisión de 6 a 15 años.

Robo de uso.

Artículo 253. Cuando el hecho a que se refiere el Artículo 248 de este Código, se cometiere con violencia, será calificado como robo de uso y sancionado con prisión de seis a dos años. Cuando concurrieren las circunstancias a que se refiere el párrafo último del artículo citado, la pena a imponer será de tres a ocho años de prisión.

Robo de fluidos.

Artículos 254. Cuando los hechos a que se refiere el Artículo 249 de este Código, se cometieren con violencia, serán calificados como robo y sancionados con prisión de seis meses a dos años.

Robo impropio.

Artículos 255. Cuando el hecho a que se refiere el Artículo 250 de este Código, se cometiere con violencia, será calificado como robo impropio y sancionado con prisión de seis meses a dos años.

Es frecuente suponer que entre las figuras del hurto y del robo, en donde la diferencia surge de la violencia ejercida o no, puede que se cometa a través del uso del internet y

de las computadoras, por cuanto, en forma solapada en perjuicio del comprador, por ejemplo, en el caso de las transacciones mercantiles o comerciales que se generan a través del internet, que este sea objeto de robo de un bien mueble, como puede ser su dinero, pero también, puede referirse a otros bienes.

En el caso del robo, también se puede circunscribir dentro del ámbito de la utilización de las computadoras, el correo, el internet, por cuanto la violencia no solo puede ser física, sino también, existe violencia psicológica, patrimonial, y que se puede fácilmente cometer a través del uso del internet.

3.6. De la extorsión y el chantaje

Extorsión.

Artículo 261. Quién, para procurar un lucro injusto o para defraudarlo obligare a otro, con violencia, 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 uno a seis años.

Chantaje.

Artículo 262. Comete delito de chantaje quien exigiere a otro, dinero, recompensa o efectos, bajo amenaza directa o encubierta de imputaciones contra su honor o prestigio, o de violación o divulgación de secretos, en perjuicio del mismo, de su familia o de la entidad en cuya gestión intervenga o tenga interés. El responsable de este delito será sancionado con prisión de tres a ocho años.

En el caso de la extorsión o el chantaje, en el medio guatemalteco, es muy común que se cometa a través de manuscritos que van dirigidos a las personas a quienes se pretende extorsionar o chantajear, sin embargo, es evidente de que resulta muy fácil

para el que opera una computadora, que a través de un monitor, se dirija al sujeto pasivo, y le infiera una serie de amenazas con efecto de chantajearlo para que haga o realice algo que no quiere y que a todas luces es ilegal, y que se puedan suscitar este tipo de delitos.

Se entrevistó de manera particular a algunos jueces, respecto a estos temas, e indicaron que respecto a la extorsión o el chantaje, este se realiza de forma tradicional, es decir, que en su experiencia no han tenido la oportunidad de conocer algún caso de éstos que se produzcan por vía de internet y uso de las computadoras, pero que no se estará muy lejos de que eso suceda, tomando en cuenta la facilidad que ofrece la utilización de estos medios para conseguir determinados propósitos de los delincuentes.

3.7. De la estafa

Estafa propia.

Artículo 263. Comete estafa, quién, induciendo a error a otro, mediante ardid o engaño lo defraudare en su patrimonio en perjuicio propio o ajeno. El responsable de este delito será sancionado con prisión de seis meses a cuatro años y multa de doscientos a diez mil quetzales.

Casos especiales de estafa.

Artículo 264. Incurrirá en las sanciones señaladas en el artículo anterior: 1o. Quién, defraudare a otro usando nombre fingido, atribuyéndose poder, influencia, relaciones o cualidades supuestas, aparentando bienes, comisión, empresa o negociaciones imaginarias. 2o. El platero o joyero que alterare en su calidad, ley o peso, los objetos relativos a su arte o comercio, o traficare con ellos. 3o. Los traficantes que defraudaren, usando pesas o medidas falsas, en el despacho de los objetos de su tráfico. 4o. Quien defraudare a otro con supuesta remuneración, a funcionarios, autoridades, agentes de

ésta o empleados públicos, o como recompensa de su mediación para obtener una resolución favorable en un asunto que de los mismos dependa, sin perjuicio de las acciones de calumnia que a éstos corresponda.

5o. Quién cometiere alguna defraudación, abusando de firma de otro, en blanco o extendiendo con ella algún documento en perjuicio del mismo o de un tercero. 6o. Quién defraudare a otro haciéndole suscribir, con engaño algún documento. 7o. Quién se valiere de fraude para asegurar la suerte en juegos de azar. 8o. Quién cometiere defraudación sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, documento u otro escrito. 9o. Quién, fingiéndose dueño de una cosa inmueble, la enajenare, gravare o dispusiere de ella, en cualquier otra forma. 10. Quien dispusiere de un bien como libre, sabiendo que estaba gravado o sujeto a otra clase de limitaciones y quien, con su enajenación o gravamen, impidiere, con ánimo de lucro, el ejercicio de tales derechos.

11. Quién enajena separadamente una cosa a dos o más personas, con perjuicio de cualquiera de ellas o de tercero. 12. Quién otorgare, en perjuicio de otro, un contrato simulado. 13. Quien, a sabiendas, adquiere o recibiere, en cualquier forma, bienes de quién no fuere su dueño o no tuviere derecho para disponer de ellos. 14. Quien, con perjuicio de otro, ejerciere un derecho de cualquier naturaleza a sabiendas de que ha sido privado del mismo por resolución judicial firme. 15. Quién destruyere o deteriorare, total o parcialmente bienes que le pertenezcan, afectos a derechos de un tercero, con el propósito de defraudar a éste. 16. Quién comprare a plazos un bien y lo enajenare posteriormente o dispusiere de él, en cualquier forma, sin haber pagado la totalidad del precio.

17. Quién negare su firma en cualquier documento de obligación o descargo. 18. Quién, con datos falsos u ocultando antecedentes que le son conocidos, celebrare dolosamente, contratos basados en dichos datos o antecedentes. 19. Quién, sin autorización o haciendo uso indebido de ésta mediante colectas o recaudaciones,

defraudare a otros. Si la recaudación o colecta se hace sin autorización y sin propósito de defraudar, o estando autorizada no se cumple con los requisitos legales correspondientes, la sanción será de multa de veinte a doscientos quetzales. 20. Quién cobrare sueldos no devengados, servicios o suministros no efectuados. 21. Quién defraudare valiéndose de la inexperiencia, falta de discernimiento o pasiones de un menor o incapacitado. 22. El deudor que dispusiere, en cualquier forma, de los frutos gravados con prenda para garantizar créditos destinados a la producción. 23. Quién defraudare o perjudicare a otro, usando de cualquier ardid o engaño, que no se haya expresado en los incisos anteriores.

Estafa mediante destrucción de cosa propia.

Artículo 265. Quién, para obtener el pago de un seguro o algún provecho indebido en perjuicio de otro, destruyere, deteriorare u ocultare, total o parcialmente, un bien propio, será sancionado con prisión de uno a tres años y multa de cien a cinco mil quetzales.

Estafa en la entrega de bienes.

Artículo 267. Quién defraudare en la substancia, calidad o cantidad de los bienes que entregue a otros, en virtud de contrato o de cualquier otro título obligatorio, será sancionado con prisión de seis meses a cinco años y multa de cien a cinco mil quetzales.

Estafa mediante informaciones contables.

Artículo 271. Los auditores, contadores, expertos, directores, gerentes, liquidadores o empleados de entidad bancaria o mercantil, sociedades o cooperativas, que en sus dictámenes o comunicaciones al público, o en sus informes, memorias o proposiciones, o en la formación de los inventarios o balances, consignaren, con ánimo de defraudar, atraer inversiones o de aparentar una situación económica que no tiene, hechos contrarios a la verdad, incompletos o simulados, serán sancionados con prisión de seis meses a cinco años y multa de cien a cinco mil quetzales.

Como se observa existe una serie de supuestos por los cuales se puede cometer el delito de estafa y algo fundamental es lo que se regula en forma abierta, cuando se señala que cualquier otra forma de estafa que no hubiera sido establecida en la ley, a pesar de que representa una analogía que aplicaría el juez en el momento oportuno, y que podría ser ilegal, la legislación penal lo regula, tal como se observa, y por lo tanto, podría estar permitido, sin embargo, no se ha hecho por parte del legislador una distinción de estas formas tradicionales de comisión de éstos delitos, pero con el uso del internet y las modalidades que deben regularse para que constituyan herramientas útiles para los jueces y se haga justicia en beneficio de la misma sociedad.

3.8. De las apropiaciones indebidas

Apropiación y retención indebidas

Artículo 272. Quién, en perjuicio de otro, se apropiare o distrajere dinero, efectos o cualquier otro bien mueble que hubiere recibido en depósito, comisión o administración, o por cualquier otra causa que produzca obligación de entregarlos o devolverlos, será sancionado con prisión de seis meses a cuatro años y multa de cien a tres mil quetzales.

Apropiación irregular

Artículo 273. Comete el delito de apropiación irregular, quien: 1o. Tomare dinero u otro bien mueble que encontrare perdido y no le pertenezca. 2o. Habiendo encontrado un tesoro lo tomare en todo o en parte, o tomare la cuota que, según la ley, corresponda al dueño del inmueble. 3o. Tomare cosa ajena que haya llegado a su poder por error o caso fortuito. Los responsables serán sancionados con prisión de dos meses a dos años y multa de cincuenta a dos mil quetzales.

En estos casos, es importante señalar que podría ser muy frecuente, porque resulta

lógicamente fácil la comisión de este tipo de delitos a través del uso del Internet. Sin embargo, como se observa en los demás delitos y en éstos, las penas son relativamente irrisorias y por lo tanto, podría ofrecer un incentivo para los delincuentes, que sugiere su confianza de que en primer lugar, sería muy difícil sancionarlos por falta de normativa, y en segundo lugar, las penas en comparación con el daño que se produce son irrisorias.

En materia propiamente de los delitos informáticos, al Capítulo VII se adicionaron algunas figuras delictivas en forma muy generalizada como se observarán incluidas dentro de los delitos contra los derechos de autor y propiedad intelectual, sin que puedan tener una relación directa entre éstos y los otros, tal como se observa con el análisis anterior, sin embargo, se han establecido y a continuación se describen las mismas:

3.9. Destrucción de registros informáticos

Artículo 274 "A". Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos.

Alteración de programas.

Artículo 274 "B"... La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

Reproducción de instrucciones o programas de computación.

Artículo 274 "C"... Se impondrá prisión de seis meses a cuatro años y multa de

quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

Registros prohibidos.

Artículo 274 "D". 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.

Manipulación de información.

Artículo 274 "E". 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, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

Uso de información.

Artículo 274 "F"... Se impondrá prisión de seis meses a dos años, y multa de 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.

Programas destructivos.

Artículo 274 "G"... 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.

3.10. Los delitos informáticos en la legislación comparada

Ley especial contra los delitos informáticos en la Republica de Venezuela.

Disposiciones generales:

Artículo 1. Objeto de la ley es la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2. Definiciones a efectos de la presente ley, y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data (datos): hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

d. Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

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

h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así

como de data expresada en cualquier forma, con el objeto de que los computadores realicen funciones específicas.

j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de Datos o de Información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta Inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

ñ. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

Mensaje de Datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3. Extraterritorialidad: cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la república, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4. Sanciones: Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley.

Artículo 5. Responsabilidad de las personas jurídicas cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Tal como se observa, esta ley parece ser más completa comparándolo con lo que sucede en el caso de la legislación penal guatemalteca, que añade al Código Penal algunos ilícitos muy generales en esta materia. Adicionalmente, ofrece un ámbito más abierto respecto a las personas individuales y jurídicas en el uso del Internet y la

afectación que pueda producir a terceros. Algo fundamental de análisis es el hecho de la territorialidad de la ley, en el caso de que se ven atadas las autoridades de este país cuando la persona que comete el delito reside en otro país y que quedará este sujeto a las leyes de ese país, sin embargo, cabría analizar que sucede si la afectación o el perjuicio se produjo en este país, y el sujeto pasivo es de este país, entonces, como queda la protección jurídica a través de las leyes que debe brindar el Estado a la sociedad.

3.11. De los delitos contra los sistemas que utilizan tecnologías de información

Artículo 6. Acceso Indebido: toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7. Sabotaje o daño a sistemas: todo aquél que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quiéndestruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8. Favorable culposo del sabotaje o daño si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las

normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9. Acceso Indebido o Sabotaje a Sistemas Protegidos: Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 10. Posesión de Equipos o Prestación de Servicios de Sabotaje: Quién importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas; con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11. Espionaje Informático: Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12. Falsificación de documentos quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

De conformidad con las normas anteriores, a juicio de quién escribe representa un gran avance en esta materia, por cuánto, no sólo se dirige a los particulares individualmente considerados sino a las redes organizaciones criminales que pudieran circunscribirse en hechos o actos como los que se describen en las figuras delictivas señaladas, y que además, las penas son considerables y las multas de igual manera.

3.12. De los delitos contra la propiedad

Artículo 13. Hurto quién a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial, sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14. Fraude: Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un

provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15. Obtención indebida de bienes o servicios Quién, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos, toda persona que por cualquier medio, crée, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias. En la misma pena incurrirá quién, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos quién se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quiénadquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18. Provisión indebida de bienes o servicios todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quién los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19. Posesión de equipo para falsificaciones todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Tal como se observa, es necesario que en el caso de la legislación guatemalteca, se contemplen casos como el que se plantean a través de la regulación como ilícita los actos en estos delitos que contempla la ley objeto de análisis, en virtud de que figuras tradicionales como la estafa o fraude, o bien el hurto o robo, también se circunscriben a hechos que se cometen a través del internet y que en el caso de la legislación penal guatemalteca no se encuentra regulado aún.

3.13. De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20. Violación de la privacidad de la data o Información de carácter personal toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un

computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. Violación de la privacidad de las comunicaciones, toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. Revelación indebida de data o información de carácter personal quién revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Este tema es muy importante de abordar especialmente porque se refiere a los derechos de la persona de protección a su intimidad, su estado civil, etc., y que podría ser muy frecuente que estos ilícitos se cometan en el caso de la sociedad guatemalteca, a través del uso del internet, la intromisión en los correos, que en la actualidad ya se esta observando, etc.

3.14. De los delitos contra niños, niñas o adolescentes

Artículo 23. Difusión o exhibición de material pornográfico, todo aquel que, por

cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24. Exhibición pornográfica de niños o adolescentes, toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

En el caso muy frecuente que es utilizado por las sociedades es traficar con niños a través del internet y que en el caso de Guatemala, no existe una regulación penal adecuada, tal como se señala en este apartado de la ley objeto de análisis.

Esto también de regularse en el caso de Guatemala, estaría en congruencia con las normas del Derecho Internacional de los Derechos Humanos de los niños.

3.15. De los delitos contra el orden económico

Artículo 25. Apropiación de propiedad intelectual, quién sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26. Oferta engañosa, toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Es frecuente que a través del internet por experiencia propia se publiciten productos, bienes, servicios, y que los usuarios al contratar se den cuenta que no se trataba de cómo se mencionaba en los anuncios, a esto se refiere la publicidad engañosa, entre otros aspectos a considerar dentro de este ilícito, tal como se observa en la norma objeto de análisis. Adicionalmente, se ha dicho que en materia de propiedad intelectual, cuando una obra, un arte, o algún escrito hecho por cualquier persona se coloque en el internet, por la naturaleza de este servicio y redes de comunicación generalizada y mundial, debe pasar a dominio público, sin embargo, para efectos de la sociedad guatemalteca, por ejemplo, y como sucede con la legislación venezolana como se analiza, esto no es posible y por lo tanto, los derechos de autor y propiedad intelectual se deben respetar aunque se trata de que el medio sea el internet o un computador, tal como se observa.

3.16. Disposiciones comunes

Artículo 27. Agravantes la pena correspondiente a los delitos previstos en la presente ley se incrementará entre un tercio y la mitad: Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

Artículo 28. Agravante especial la sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29. Penas accesorias además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes:

1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos 10 y 19 de la presente Ley

2. El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente.

4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de

cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30. Divulgación de la sentencia condenatoria el tribunal podrá además, disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31 Indemnización civil en los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos.

Como se observa respecto a las penas, los agravantes, las penas accesorias y la responsabilidad civil, es importante señalar que a juicio de quiénescribe son muy severas, y por lo tanto, resulta oportuno comparar con lo que sucede en el caso de Guatemala, lo cual dista mucho de equipararse a estas formas de control que tiene el Estado a través de la ley.

Disposiciones finales.

Artículo 32. Vigencia la presente ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Artículo 33. Derogatoria se deroga cualquier disposición que colida con la presente Ley. Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los cuatro días del mes de septiembre de dos mil uno. Año 191º de la Independencia y 142º de la Federación.

3.17. República de Colombia

En el caso de este país, el Congreso Colombiano aprobó la ley que modifica el Código Penal para incorporar los delitos que violen la protección de la información y de los datos. Como lo señala el autor Luis Alcalá;" veintidós años después de que Estados Unidos adoptó el Acta de Fraude y Abuso Computacional, y siete años después de que Europa firmó el Convenio de Cibercriminalidad, Colombia está contando actualmente con una legislación para combatir los delitos informáticos.

La plenaria del Senado de la República de Colombia aprobó la ley que modifica el Código Penal con el fin de crear una nueva serie de delitos en torno a la violación de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Los ajustes realizados a la regulación permitirán que el ordenamiento colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad en el ciberespacio y le brinde herramientas a la comunidad internacional para la persecución de estos flagelos.

Esta ley, establece penas de prisión de 4 a 8 años para los delincuentes informáticos y multas de 100 a 1.000 salarios mínimos mensuales, es decir de 46,1 a 46,5 millones de pesos." [28]

Entre las conductas tipificadas como delito están el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas computacionales o redes de telecomunicaciones, la interceptación de datos informáticos, el uso de software

[28] Maldonado. **Ob. Cit.** Pág. 63.

malicioso, la violación de datos personales y la suplantación de portales de Internet para capturar datos personales, entre otras.

Mientras no existía esta ley, las personas que eran sorprendidas cometiendo este tipo de crímenes debían ser procesadas por delitos genéricos. Dentro de las figuras que se encuentran en estas reformas a la ley penal, se encuentran:

- Acceso abusivo a un sistema informático. Será sancionado quiénsin autorización acceda a un sistema informático protegido o se mantenga dentro del mismo en contra de la voluntad de quiéntenga el legítimo derecho a excluirlo.

- Obstaculización ilegítima de sistema informático o red de telecomunicación. Se penalizará a quiénimpida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

- Interceptación de datos informáticos. Bajo este delito serán castigadas las personas que, sin orden judicial previa, intercepten datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte.

- Daño informático. Se sancionará a quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

- Uso de software malicioso. El proyecto de ley señala que serán castigadas las personas que, sin estar facultadas para ello, produzcan, trafiquen, adquieran,

distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

- Violación de datos personales. Este delito cobijará a quienes, sin estar facultados para ello, con provecho propio o de un tercero, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

- Suplantación de sitios web para capturar datos personales. Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También quiénmodifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. En este caso la pena se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

3.18. Republica de España

Se ha podido tener conocimiento de que los países europeos, han propiciado los cambios necesarios dentro de sus respectivas legislaciones para contrarrestar la problemática de la comisión de ilícitos a través del internet, precisamente, creando en conjunto la convención contra el ciber crimen.

En este país, se cuenta con la Ley Orgánica, número 10/1995, de fecha 23 de Noviembre de 1.995, que en materia de los delitos informáticos se refiere a los

siguientes:

Artículo 197.

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quiénlos altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las

personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198.

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200.

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201.

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211.

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212.

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238.

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1º.- Escalamiento.

2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.

4º.- Uso de llaves falsas.

5º.- Inutilización de sistemas específicos de alarma o guarda.

Artículo 239.

Se considerarán llaves falsas: 1º.- Las ganzúas u otros instrumentos análogos. 2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción. 3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo. A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248.

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255.

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º.- Valiéndose de mecanismos instalados para realizar la defraudación.

2º.- Alterando maliciosamente las indicaciones o aparatos contadores.

3º.- Empleando cualesquiera otros medios clandestinos.

Artículo 256.

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 263.

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264.

1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º.- Que se cause por cualquier medio, infección o contagio de ganado.

3º.- Que se empleen sustancias venenosas o corrosivas.

4º.- Que afecten a bienes de dominio o uso público o comunal.

5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.

6.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270.

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quiénintencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278.

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio

de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400.

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536.

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses

Como se observa en las legislaciones analizadas anteriormente, resulta procedente determinar que a nivel mundial los Estados están preocupados por adoptar en sus legislaciones marcos normativos actualizados y precisamente tendientes a sancionar las conductas ilícitas que se producen a través del uso del internet, y que han pretendido ir mucho más allá en cuanto a sancionar no solo a personas individualmente consideradas, sino también a empresas y entes que se dedican a estos menesteres, y fundamentalmente a atacar el fondo del asunto.

CAPÍTULO IV

4. Los sistemas de control de origen en los delitos cometidos por el uso de Internet en el caso de los metatags y la necesidad de su regulación

Como se ha podido observar, en la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. A la par de ello, evidentemente por las bondades que ofrecen estas herramientas, han sido motivaciones suficientes para los criminales y en este caso, los de alta jerarquía cultural y educativamente hablando, para cometer ilícitos, como los que se han señalado en el transcurso de este trabajo.

Aquí se esta entonces, ante un problema mayor para el Estado, como garantizador del bienestar social y de la protección a los bienes jurídicos ya tutelados en la ley penal y que se cometen frecuentemente, pero utilizando como herramienta no precisamente a través de las formas tradicionales, sino la herramienta el internet y las computadoras.

Es por ello, que aparte de que en este trabajo se hace una descripción de las figuras delictivas consideradas como delitos informáticos, como se ha venido analizando, también es que debe el Estado regular aspectos fundamentales pero desde el punto de vista del quebrantamiento de los sistemas de control de origen en el caso de los delitos que se cometen por el uso del internet y no precisamente, como se regula en el Código Penal, refiriéndose a figuras delictivas generalizadas y tradicionales dejando por un lado, y bajo un estado de impunidad, las que se han señalado y que más adelante se refiere el autor con mayor detalle.

4.1. Los registros

Todos los sistemas, aplicaciones y redes informáticas, y las aplicaciones de correo electrónico poseen capacidades de registración de las sesiones de conexión, que capturan como mínimo, cualquier intento de conexión (con o sin éxito), la identificación de la conexión, la fecha y hora de cada intento de conexión enumerando la identificación (ID) del usuario, los dispositivos utilizados, las funciones realizadas una vez que se conectó, y la aplicación o función que el sospechoso trató de solicitar.

Es por ello, que a través de esta forma puede ejercerse control en los sistemas computarizados e informáticos para el control en la comisión de hechos delictivos.

Respecto a como funcionan estos registros, conviene señalar que estos archivos de acceso son generados por el sistema operativo básico de la red, así como las aplicaciones instaladas en ese sistema operativo. Los reportes de conexiones a la red y los registros de tráfico producen numerosos asientos que detallan la autenticación y la autorización para los servidores de directorio, servidores de bases de datos, servidores de archivo e impresión, rute adores de acceso, cortafuegos, servidores sustitutivos, servidores de correo, y entradas de redes virtuales privadas (VPN). Los sistemas de intrusión-detección (HIDS) con base en servidores host y los sistemas de control de acceso con base en la computadora central son soluciones basadas en software que tienen la capacidad de monitorear, llevar el registro, e informar virtualmente todas las transacciones que ocurren en los sistemas de servidores host de una organización.

En el caso de los metatags entonces, éstos deben estar registrados, cuando no se utilizan con fines delictivos, por cuanto, debe establecerse los aspectos o el marco en que se desarrollen los mensajes que tratan de inducir o dirigir al operador del Internet desde su posición hacia determinada publicidad, pero que ésta no sea con motivo de eliminar o cometer competencia desleal respecto de una empresa o un servicio o bien.

Entonces, a pesar de que deben permitirse, el hecho de que se utilice para otros fines, es en donde debe intervenir el Estado, especialmente en el registro de los mismos.

Todo lo anterior, desde actividades de conexión completadas satisfactoriamente hasta intentos fracasados de conexión, pasando por una lista de archivos agregados, modificados o eliminados, puede ser fácilmente rastreado por los HIDS, los cuales proporcionan un registro de auditoría detallado de las acciones de una persona. De la misma manera como los HIDS pueden rastrear a los usuarios que ingresan a las computadoras host del hogar, centro de trabajo, o inmueble, sin embargo, a nivel de organizaciones, en la mayoría éstas disponen de algún tipo de sistema intrusión-detección con base en la red (NIDS) para rastrear actividades a través de la red.

Este NIDS reside generalmente en el segmento interno de los cortafuegos para monitorear y proporcionar reportes de todo el tráfico hacia y desde la Internet. Mientras el tráfico de los usuarios atraviesa la red, la información en pequeños paquetes es reunida, lo que permite que los reportes de conexión NIDS identifiquen a los usuarios por su ID de usuario; la dirección del protocolo de Internet (IP), de ser aplicable; el nombre del servidor host visitado; el identificador de aplicación; y la hora de inicio, duración y salida de sesión del usuario. Se puede capturar la información de conexión NIDS para todos los sucesos de la red que impliquen el acceso a los servidores corporativos de intranet y de correo electrónico, y de la actividad en la red que está destinada a la Internet o se origina de ella.

En virtud de lo anterior, resulta oportuno entonces, no sólo que en el caso del ente persecutor de los crímenes, como es el Ministerio Público, se encuentre dotado de personal capacitado para ello, es menester decomisar el computador que fue objeto de uso, para que a través de la práctica forense científica se pueda determinar todos los aspectos de interés para determinar como se produjo el ilícito.

Además, los rastros de verificación de los cortafuegos pueden ser particularmente útiles para el investigador al considerar los fraudes a gran escala que impliquen el acceso vía la Internet. Los cortafuegos generan un archivo de registro que contiene un sello con la hora y un identificador único de tiempo transcurrido de la conexión; un número único de identificación de la sesión; las direcciones de la fuente y del destinatario IP, incluyendo la dirección de la conexión y un identificador de la ubicación del rute ador de origen, y un código único de identificación del proveedor del servicio de Internet (ISP), incluyendo el identificador de cuenta del usuario. Al capturar el código de identificador del ISP del infractor, así como la información sobre la dirección del ISP infractor y el número telefónico de origen del ISP, el investigador puede presentar evidencia convincente al fiscal, juez y mejorar enormemente las posibilidades de un proceso exitoso.

Un método común para intentar frustrar el monitoreo y restricción de uso en el acceso a una red ocurre cuando intrusos externos o internos tratan de evadir el cortafuegos o el servidor sustitutivo empleando el acceso mediante el marcado telefónico a través de líneas conectadas a un puerto de red abierto. Para contrarrestar ésto, ahora muchas organizaciones ponen en funcionamiento sistemas de escaneo de puertos externos, los que identifican todos los puertos abiertos y permiten cerrar los puertos que no estén en uso. Los sistemas de escaneo de puertos también pueden tener un uso especial en las investigaciones porque proporcionan un reporte de las sesiones de conexión que muestra la ubicación del puerto de todas las transacciones en la red.

Se puede configurar el registro de un cortafuego en cualquier dispositivo que está diseñado para capturar el acceso a un sistema, incluyendo un servidor o un rute ador de cortafuegos y cualquier aparato separado de la red que contenga software de cortafuegos. Independientemente del tipo de cortafuegos que se usa, el programa sirve como un punto único de ingreso a la red y evalúa todos los pedidos de conexión.

Debido a que los cortafuegos utilizan un conjunto predefinido de reglas en las cuales se basan las excepciones y alertas, la actividad fraudulenta puede ser capturada con facilidad.

Los registros con rastros de verificación identifican sucesos tales como intentos múltiples de acceso no autorizado en un período de tiempo dado, fallas repetidas de conexión, actividad en los puertos de la red no utilizados, y potenciales ataques para negar el servicio, se hace necesario y fundamental en el caso del uso de los mensajes denominados metatags.

4.2. Ausencia de regulación

En términos generales, tradicionalmente, el desarrollo de Internet ha disfrutado de una total ausencia de regulación, siendo considerado como el máximo exponente de la libertad de expresión y difusión de ideas en un mundo globalizado. Si al factor de libertad de oferta de contenidos le añadimos el acceso gratuito a los mismos obtenemos un resultado que se ha plasmado en la extensión de este entorno a millones de hogares en el mundo, acuñándose el concepto de la Sociedad de la Información para definir este fenómeno. Dicha ausencia de regulación no está exenta de riesgos, ya que, como sucede con todos los inventos humanos, su uso puede desviarse de las finalidades originales hasta desvirtuar sus resultados más beneficiosos, tal como se ha experimentado en la realidad.

En efecto, Internet puede ser utilizado como un medio idóneo para la comisión de delitos e ilícitos que pueden quedar impunes al amparo del elemento internacional inherente a su esencia, al estar en presencia de varias jurisdicciones nacionales que pueden ofrecer soluciones diversas o por las propias dificultades de investigación que plantea su entorno. Esto se agrava aún más con la situación que ostenta Guatemala, ante las pocas normas relacionadas al tema que existen y que no ofrecen discusión y

solución especialmente para el ente investigador y fundamentalmente para los jueces, que a pesar de que se tiene conocimiento que no son muy frecuentes en los tribunales de sentencia, el juzgamiento de esta forma de ilícitos, aún, es posible que en un futuro muy cercano eso sea diferente.

Otro elemento que está favoreciendo la necesidad de regular la WEB es el deseo de potenciar el comercio electrónico, que requiere garantizar unas condiciones de seguridad jurídica en el tráfico que favorezcan la confianza de las empresas y de los consumidores. Son evidentes las beneficios que aporta Internet al comercio, tanto por el factor publicitario que incorpora, multiplicando el público objetivo al que se destina de forma prácticamente ilimitada – con las lógicas limitaciones del medio y del transporte físico de ciertas mercancías -, como por las facilidades de transacción en tiempo real propias de su entorno.

Esto no podría ser diferente en el caso de los mensajes publicitarios que a través de la web se dirigen a los usuarios que se denominan metatags, por lo que en el caso de Guatemala, se propone una regulación especifica dentro de los delitos informáticos en el Código Penal.

4.3. Las restricciones de acceso

Ahora bien, pudiera ser que la clave para evitar una serie de abusos que se constituyen posteriormente en ilícitos que provocan perjuicios al sujeto pasivo con la utilización de la web, correos electrónicos, realizar el comercio electrónico, asuntos del estado civil, etc., es que se manejen determinadas restricciones de acceso habilitadas claro esta, únicamente para quién efectivamente tenga interés en el asunto, y bajo su responsabilidad.

En ese sentido, ciertas restricciones están destinadas a compensar otros derechos legítimos o intereses públicos en presencia, como son el orden público, la seguridad pública y la defensa nacional, la dignidad de la persona y el principio de no discriminación por razón de raza, sexo o religión, la protección de la infancia y la juventud, o la protección de los datos personales. No podía ser de otro modo. Se debe buscar entonces, un lógico equilibrio entre la libertad de expresión y de prestación de servicios y la defensa de otros derechos fundamentales o de orden público.

Las restricciones de acceso, pueden suscitarse de dos formas: una que el propio usuario las realice desde su computadora, con claves de seguridad, y por otro lado, cuando los que proporcionan los servicios también desde esa fuente, se determinen, sin embargo, es una realidad que eso no puede ser controlado totalmente, y es axial que en el caso de los metatags ha habido prácticamente una intromisión en la actividad de navegación por la web y el Internet que realiza el usuario que no se puede evitar, o por lo menos resulta muy difícil, es por ello, que mediante mensajes subliminales de determinados productos o bienes o bien servicios, se induce al usuario a seleccionar determinado bien o servicio, en detrimento de la posibilidad que tiene de conocer otros, o bien en detrimento de otras empresas que también prestan estos servicios y que si cumplen con las formas establecidas de introducción en el sistema de la web para dar a conocer sus bienes o servicios, y que eso precisamente constituye parte de la competencia desleal que debe ser considerada como ilícita, y como consecuencia se debiera regular en el caso de Guatemala, en el Código Penal.

4.4. Los prestadores de los servicios de Internet y su responsabilidad

También juegan un papel importante las personas directas que prestan los servicios deinternet, por lo que se deben regular las obligaciones a las que se someten los prestadores de servicios en sus relaciones con los destinatarios, entre las que cabe destacar ciertas obligaciones de información previa tanto a los destinatarios como a las autoridades competentes en relación con el nombre o denominación social, domicilio,

dirección de correo electrónico, datos del Registro Mercantil, datos de posibles autorizaciones relacionadas con su actividad o datos profesionales, número de identificación fiscal e información clara y exacta sobre precios de los productos que comercializa.

En ningún caso se debe interpretar estas obligaciones como un atentado contra el principio de libre prestación de servicios, sino una mera consecuencia de la necesidad de garantizar la seguridad jurídica del comercio electrónico. En efecto, la impunidad que permitiría la ocultación de la identidad, muy fácil en un medio como el de Internet, y la posición de indefensión en la que se situaría a los destinatarios de la información y los servicios frente a los abusos, hacen necesaria la identificación de los proveedores de servicios y su sujeción a determinadas normas de conducta.

En el marco normativo se debe establecer la obligación de los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso de redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos, de retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período de tiempo determinado, por ejemplo, seis meses, en los términos establecidos que reglamentariamente se establezcan.

No cabe duda que la carga que se establece para dichos agentes no es perjudicial, ya que dicha obligación requerirá además de una gran capacidad de almacenamiento, para someter este proceso a la regulación de protección de datos y de medidas de seguridad de ficheros electrónicos con el fin de impedir accesos no autorizados.

Evidentemente, todo ello supone un enorme costo para los actores del mercado, que puede llegar incluso a provocar la desaparición de aquéllas empresas que no estén preparadas técnica o económicamente para adaptarse a estas nuevas reglas del juego,

sin embargo, el brindar mayor seguridad para quienes se encuentran en el juego es superior y por lo tanto, ofrecería mejores garantías no solo del servicio, sino también de protección en el caso del Estado.

Uno de los aspectos importantes de regular esta forma o obligaciones en el caso de los prestadores de los servicios de internet es el tratamiento de la responsabilidad de los prestadores de servicios, precisamente por los contenidos ilícitos que transmiten o alojan en sus servidores, estableciéndose el principio general de ausencia de responsabilidad cuando no se manipule la información transmitida. Sin que exista una obligación genérica de supervisión de dichos contenidos.

En el caso de las comunicaciones comerciales, o el comercio electrónico, respecto a los spam que son mensajes que se interceptan en las comunicaciones, debe el Estado inclinarse por una regulación protectora del receptor de los mensajes que no provoquen perjuicio o bien otros intereses creados por parte de organizaciones criminales. La solución de ésto consiste en exigir la identificación del transmisor del mensaje y que éste incluya la palabra publicidad con objeto de permitir a su destinatario la opción de descartar su lectura, por ejemplo, o bien la utilización de la firma electrónica o la clave digital.

Por otro lado, en el caso del comercio electrónico, por ejemplo, se debe prohibir taxativamente el uso del correo electrónico para mensajes publicitarios cuando no hayan sido expresa y previamente requeridos.

Es por eso la importancia de que a través de éstos se pueda tener un punto de partida para regular los mensajes o los metatags que se producen en forma indebida y aparecen en la web en la navegación que realizan miles y miles e usuarios de Internet y que con ello, prácticamente se están cometiendo hechos que debieran ser prohibidos.

4.5. La creación de la figura tercero de confianza en las transacciones vía Internet

Algo novedoso que se ha podido observar en el campo de los delitos electrónicos o como se denomina en la legislación guatemalteca, delitos informáticos, es el denominado tercero de confianza. Éste puede intervenir en la celebración de los contratos electrónicos para dar fe de las declaraciones de voluntad de las partes contratantes y de la fecha y la hora en que se realizan. En la legislación comparada, se pudo corroborar que esta figura no tiene nada que ver con la intervención de los Notarios o funcionarios habilitados para dar fe pública, a los que no pretenden sustituir, sino que su intervención se produce por deseo de las partes para garantizar el procedimiento de contratación y evitar la paradoja del envío de acuses de recibo entre las partes previniendo algún acto de corrupción, delincuencial o fraude.

El acuse de recibo de la aceptación de la oferta constituye una de las obligaciones del prestador de servicios de red, también, debe ser regulado como una obligación que diera hacerse por medio de correo electrónico o por medio equivalente utilizado para realizar la oferta. Además, el prestador de servicios debe tener otra serie de obligaciones previas o posteriores a la celebración del contrato como son las de información sobre los términos, y soporte de los contratos, así como en el caso de contratos sometidos a condiciones generales de contratación ponerlas a disposición del destinatario y facilitar su almacenamiento y reproducción.

4.6. La necesidad de que se regule en el Código Penal los sistemas de control de seguridad en el origen de los delitos cometidos por el uso del internet por medio de los metatags

Como se ha venido desarrollando en la presente investigación, el análisis de la problemática que se ocasiona con el uso del Internet y los computadores en la comisión de hechos delictivos. Como sucede en cualquier ámbito de la vida, los delincuentes, a

todo nivel buscan las formas de poder agenciarse de dinero a través del fraude, estafa, robo, hurto, amenazas, etc., y que a través de estos medios resulta ser muy fácil para ellos, entonces, la contrapartida sería que el Estado interviniera en la protección de los usuarios de estas redes o sistemas computarizados a través de una legislación que responda efectivamente a estos intereses.

De por si ya existe el problema de la territorialidad de la ley en el caso de que el problema surja entre Estados y de aquí surge entonces, la necesidad de los denominados acuerdos nacionales, bilaterales, multilaterales entre los países, en respuesta a la preocupación de la Organización de las Naciones Unidas, por contrarrestar esta problemática.

Todos los países sin discriminación, en forma equilibrada y transparente, cada uno actuando en su territorio debe apoyar a los ciudadanos de **Internet** que circunstancialmente moran en él, a través de regular los sistemas de control de origen en el caso de la posibilidad de que se cometan ilícitos previamente regulados y señalados en la ley penal.

Tomando en cuenta que el internet es una cosa, que se ingresa a través de una máquina (computadora) y por lo tanto, transporta mensajes, nadie es dueño de ello, todos pueden utilizarlo, y todos pueden tratar de mejorarlo, el asunto estriba entonces, en los mecanismos de seguridad contra violaciones a derechos fundamentales.

Como se ha dicho, el Internet; "es la red nerviosa que vincula las sociedades del conocimiento, y sus personas físicas y organizaciones/personas jurídicas. Mediante ella se genera un nuevo territorio virtual, un nuevo planeta, donde se radican infinidad de construcciones de sus ciudadanos o seres pensantes."[29]

Entonces, no depende de los gobiernos. Si bien los gobiernos podrían regular ciertos aspectos vinculados a algunos tipos de enlaces, siempre los "mensajes" podrán ser

[29] De Paz Pérez, Miguel. **Política administrativa del Estado de Guatemala,** pág. 46.

ruteados por otros, libres de la regulación legal o impuesta por los estados o en todo caso empresas. En términos humanos ¿como sería el acuerdo Internet?, muy simple. A cambio de participar y poder enviar y recibir mensajes, cada persona acuerda trasmitir los mensajes que reciba que no estén destinados a ella.

Así cuando Perico recibe un mensaje para Juan, si lo conoce se lo lleva, si no lo conoce se lo da al amigo que tenga mas posibilidades de conocer a Juan –que este mas cerca en algún sentido-, por ejemplo Pedro. Y Pedro hace lo mismo, y así sucesivamente hasta que llegue a Juan. No importa si usan teléfonos, correo, la radio, la televisión, palomas mensajeras, satélite, boca a boca, email, mensajeros, etc. No importa si el mensaje tiene dirección de origen, no importa si el mensaje es un texto, un programa, una foto, una canción, si esta encriptado, etc... Hay muy pocas cosas a decidir en Internet. No es gobernable, como un país, o eventualmente el planeta, porque no hay cosas que decidir en forma conjunta, cada uno de los que participan toman sus decisiones.

Por otra parte los ciudadanos del mundo no delegaron a sus gobiernos nacionales autoridad constitucional, legal o consuetudinaria sobre sus mensajes en Internet o sobre Internet misma. Para que un gobierno democrático pueda atribuirse legitimidad de origen sobre su porción de Internet (y costaría mucho definir tal cosa) debería hacer un plebiscito. Es difícil ver, por otro lado, el interés social de este proceso. Por un lado los ciudadanos virtuales -usuarios- no tienen un peso proporcional al que les daría la representatividad de su gobierno. Es más, el concepto de peso relativo, esencial a la idea de democracia y gobierno le es ajeno.

La mayoría de quienes utilizan el internet tienen cuentas de mails ubicadas en varios países, paginas web distribuidas en diferentes continentes, amigos por todos los países, uso servicios y servidores de mensajería que no se donde están, fotos en cualquier parte del mundo.

Las decisiones en Internet las toman los dueños de sus propias computadoras y utilizando sus claves de acceso, es decir sus ciudadanos o usuarios. Los ciudadanos virtuales como se les ha denominado, acceden a él a través de formularios Web. Internet es producto de la decisión de estas personas, que eligieron el protocolo IP (de los hackers) sobre los otros disponibles: IPX de Novell, DECNET de Digital, SNA de IBM, SMB de Microsoft, etc.

Entonces, en este caso, son muy pocas las fuentes o sistemas de control de origen, que bien pueden ser tomadas en cuenta en forma especifica para contrarrestar virtualmente ilícitos penales que los propios usuarios decidan cometer, sabiendo previamente éstos que tales actos o hechos constituyen delito, pero sin embargo, si no se regulan estos sino se tienen un control en éstos sistemas, como se podrá regular por parte del Estado, a pesar de las circunstancias en que éste se encuentra ante la globalización y tendencia de la utilización de este servicio.

Entonces, tal como se encuentra en la actualidad, el uso ilimitado de Internet, las formas en que los usuarios experimentan y que algunos de estos, tienen otros fines como delictivos, implica comprender de que se trata de un universo evolutivo nuevo que por derecho propio y en el que la gente define su propio espacio normativo, se esta desarrollando si no existe alguna forma de control.

Como bien lo dijo Broud Spencer;" el vencedor entre otros mundos paralelos posibles, es el internet y éste se define al adaptar las nuevas tecnologías a lo que el ser humano y sus sociedades pueden aceptar y disfrutar. Tiene sus genes (código IP) y un cerebro automático determinado por los genes, las posibles decisiones a tomar son pocas e irrelevantes. Es producto de aplicar nuevas ideas al filtro de las sociedades humanas, por eso reitera que el Internet es "la mas humana de las redes posibles" e intentar plantear un control legal, ideológico controlante, y/o interesado externo al producto de un exquisito equilibro de relaciones humanas y tecnología es equivocar el camino, porque surgirá otra red que será rápidamente adoptada por los humanos." [30]

[30] Broud Spencer. **La computación, la comunicación y el futuro.** Pág. 63.

Agrega este autor que cada vez que un ciudadano virtual ejecuta un programa, lo elige y vota por el, que la gente no sea consciente de ello, es tan poco importante como que los votantes de Bush supieran que este iba a empezar una guerra en Irak, citando un ejemplo de lo que sucede con ésto.

A pesar de que se tiene el concepto de que el Internet es y debe seguir siendo una red universal, redundante, descentralizada, con ciudadanos con la posibilidad de anonimato o identidad virtual, debe constituirse también paralelamente un marco normativo precisamente para que ese mundo virtual continué siéndolo dentro de un ambiente de paz, armonía entre los que se comunican y no de desconfianza, traición, etc., en que se puede volver a través de la comisión de los hechos delictivos, tal como se han venido analizando.

Tomando en consideración que el Internet es un nuevo espacio mundial no sujeto a fronteras nacionales, corporaciones globales, sino a la voluntad dispersa y en votación continua de sus ciudadanos que deciden que protocolo, redes, hardware, y software utilizan para sus mensajes, entonces, no se trata de un problema de un Estado, sino amerita que los Estados conformen el marco rector normativo que regirá precisamente a los Estados parte, para prevenir y sancionar hechos o actos delictivos que se ocasionen a través del uso del internet, fundamentalmente los sistemas de control que es allí en donde debe enmarcarse la problemática de los abusos que se cometen vía internet.

Dentro de los problemas que los gobiernos deben observar se encuentran los denominados spam, que como se dijo, representan mensajes subliminales que aparecen constantemente y que provocan incitar al usuario a entrar, así también el hecho de que un usuario proceda a dar lectura de mensajes privados indebidamente y que con ello provoque un perjuicio, el terrorismo de Estado y espionaje a las personas por los Estados, etc., constituyen figuras delictivas que necesariamente deben sancionarse.

Generado de la constancia en la comisión de ilícitos, cabe señalar también, que los que más con frecuencia se cometen son los relacionados con los derechos de autor. Es cierto que cada país participa de ámbitos internacionales donde se acuerdan las cuestiones vinculadas a los derechos de autor, las patentes y las marcas, sin embargo, eso no ha sido suficiente.

Se han señalado unas virtudes del Internet que permiten inferir la difícil tarea de los gobiernos por crear marcos regulatorios evitando los abusos y consecuentemente la comisión de hechos y actos delictivos. Estas son:

a. El Internet no tiene dueño. Quiere decir que es una cosa, que no puede ser apropiada en forma exclusiva. Es un acuerdo. No solo esta en el dominio publico, sino que es un dominio público.

b. Es un recurso confiable. Funciona, no obliga ha hacer nada que no se quiera y lo que se haga independientemente de que no incrementa su precio.

d. No hay problemas de que unas partes funcionen con un proveedor y otras con otros, o con una empresa si y con otra no.

e. El mantenimiento esta distribuido entre sus participantes. No concentrado en las manos de una empresa que puede quebrar.

f. Todos y todas pueden usar el Internet. Esta pensado para incluir a todos en el planeta. Habrá que resolver problemas de pobreza o geografía, pero nada impide que solucionados los problemas estructurales de la humanidad, todos la puedan usar.

g. Todos y todas la pueden mejorar Todos pueden contribuir y hacerla un lugar mejor, contribuyendo con algo. Es muy difícil empeorarla.

En virtud de ello, una manera de control es a través del establecimiento de patentes, en el control de las PCS con TCG. Estas patentes necesariamente tienen que ser dirigidas por el Estado, porque si se deja en manos privadas, es fácil suponer que la empresa más poderosa del mundo, puede controlar estos sistemas permite inferir que podrá controlar en forma negativa el mundo a través de la PC. Por ende nadie debe controlar nada, a excepción del Estado que es el único que en apariencia busca o debe buscar el bien común.

En consecuencia de lo anterior, deben ser considerados los metatags como parte de la competencia desleal y como tal debe ser regulado en los delitos informáticos que se señalan en el Código Penal.

4.7. La regulación de los procedimientos para el control de los sistemas automatizados que contribuyen a la comisión de hechos delictivos por el uso de los metatags en el internet

Éstos son mecanismos que deben emplear los Estados, precisamente para resguardar una serie de derechos que le asisten a los usuarios de Internet[31] y que de alguna manera a través del uso de este sistema de redes también se puede contrarrestar, se deben identificar tres tipos de tecnologías para combatir la delincuencia: de identificación, de vigilancia y de investigación. Las principales tecnologías de identificación son las contraseñas, los cookies y los procedimientos de autenticidad. Las contraseñas son los símbolos convenidos que el usuario utiliza para entrar en esta red. Los cookies son marcadores digitales que los web sites así equipados insertan automáticamente en los discos duros de los ordenadores que los conectan. Una vez que un cookie entra en un ordenador, todas las comunicaciones de dicho ordenador en la red son automáticamente registradas en el web site originario del cookie.

En este caso, los procedimientos de autenticidad son firmas digitales que permiten a los ordenadores verificar el origen y características de las comunicaciones recibidas.

[31] **Ibid.**

Generalmente, utilizan tecnología de encriptación. Trabajan por niveles, de modo que los servidores identifican a usuarios individuales y las redes de conexión identifican a los servidores.

Las tecnologías de vigilancia permiten interceptar mensajes, insertar marcadores gracias a los cuales se puede seguir la comunicación de un ordenador o un mensaje marcado a través de la red; también consisten en la escucha continua de la actividad de comunicación de un ordenador o de la información almacenada en dicho ordenador. El famoso programa Carnivore; "del FBI permite analizar mediante palabras clave enormes masas de información de las comunicaciones telefónicas o Internet, buscando y reconstruyendo en su totalidad aquellos mensajes que parezcan sospechosos (aunque algunas detenciones sobre esas bases resultaron bastante chuscas, arrestando a buenas madres de familia que comentaban electrónicamente el peligro del consumo de drogas en la escuela de sus hijos).

Las tecnologías de vigilancia permiten identificar el servidor originario de un determinado mensaje. A partir de ahí, por colaboración o coacción, los mantenedores de los servidores pueden comunicar al detentor del poder la dirección electrónica de donde provino cualquier mensaje.

Por ello, las tecnologías de investigación se organizan sobre bases de datos obtenidos del almacenamiento de la información resultante de las tecnologías de vigilancia. A partir de esas bases de datos se pueden construir perfiles agregados de usuarios o conjuntos de características personalizadas de un usuario determinado. Por ejemplo, mediante el número de tarjeta de crédito, asociado a un número de carné de identidad y a la utilización de un determinado ordenador, se puede reconstruir fácilmente el conjunto de todos los movimientos que realiza una persona que dejen registro electrónico.

Como eso es algo que hacemos todos los días (teléfono, correo electrónico, tarjetas de crédito), parece evidente que ya no hay privacidad desde el punto de vista de la

comunicación electrónica. O sea, la combinación de las tecnologías de identificación, de vigilancia y de investigación configuran un sistema en que quién tenga el poder legal o fáctico de acceso a esa base de datos puede conocer lo esencial de lo que cada persona hace en la red y fuera de ella y ésto es importante para las políticas de prevención que ostenta el Derecho Penal." [32]

Desde ese punto de vista, la red no se controla, pero sus usuarios están expuestos aún control potencial de todos sus actos más que nunca en la historia. Así pues, un poder político, judicial, policial o comercial (defensores de derechos de propiedad) que quiera actuar contra un internauta determinado puede interceptar sus mensajes, detectar sus movimientos y, si están en contradicción con sus normas, proceder a la represión del internauta, del prestador de servicios, o de los dos. Lo anterior denota que si efectivamente puede existir un control y no precisamente como aducen muchos, que el uso del internet permite a su usuario mantenerse en el anonimato.

Obviamente, el control de esa manera podría no solo provenir del Gobierno y de la policía sino también de determinadas empresas privadas. Se ha sabido que algunas empresas vigilan rutinariamente el correo electrónico de sus empleados y también, se tiene conocimiento en el caso de las universidades, el de sus estudiantes, porque la protección de la privacidad no se extiende al mundo del trabajo, bajo el control de la organización corporativa, que si bien constituye un tema interesante de abordar, no será motivo de ello, por el enfoque que se pretende darle a la presente investigación.

Resulta entonces, muy difícil pero no imposible que basándose en el principio de libertad, en un mundo en que la tecnología puede servir para el control de las vidas de los seres humanos mediante su registro electrónico, y la tendencia al control ubicuo es ya de por si irreversible. En sociedad, todo proceso está hecho de tendencias y contra tendencias, y la oposición entre libertad y control continúa sin fin, a través de nuevos medios tecnológicos y nuevas formas institucionales, basados en la necesidad de

[32] Repolles. **Ob. Cit.** Pág. 53

prevenir ilícitos que afecten precisamente a la sociedad y la tranquilidad de la misma dentro de un aspecto de la vida de los ciudadanos.

Por eso, como lo han establecido algunos tratadistas respecto del tema, que a las tecnologías de control y vigilancia se contraponen tecnologías de libertad. Señalan que por un lado, el movimiento para el software de fuente abierta permite la difusión de los códigos sobre los que se basa el procesamiento informático en las redes. Por consiguiente, a partir de un cierto nivel de conocimiento técnico, frecuente entre los centros de apoyo a quienes defienden la libertad en la red, se puede intervenir en los sistemas de vigilancia, se pueden transformar los códigos y se pueden proteger los propios programas. Naturalmente, si se pone un ejemplo de lo que se dijo anteriormente, el mundo en general, y en Guatemala no es la excepción, se acepta sin mayores complicaciones el mundo de Microsoft, aunque en muchos casos, a través de esta red, se acaba cualquier posibilidad de privacidad y, por tanto, de libertad en la red, porque los usuarios se someten a las reglas de esta entidad para navegar en el internet.

Al tener un marco regulatorio sobre los controles de origen, resulta fácilmente comprensible y viable la regulación de los mensajes o los metatags indebidos que a través de la web se introducen al usuario cuando este se encuentra utilizando el Internet.

Como producto de lo anterior, aparte de que se deben regular la prohibición de los metatags que no se encuentren debidamente registrados, también, deben existir otras medidas tendientes a hacer positiva la normativa de prohibición que se propone con respecto de los metatags, y por ello, se deben considerar las siguientes medidas que debieran regularse:

4.8. La ciencia de la encriptación

Este sistema se refiere a la utilización de impresiones digitales, firma digital o claves que constituyen procedimientos de verificación de identidad del emisor y destinatario.

Si bien es cierto que, como toda tecnología, su relación con la libertad es ambigua, como señala Lessig;" porque, por un lado, protege la privacidad del mensaje pero, por otro, permite los procedimientos de autentificación que verifican la identidad del mensajero. Sin embargo, en lo esencial, las tecnologías de encriptación permiten, cuando funcionan, mantener el anonimato del mensaje y borrar las huellas del camino seguido en la red, haciendo difícil, pues, la interceptación del mensaje y la identificación del mensajero. Por eso, la batalla sobre la encriptación es, desde el punto de vista técnico, es una batalla fundamental por la libertad en internet." [33]

4.9. El control de los hackers

Como se ha mencionado, los hackers son personas con conocimientos técnicos informáticos cuya pasión es inventar programas y desarrollar formas nuevas de procesamiento de información y comunicación electrónica. "Según este autor, para ellos, el valor supremo es la innovación tecnológica informática. Y, por tanto, necesitan también libertad. Libertad de acceso a los códigos fuente, libertad de acceso a la red, libertad de comunicación con otros hackers, espíritu de colaboración y de generosidad (poner a disposición de la comunidad de hackers todo lo que se sabe, y, en reciprocidad, recibir el mismo tratamiento de cualquier colega). Algunos hackers son políticos y luchan contra el control de los gobiernos y de las corporaciones sobre la red, pero la mayoría no lo son, lo importante para ellos es la creación tecnológica. Se movilizan, fundamentalmente, para que no haya cortapisas a dicha creación. Los hackers no son comerciales, pero no tienen nada contra la comercialización de sus conocimientos, con tal de que las redes de colaboración de la creación tecnológica sigan siendo abiertas, cooperativas y basadas en la reciprocidad.

La cultura hacker se organiza en redes de colaboración en Internet, aunque de vez en cuando hay algunos encuentros presenciales. Distintas líneas tecnológicas se agrupan en torno a grupos cooperativos, en los cuales se establece una jerarquía tecnológica

[33] Lessig, Robert. **El internet**. Pág. 6.

según quiénes son los creadores de cada programa original, sus mantenedores y sus contribuidores." [34]

En virtud de la habilidad que tienen estos personajes y de la forma en que se introducen en las fuentes de información y de comunicación, a pesar de que favorece el principio de libertad, este debe ser restringido por el principio de seguridad, por ello, se ha establecido especialmente en la legislación que se ha analizado en este trabajo, la necesidad de que se regule su intervención, porque a pesar de la habilitad técnica que éstos tienen y de la forma en que se introducen también existe el peligro de que provoquen ya no actos que tiendan a la aspiración de libertad, sino que sus fines sean puramente criminales.

Este autor, a manera de ejemplo, se refiere a lo sucedido con uno de los movimientos más representativos de lo que realizan los hackers en el mundo, cuando trata lo relativo al movimiento hacker más político (en términos de política de libertad tecnológica) que fue el creado por Richard Stallman, un programador de MIT, que constituyó en los años ochenta la Free Software Foundation para defender la libertad de acceso a los códigos de UNIX cuando ATT trató de imponer sus derechos de propiedad sobre UNIX, el sistema operativo más avanzado y más compatible de su tiempo, y sobre el que se ha fundado en buena parte la comunicación de los ordenadores en la red. A tal grado llegó la intervención de este hacker que sustituyó el copy right por el copy left. Es decir, que cualquier programa publicado en la red por su Fundación podía ser utilizado y modificado bajo licencia de la Fundación bajo una condición: difundir en código abierto las modificaciones que se fueran efectuando.

Sobre esa base, desarrolló un nuevo sistema operativo, GNU, que sin ser Unix, podía utilizarse como Unix. Pero lo que esto significa es lo siguiente: una gran transformación tecnoeconómica necesita un caldo de cultivo en un sistema de valores nuevo que motive a la gente para hacer lo que hace. En el caso del capitalismo, fue la ética del

[34] Raimond, Levy. **Los hackers en el internet**. Pág. 98

trabajo y de la acumulación de capital en la empresa como forma de salvación personal (lo cual, desde luego, no impidió, sino que justificó, la explotación de los trabajadores).

En suma, en la medida en que los sistemas informáticos y las comunicaciones por Internet se han convertido en el sistema nervioso de las sociedades actuales, la interferencia con su operación a partir de una capacidad técnica de actuación en la red es un arma cada vez más poderosa, que puede ser utilizada por distintos actores y con distintos fines, por ello, es que amerita que exista una regulación al respecto.

La vulnerabilidad de los sistemas informáticos plantea una contradicción creciente entre seguridad y libertad en la red. Por un lado, es obvio que el funcionamiento de la sociedad y sus instituciones y la privacidad de las personas no pueden dejarse al margen de cualquier acción individual o de la intromisión de quienes tienen el poder burocrático o económico de llevarla a cabo. Por otro lado, como ocurre en la sociedad en general, con la necesidad de proteger la información en la red se acude al control sobre la libre comunicación, para evitar los abusos en que se puedan encontrar unos con otros se supere por la técnica y la habilidad como sucede con los hackers y que esto sea negativamente empleado en perjuicio.

Sin embargo, es evidente de que la sociedad en general se encuentra ante un dilema que no ha sido resuelto, de tal manera que las cosas se encuentran como están en la actualidad. Ésto es en cuanto a que el debate sobre seguridad y libertad se estructura por un lado, la regulación político-jurídica de la red; por el otro, la autoprotección tecnológica de los sistemas individuales. Quienes defienden la capacidad de autorregulación de la red argumentan que existen tecnologías de protección que son poco vulnerables, sobre todo cuando se combinan los fire walls (o filtros de acceso) de los sistemas informáticos con las tecnologías de encriptación, que hacen muy difíciles de interceptar los códigos de acceso y el contenido de la comunicación. Es así como están protegidos los ordenadores del Pentágono, por ejemplo, en los Estados Unidos, o bien algunos de los bancos más famosos del mundo.

Porque si la mayor parte de las instituciones de poder y de las grandes empresas tiene sistemas de seguridad a prueba de cualquier intento de penetración, ésto no sucede igual en el caso de cualquier persona, si los mismos riesgos o peores podrían estarle sucediendo dentro de la perspectiva de los derechos fundamentales.

Otro ejemplo, que se ha citado respecto a los sistemas de control, es lo ocurrido en el año 2000 cuando los crackers se introdujeron en el sistema de Microsoft y obtuvieron códigos confidenciales, a partir de la penetración en el sistema personal de un colaborador de Microsoft que tenía acceso a la red central de la empresa. Es manifiestamente imposible proteger el conjunto de la red con sistemas de fire walls y encriptación automática.

Este autor se refiere; "a que sólo la difusión de la capacidad de encriptación y de autoprotección en los sistemas individuales podría aumentar la seguridad del sistema en su conjunto. En otras palabras, un sistema informático con capacidad de computación distribuida en toda la red necesita una protección igualmente distribuida y adaptada por cada usuario a su propio sistema. Pero eso equivale a poner en manos de los usuarios el poder de encriptación y autoprotección informática. Algo que rechazan los poderes políticos con el pretexto de la posible utilización de esta capacidad por los criminales (en realidad, las grandes organizaciones criminales tienen la misma capacidad tecnológica y de encriptación que los grandes bancos). En último término, la negativa de las administraciones a permitir la capacidad de encriptación y de difusión de tecnología de seguridad entre los ciudadanos conlleva la creciente vulnerabilidad de la red en su conjunto, salvo algunos sistemas absolutamente aislados y, en última instancia, desconectados de la red." [35]

De ahí que gobiernos y empresas busquen la seguridad mediante la regulación y la capacidad represiva de las instituciones más que a través de la autoprotección tecnológica de los ciudadanos.

[35] Season, Albert. **Los sistemas de control en el internet**. Pág. 187.

Como señalaba el abogado de Kriptópolis, Sánchez Almeida; "ya existen suficientes normativas para proteger los derechos de los ciudadanos y penalizar las conductas delictivas, dentro y fuera de la red. Basta con aplicarlas. El problema puede ser técnico, la dificultad de aplicar esas sanciones en la red, lo cual requiere una modernización de las instituciones judiciales y policiales." [36]

La dificultad de esa modernización intenta resolver el problema descentralizando la censura previa a la estructura de prestadores de servicios y haciéndolos responsables de las excepcionales infracciones que puedan representar algunos contenidos. Es como hacer responsables a los propietarios de las imprentas por las consecuencias que pudieran resultar de la publicación de ciertos artículos en la prensa. O a los operadores de telecomunicaciones por las conversaciones telefónicas entre mafiosos que planean un robo.

La segunda observación se refiere a la postura ideológica defensiva de los reguladores de Internet. Se multiplican las fórmulas precautorias para afirmar la importancia de Internet y de su libre expresión, en línea con la ideología liberal que predomina en la mayoría de los gobiernos europeos, cualquiera que sea su tendencia política. Pero los viejos reflejos estatistas se combinan con esa ideología, llevando a formulaciones ambiguas y políticas titubeantes, cuya plasmación legislativa contribuye a la confusión.

En tercer lugar, es notable la capacidad de reacción de la comunidad internauta a cualquier intento de coartar su libertad. No tendrán la vida fácil quienes aún piensen que las instituciones del Estado pueden continuar operando como antes del desarrollo de Internet. Ahora bien, la defensa de la libertad en Internet tiende a ser selectiva. Se reacciona contra el Estado, pero se descuida la defensa de la libertad de los usuarios, de los ciudadanos y de los trabajadores, en un mundo en que los abusos de poder y la desigualdad no han desaparecido ante la magia de la red.

[36] Sánchez Almeida, Luis. **Kriptopolis.** Pág. 56.

Por un lado, muchos prestadores de servicios imponen condiciones económicas leoninas para acceder a la red, invaden la privacidad de sus usuarios y organizan enlaces en la red según sus intereses comerciales, por ejemplo, jerarquizando los web sites en los buscadores. La defensa de la libre expresión y comunicación en la red debería alcanzar a todo el mundo, a los consumidores, a los trabajadores, a las organizaciones cívicas. Y en esa libertad parece normal incluir las condiciones materiales de dicha libertad, empezando por las tarifas de conexión y la difusión de los medios informáticos de comunicación en el conjunto de la población. La libertad sin igualdad se convierte en privilegio y debilita los fundamentos de su defensa por parte de la sociedad en su conjunto.

4.10. Encriptación

Las organizaciones de poder, a lo largo de la historia, han hecho del secreto de sus comunicaciones un principio fundamental de su actividad. Dicho secreto se intentó proteger mediante la encriptación, es decir, la codificación del lenguaje mediante una clave secreta sólo conocida por la organización emisora del mensaje y el destinatario del mensaje determinado por dicha organización.

"El origen de la informática contemporánea durante la Segunda Guerra Mundial parece estar relacionado con los esfuerzos de matemáticos extraordinarios, como el inglés Turing, para desarrollar algoritmos capaces de descifrar los códigos del enemigo. Por tanto, en cierto modo, no es de extrañar en la era de la información, basada en la comunicación de todo tipo de mensajes, que el poder (y, por tanto, la libertad) tenga una relación cada vez más estrecha con la capacidad de encriptar y descifrar. La encriptación es el principal campo de batalla tecnológico-social para la preservación de la libertad en Internet."[37]

Este método requeriría de una centralización total del sistema de claves únicas y, por tanto, puede ser vulnerable a quiénpenetra en esa base de datos, con habilidades para

[37] **Ibid.**

ello. Esta forma de claves, puede ser comparada con lo que sucede con el secreto militar, o las agencias de inteligencia de los Estados Unidos, el FBI por ejemplo.

Considerando todos los argumentos expresados anteriormente, se propone el siguiente proyecto de ley respecto de sus bases para regular lo relativo a los delitos informáticos, desde el enfoque de los sistemas de control de origen y no en forma generalizada tal como se encuentra regulado en el Código Penal, siendo menester por la especialidad o naturaleza de la comisión de este tipo de ilícitos, que se crée una ley especifica al respecto, sin embargo, mejorar las que establece el Código Penal también podrían resultar aceptables para proteger a los ciudadanos en el uso del Internet de abusos y de hechos constitutivos de ilícitos.

Como bien se sabe, utilizando como herramienta la Internet y los sistemas computarizados, se cometen, delitos comunes que ya se encuentran regulados en el Código Penal, como hurto, estafa, robo, usurpación de calidad, falsificación de documentos, etc., entonces, debiera en cada uno de estos delitos comunes que se establecen en el Código Penal, establecer lo relativo al medio especial como es el uso de la computadora y el Internet.

En ese orden de ideas, a continuación, se propone que se regule de manera específica las siguientes figuras.

- En los primeros artículos, es indispensable que se establezcan definiciones que permitirán comprender el contenido del marco normativo, como 1. Sistema informático: todo dispositivo o grupo de dispositivos interconectados o relacionados a través de redes informáticas o de telecomunicaciones, que conforme a un programa realizan el procesamiento y transmisión automatizada de datos; 2. Dato Informático o Electrónico: significa cualquier representación de hechos o información o señal de telecomunicaciones, susceptible de ser procesada en un sistema informático. 3. Acceso ilegal. El que sin autorización realice cualquier acto tendiente a acceder o acceda a un sistema informático, será

castigado con presidio menor en su grado mínimo. 4. Adueñarse de información. El que sin autorización conozca, use o se apodere de datos contenidos en un sistema informático, será castigado con presidio menor en sus grados medio a máximo.

- Sabotaje informático. El que maliciosamente destruya o inutilice un sistema informático o sus medidas de protección, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en sus grados medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo. 6. Intercepción, interferencia y alteración de datos. El que maliciosamente intercepte, interfiera, altere, dañe o destruya los datos contenidos en un sistema informático, será castigado con presidio menor en sus grados medio a máximo. 7. Mal uso de dispositivos o programas de diseminación de virus. La creación o distribución de cualquier dispositivo o programa, con el objeto de materializar las conductas sancionadas por los artículos anteriormente mencionados de este marco normativo, será castigado con presidio menor en su grado máximo. 8. Revelación o difusión de datos. El que maliciosamente revele o difunda los datos contenidos en un sistema informático, sufrirá la pena de presidio menor en su grado medio. Si quiénincurre en estas conductas es el responsable del sistema informático, la pena se aumentará en un grado; 9. Fraude informático. Incurrirán en penas de prisión y multa quiéncon ánimo de lucro, obtengan mediante una manipulación de un sistema informático, una transferencia indebida de cualquier activo patrimonial en perjuicio de tercero.

- Debe establecerse un capítulo que se refiera exclusivamente a los delitos contra los sistemas que utilizan tecnologías de información, y dentro de este, se debieran establecer figuras delictivas como: 1. Acceso Indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será sancionado con penas de prisión no menores de 15 años y multa. 2. Sabotaje o

Daño a Sistemas. Todo aquél que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será sancionado con penas de prisión que no superen los l5 años y multa. Deberá incurrir en la misma pena quién destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena se aumentara si los efectos o las consecuencias se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo. 3. Favorecimiento culposo del sabotaje o daño. Si el delito que se señala en el numeral 2 se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se deberá aplicar la misma pena, solo que con una reducción entre la mitad y dos tercios. 4. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en las figuras delictivas señaladas en los numerales 2 y 3 se deberán aumentar entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

- Posesión de Equipos o Prestación de Servicios de Sabotaje. Quién importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas; con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será sancionado con penas de prisión que no sean menores de l5 años y pena de multa. 6. Espionaje Informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será sancionado con penas de prisión que no superen los l5 años y multa. Se tendrá que aumentar esta pena si el delito previsto en este apartado se cometiere con el fin de obtener algún tipo de beneficio para sí o para

otro. Procederá también un incremento en la pena, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado. 6. Falsificación de Documentos. Quién, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será sancionado con penas de prisión que no superen los l5 años y de multa. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena impuesta deberá aumentarse. Se deberá también incrementar la pena si del hecho resultare un perjuicio para otro. 7. Acceso abusivo a un sistema informático. Será sancionado quién sin autorización acceda a un sistema informático protegido o se mantenga dentro del mismo en contra de la voluntad de quién tenga el legítimo derecho a excluirlo. 8. Obstaculización ilegítima de sistema informático o red de telecomunicación. Se penalizará a quién impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones. 9. Interceptación de datos informáticos. Bajo este delito serán castigadas las personas que, sin orden judicial previa, intercepten datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte. 10. Daño informático. Se sancionará a quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. 11. Uso de software malicioso. El proyecto de ley señala que serán castigadas las personas que, sin estar facultadas para ello, produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos. 12. Suplantación de sitios web para capturar datos personales. Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También

quiénmodifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. En este caso la pena se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- También, deberá establecerse en los delitos contra la propiedad, y las figuras delictivas que se analizaron en este trabajo, aspectos relacionados con el robo y el hurto, y señalar: 1. Respecto del robo y el hurto. Quién a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con penas de prisión que no menor de l5 años y pena de multa. 2. Fraude Computarizado. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión y multa.

- Obtención Indebida de Bienes o Servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con penas de prisión que no superen los l5 años y de multa. 4. Manejo Fraudulento de Tarjetas Inteligentes o Instrumentos Análogos. Toda persona que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías

de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será sancionada con prisión que no supere los l5 años y pena de multa. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

- Apropiación de Tarjetas Inteligentes o Instrumentos Análogos Quién se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será sancionado con penas de prisión que no supere los l5 años y pena de multa... La misma pena se impondrá a quién adquiera o reciba la tarjeta o instrumento a que se refiere la presente figura delictiva. 6. Provisión Indebida de Bienes o Servicios Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quién los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será sancionado con pena de prisión que no supere los l5 años y pena de multa.

- Posesión de Equipo para Falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será sancionado con pena de prisión que no supere los l5 años y pena de multa.

- También, debiera establecerse un capítulo que se refiera a los delitos contra la privacidad de las personas y de las comunicaciones, y separar los que ya se analizaron que se encuentran contenidos en el Código Penal, respecto de las figuras delictivas parecidas; se debiera como mínimo, establecer las siguientes figuras delictivas: 1. Violación de la Privacidad de la Data o Información de Carácter Personal Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será sancionado con pena de prisión que no supere los l5 años y pena de multa.. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero. 2. Violación de la Privacidad de las Comunicaciones. Toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con penas de prisión que no superen los l5 años y pena de multa. 3. Revelación Indebida de Data o Información de Carácter Personal. Quién revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios ya indicados, será sancionado con penas de prisión que no supere los l5 años y pena de multa. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena deberá aumentarse de un tercio a la mitad. 4. Violación de datos personales. Este delito cobijará a quienes, sin estar facultados para ello, con provecho propio o de un tercero, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
- Importante resulta incluir un capítulo que se refiera a la protección de los niños, niñas y adolescentes y deberá establecerse como mínimo los siguientes ilícitos: 1. Difusión o Exhibición de Material Pornográfico Todo aquel que, por cualquier

medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con penas de prisión que no supere los l5 años y pena de multa. 2. Exhibición Pornográfica de Niños o Adolescentes. Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será sancionada con pena de prisión que no supere los l5 años y pena de multa.

- Es importante también, señalar un capítulo referido exclusivamente a los delitos contra el orden económico e incluir las siguientes figuras delictivas: 1. Apropiación de Propiedad Intelectual. Quién sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con penas de prisión que no menor de l5 años y pena de multa. 2. Oferta Engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con penas de prisión que no sean inferiores a l5 años y penas de multa, sin perjuicio de la comisión de un delito más grave.

- También para estos delitos se deben establecer las agravantes especiales para los mismos. Además, las penas accesorias, como por ejemplo: 1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en esta ley. 2. El trabajo comunitario por el término de hasta tres años. 3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo

por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente. 4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica. 5. Divulgación de la Sentencia Condenatoria. El Tribunal podrá además, disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

- En este caso, si se crea una ley especifica se debe regular lo relativo a la indemnización civil o la reparación. La indemnización en favor de la víctima debe ser por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos.

CONCLUSIONES

1. A pesar de que en el Código Penal guatemalteco se establecen los bienes jurídicos que deben ser protegidos por ser considerados esenciales para la sociedad guatemalteca, los mismos han quedado rezagados ante el avance de la era tecnológica, porque existen una serie de actos vinculados con el uso de Internet que aún no han sido tipificados como delitos.

2. Debido a que el Código Penal guatemalteco data del año 70 del siglo XX, el mismo no ha sido adecuado para incluir bienes jurídicos a ser protegidos tales como los relacionados al control del origen del Internet; porque la ausencia de tipificaciones acerca de estos hechos limita la posibilidad de perseguirlos penalmente por parte del Ministerio Público.

3. Aun que el surgimiento y difusión del Internet ha contribuído a acercar a las sociedades en el mundo, el mismo también ha permitido la difusión de actos ilícitos, los cuales muchas veces no han sido tipificados como tales, permitiéndole a los perpetradores de los mismos continuar realizándolos impunemente mientras no exista normativa nacional e internacional para perseguirlos.

4. Los delitos informáticos surgen a partir del uso de la computadora, en contra de programas de computación o a través de Internet, lo cual vuelve complicada la tipificación de estos ilícitos si los legisladores no cuentan con la asesoría técnica del caso, pues su ausencia puede dejar fuera acciones o hechos perjudiciales para la sociedad y tipificar casos que resultan ser de bagatela.

5. Uno de los actos más comunes que se realiza a través de Internet es la colocación de ventanas publicitarias conocidas como metatags, los cuales constituyen mensajes que se introducen en el Internet a cualquier hora, momento y espacio, siendo puestas al usuario sin su consentimiento, lo cual es una violación al derecho a la intimidad que actualmente no se encuentra calificada como ilícito.

RECOMENDACIONES

1. Que el Colegio de Abogados y Notarios de Guatemala promueva un encuentro de especialistas en derecho informático e informática para que los mismos analicen los delitos informáticos que se encuentran regulados actualmente en el Código Penal, y con ello establecer la validez y claridad de los mismos o bien determina propuestas de cambio; modificación o ampliación que requieran.

2. El Ministerio de Economía y la Unidad de Capacitación del Ministerio Público deben promover cursos sobre derecho informático e informático a los fiscales con el objeto de que los mismos, así como los agentes y auxiliares fiscales, puedan comprender los elementos distintivos de los delitos informáticos y la mejor manera de encuadrar los ilícitos que llevan a cabo los sindicados; para una mejor persecución penal.

3. El Congreso de la República a través de la comisión de de legislación y puntos constitucionales debe establecer vínculos con expertos en derecho informático e informática que hayan elaborado legislaciones penales, donde se tipifiquen los delitos informáticos para que orienten la redacción de nuevos ilícitos orientados a la protección de bienes jurídicos; que pueden ser lacerados por Internet.

4. El Organismo Judicial, el Ministerio Público y el Instituto Público de la Defensa Penal, deben coordinar la implementación de cursos entre sus funcionarios vinculados al ejercicio penal, para que los mismos tengan homogeneidad en la comprensión de los delitos informáticos y sus características para que las acciones penales vinculadas con esos ilícitos sean más eficientes y basadas en las normas jurídicas.

5. Las universidades que impartan la carrera de abogacía y notariado deben implementar cursos obligatorios sobre tipificación de los delitos informáticos, para que sus estudiantes comprendan los elementos característicos que establecen

los bienes jurídicos protegidos, que permitan diferenciarlos y especificarlos con lo cual podrán comprender y aplicar de mejor manera esta nueva rama del derecho penal.

BIBLIOGRAFÍA

AYAU, Manuel. **Como mejorar el nivel de vida**. Guatemala: Ed. Piedra santa, l987.

BROUD, Spencer. **La computación, la comunicación y el futuro.** Madrid, España: Ed. Bosch, 2003.

CÓRDOVA, Marco Antonio. **Delitos monetarios y reserva de ley orgánica.** México: (s.e.), (s.l.i.).

DE MATA VELA, José Francisco y Héctor Aníbal De León Velasco. **Derecho penal guatemalteco.** Guatemala: Ed. Editores, 2001.

DE PAZ PÉREZ, Miguel. **Política administrativa del Estado de Guatemala**. Guatemala. Ed. Universitaria, 2007.

LESSIG, Robert. **El internet.** Madrid, España: (s.e.), 2009.

MALDONADO JUÁREZ, Edgar. **Análisis jurídico crítico del juzgamiento por analogía en los caos de la participación en el delito.** México, D.F.: Ed. Porrua, 1986.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. Madrid, España: Ed. Bosch, 1972.

RAIMOND, Levy. **Los hackers en el internet.** Chile: (s.e.), 2009.

REPOLLES, José Luis. **Manual de derecho penal guatemalteco.** Guatemala: Ed. Piedra Santa, 1983.

SÁNCHEZ, ALMEIDA, Luis. **Kriptopolis**. Chile: Ed. La Paz, 2008.

SANDOVAL RAMÍREZ, Luis. **La computación en el siglo veinte.** Buenos Aires, Argentina: Ed. Capeluz, 2006.

SEASON, Albert. **Los sistemas de control en el internet.** Madrid, España: (s.e.), 2009.

TÉLLEZ VALDÉZ, Julio. **Los delitos informáticos.** Buenos Aires, Argentina: Ed. Capeluz, (s.l.i.).

Legislación:

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

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

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

Ley del Organismo Judicial. Decreto número 2-89 del Congreso de la República de Guatemala.