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

NECESIDAD DE REGULAR EN EL CÓDIGO PENAL LOS DELITOS CIBERNÉTICOS

EDLYN BELEM GUZMÁN MONTES

GUATEMALA, OCTUBRE DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

NECESIDAD DE REGULAR EN EL CÓDIGO PENAL LOS DELITOS CIBERNÉTICOS

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

EDLYN BELEM GUZMÁN MONTES

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, octubre de 2015

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

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

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera fase:

Presidente:	Lic. Jaime Ernesto Hernández Zamora
Vocal:	Licda. Olga Aracely López
Secretario:	Lic. Mauro Danilo García Toc

Segunda Fase:

Presidente:	Lic. Jorge Mario Yupe Cárcamo
Vocal:	Lic. Marco Vinicio Hernández
Secretario:	Lic. Marvin Hernández

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 27 de octubre de 2014.

Atentamente pase al (a) Profesional, **JORGE APARICIO ALMENGOR VELASQUEZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **EDLYN BELEM GUZMÁN MONTES**, con carné **200717573**, intitulado **NECESIDAD DE REGULAR EN EL CÓDIGO PENAL LOS DELITOS CIBERNÉTICOS.**

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

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

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIDAD DE ASESORÍA DE TESIS
GUATEMALA, C. A.

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

Fecha de recepción 20 / 01 / 2015. f)

Asesor(a)
JORGE APARICIO ALMENGOR VELASQUEZ
ABOGADO Y NOTARIO

LICENCIADO JORGE APÁRICIO ALMENGOR VELASQUEZ

ABOGADO Y NOTARIO

Guatemala C. A. Tel. 24330096, 5 Calle 13 Ave. "A" Col. Monte Real II Z. 4 de Mixco

Guatemala, 24 de febrero de 2015.

Dr. Bonerge Amilcar Mejía Orellana

Jefe de la Unidad de Asesoría de Tesis

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala

Presente.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
26 FEB. 2015
UNIDAD DE ASESORÍA DE TESIS
Hora:
Firma:

Señor Jefe de la Unidad de Asesoría de Tesis:

En atención a la providencia de esa dirección, de fecha 20 de enero de 2015, en la cual se me nombra asesor de tesis del bachiller EDLYN BELEM GUZMÁN MONTES, quien elaboró el trabajo de tesis intitulado **"NECESIDAD DE REGULAR EN EL CÓDIGO PENAL LOS DELITOS CIBERNÉTICOS".** Hago constar que no tengo ningún parentesco dentro de los grados de ley con el asesorado, asimismo informo que habiendo asesorado el trabajo encomendado, me permito emitir el siguiente:

DICTAMEN

El trabajo investigado tiene un profundo y fiable contenido científico y técnico ya que fue basado en libros especializados en la materia como podrá corroborarse en la bibliografía respectiva; la metodología utilizada se basa en los métodos científico, histórico, inductivo, deductivo y el analítico; las técnicas de investigación utilizadas fueron las bibliográficas, las documentales y estadísticas. En la redacción de la tesis le recomendé que por tratarse de un tema técnico jurídico, debería emplear un lenguaje escrito comprensible para alcanzar la finalidad de la misma, que es dar conocer a la sociedad la importancia que sean reguladas las conductas ilícitas en el ámbito cibernético y/o informático.

En la elaboración del indicado trabajo de investigación, el autor siguió las instrucciones y recomendaciones anotadas anteriormente, en cuanto al título, la presentación y desarrollo de la misma.

LIC. JORGE APARICIO ALMENGOR VELASQUEZ

ABOGADO Y NOTARIO

Guatemala C. A. Tel. 24330096, 5 Calle 13 Av. "A". Col. Monte Real II Z. 4 de Mixco.

Se han desarrollado adecuadamente cada uno de los capítulos, en ellos se fundamenta la comprobación de la hipótesis, lo cual genera una contribución científica al sistema formativo guatemalteco.

En la conclusión discursiva el bachiller manifiesta que debido a la información presentada se necesita regular en el Código Penal los Delitos Cibernéticos.

Es por ello que como asesor del trabajo de tesis, y al haberse cumplido con los requisitos establecidos en el Artículo 31 del normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, resulta, procedente aprobar el trabajo de tesis asesorado, razón por la cual doy mí **DICTAMEN** en sentido **FAVORABLE**.

Deferentemente;

Lic. Jorge Aparicio Almengor Velásquez
Abogado y Notario
Colegiado No. 6,422
Asesor de Tesis

JORGE APARICIO ALMENGOR VELASQUEZ
ABOGADO Y NOTARIO

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 15 de abril de 2015.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante EDLYN BELEM GUZMÁN MONTES, titulado NECESIDAD DE REGULAR EN EL CÓDIGO PENAL LOS DELITOS CIBERNÉTICOS. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

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

BAMO/srrs.

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

Lic. Avidán Ortiz Orellana
DECANO

DEDICATORIA

A DIOS: Mi Padre Celestial, que me da la vida, salud y la capacidad intelectual, que me alienta día a día a superarme y superar mis retos personales y en especial este que estoy culminando, "Gracias Señor Jesús"

A MI ESPOSO: Mi ayuda idónea, que con su apoyo incondicional y constante supo alentarme y ayudarme a lograr mi propósito profesional, como también ser mi apoyo emocional en momentos de flaqueza e incertidumbre.

A MI HIJA: Sofia Monroy, mi pedacito de cielo aquí en la tierra, que desde que estaba en el vientre me acompañaba en las aulas de los últimos semestres y quien ha sido mi inspiración para seguirme superando y luchando por ser mejor y contribuir para que este mundo sea un lugar adecuado para su desarrollo.

A MIS PADRES Y HERMANAS: Mis padres Elvis Guzmán y Marleni Montes, por ser el instrumento de Dios para traerme a este mundo y por sus cuidados, a mis hermanas por su compañía y apoyo.

A LOS PROFESIONALES: Licenciados: Héctor Manfredo Maldonado Méndez, Rolando Antonio Solomán Rangel, Benjamín Reyes, Morey Zuleta, Jorge Almengor, Bonerge Mejía, William López Morataya, Hugo Cabrera, Mario Alegría, Menfil Fuentes, Juan Carlos Rios, Alex Ortiz, Avidán Ortiz, Edwin Rueda, Héctor Indalecio, Luis Renato Pineda, Polanco Gil, Velas Luna, Arely Camey, Eloisa Mazariegos, Eugenia Fratti.

A MIS COMPAÑEROS DE ESTUDIO: Por compartir conmigo los éxitos y fracasos, a lo largo de este camino lleno de obstáculos y a veces tropiezos, no hubiese sido igual si no hubiera tenido su apoyo y su compañía.

A MI CASA DE ESTUDIOS: La Tricentenaria Universidad de San Carlos de Guatemala, por ser mi segundo hogar durante este proceso y haberme dado la oportunidad de desarrollarme profesionalmente y lograr mis proyectos personales.

A MI FACULTAD: La Facultad de Ciencias Jurídicas y Sociales, que me brindo junto con cada uno de los catedráticos la oportunidad de adquirir conocimiento y sabiduría, instrucción y colaboración, para la culminación de mi profesionalización.

PRESENTACIÓN

La presente investigación se origina de la necesidad de legislar y dar certeza jurídica a la informática, ya que en la actualidad no existe el tipo penal adecuado para combatir los delitos cibernéticos, el ordenamiento jurídico vigente no cuenta con los tipos penales adecuados para poder contrarrestar este crimen que se ha convertido en un delito de tipo transnacional, pues puede ser cometido en cualquier parte del mundo.

El presente estudio se ha hecho bajo el método cualitativo, haciendo un análisis del derecho comparado, la legislación vigente en otros países que ya cuentan con los tipos penales para combatir esta clase de crímenes, y la legislación penal vigente en virtud de ser una rama del derecho penal.

No obstante, durante su desarrollo se ha hecho énfasis en el proceso penal guatemalteco, como ya mencionamos es una rama eminentemente penal, porque al no contar con una legislación acorde se hace muy vulnerable todo el sistema informático.

La legislación penal vigente en Guatemala, ya no esta acorde a la necesidad de combatir el crimen cibernético, por lo tanto para combatirlo se debe reformar el Código Procesal Penal guatemalteco y crear tipos penales específicos, para procesar penalmente a los responsables.

HIPÓTESIS

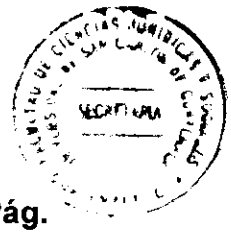
La informática es una ciencia joven pero de mucha importancia en las actividades del ser humano y es por ello la importancia de la creación de nuevas figuras delictivas que se deben incluir en nuestro ordenamiento jurídico.

Si el poder Legislativo creara normas acordes con el avance de la tecnología y el Ejecutivo aportara los recursos económicos necesarios para divulgar y concienciar a la población sobre este tema específico, el juez encargado de aplicar la justicia ante esta clase de delitos cibernéticos, no se vería imposibilitado de aplicar la norma puesto que si bien es cierto existe un capítulo que regula lo concerniente de una manera general, es importante que la norma sea mas específica para su aplicación.

Por lo que se puede afirmar: Se pueden combatir los delitos cibernéticos con la legislación actual en Guatemala, sobre esta base se puede decir que con la legislación actual no es posible enfrentar un flagelo que día con día se va convirtiendo en un delito transnacional, puesto que trasciende todas las fronteras patrias, la informática actualmente no tiene límites, y se va renovando constantemente, modernizando cada vez mas los mecanismos de la informática, por lo tanto los que cometen esta clase de delitos son personas que lo hacen desde cualquier lugar del mundo.

COMPROBACIÓN DE HIPÓTESIS

La informática es una ciencia joven pero de mucha importancia en las actividades del ser humano, y le legislación vigente en Guatemala, ya no es acorde a las necesidades y al combate del crimen cibernético, lo que conlleva la urgente necesidad de crear los tipos penales que tiendan a combatir el crimen organizado en la rama de la informática, además que implica que se ha convertido en un crimen transnacional, siendo el método cualitativo el más apropiado para nuestra comprobación de hipótesis puesto que se ha analizado la legislación de otros países con la de Guatemala, derivando que es necesario que el legislador tome en cuenta la magnitud que representa esta clase de delitos informáticos y lo que repercute en el ámbito penal.



ÍNDICE

Pág.

Pág.

CAPÍTULO III

Pág.

CAPÍTULO IV

INTRODUCCIÓN

Es importante hacer notar, que uno de los propósitos por el cual se ha elegido el tema es porque la legislación vigente en Guatemala ya no responde para combatir los crímenes cibernéticos, pues es un delito que trasciende fronteras, siendo que el que lo comete puede estar en cualquier país del mundo y su efecto delictuoso puede ser en Guatemala.

Uno de los objetivos generales de la investigación radica, en la necesidad de regular en el Código Penal los delitos informáticos, haciendo un análisis de las disposiciones legales guatemaltecas, y proponer reformas que tiendan a prevenir, combatir y sancionar los delitos cibernéticos.

Se pudo establecer que la hipótesis planteada se comprobó en la elaboración del informe final, en el sentido que la informática es una ciencia joven y que no existe en nuestra legislación tipos penales acordes para el combate del cibercrimen. El Organismo Legislativo es el que debe crear normas penales, el Organismo Ejecutivo es el encargado de dar los recursos necesarios y el Organismo Judicial, el encargado de aplicar los tipos penales y se sancione al o a los responsables.

Los delitos informáticos, están comprendidos por todos aquellos actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de

ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de computadoras y a través del mundo virtual del internet.

La naturaleza jurídica de esta clase de delitos, conforme a la metodología aplicada, en especial el método analítico y la técnica jurídica, ha sido planteada y se ha convertido en una labor realmente complicada para todos los tratadistas. Derivado de esta situación, es menester acudir a los postulados de dos escuelas del Derecho Penal, como lo es la Escuela Clásica y la Escuela Positiva. Según de León Velasco y De Mata Vela, la Escuela Clásica considera que el delito es un acontecimiento jurídico, una infracción a la ley del Estado, un choque a la actividad humana con la norma penal, es en esencia, un ente jurídico. Mientras que la Escuela Positiva concibe el delito como una realidad humana, como un fenómeno natural o social, como una acción humana resultante de la personalidad del delincuente.

La investigación está compuesta por cuatro capítulos, tratándose el primero del origen del delito informático, donde se hace un análisis histórico, como una comparación de la legislación de otros países; en el capítulo segundo se hace una reseña histórica de los delitos informáticos; en el tercero se trata de lo que es el proceso penal en Guatemala; y en el cuarto se refiere a algunos instrumentos internacionales en el ámbito de delitos informáticos, con lo cual se pretende aportar a nuestra investigación que es urgente hacer reformas a la ley penal.

CAPÍTULO I

1. Origen del delito informático

Los virus informáticos fueron los primeros delitos desde la aparición de los virus informáticos en el año de 1984 y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de internet. El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a internet. El "Grupo de Lyón" utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.

1.1. Que son los delitos informáticos

Son todos aquellos actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de computadoras y a través del mundo virtual del internet.

1.2. Naturaleza jurídica

La determinación de la naturaleza jurídica del delito se ha convertido en una labor realmente complicada para todos los tratadistas. Derivado de esta situación, es menester acudir a los postulados de dos escuelas del Derecho Penal, como lo es la Escuela Clásica y la Escuela Positiva. Según de León Velasco y De Mata Vela, la Escuela Clásica considera que el delito es un acontecimiento jurídico, una infracción a la ley del Estado, un choque a la actividad humana con la norma penal, es en esencia, un "ente jurídico". Mientras que la Escuela Positiva concibe el delito como una realidad humana, como un "fenómeno natural o social", como una acción humana resultante de la personalidad del delincuente.[1]

1.3. Historia de los delitos informáticos

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.[2]

---

[1]De León Velasco, Héctor Aníbal y José Francisco De Mata Vela. **Curso de derecho penal guatemalteco, parte general y parte especial**. Pág. 124-125.
[2]Téllez Valdés, Julio. **Derecho informático**. Pág.103-104.

"A Nivel internacional se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión delitos informáticos esté consignada en los Códigos Penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún".[3]

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales. En dicho estudio participaron varios juristas con el fin de lograr leyes penales que a nivel internacional puedan servir para combatir los delitos informáticos, siendo una de las juristas la Doctora María José Viega Rodríguez, escribana de la República de Uruguay.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos

[3]Callegari, Lidia. **Delitos informáticos y legislación en revista de la facultad de derecho y ciencias políticas de la universidad pontificia bolivariana**. Pág.115.

existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el principio de subsidiariedad.

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

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

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

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

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

"En este punto debe hacerse un punto y notar lo siguiente"

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

En términos genéricos se puede decir que los delitos informáticos son todas las operaciones ilícitas realizadas por medio de Internet y que su fin es destruir y dañar ordenadores, medios electrónicos y redes de Internet. Mas sin embargo mediante la informática se pueden cometer una serie de delitos tradicionales, como son el fraude, robo, chantaje, falsificación, malversación de caudales públicos, y todo por la complejidad de la informática.

Se pueden incluir una diversidad de crímenes, que se puede dividir en dos grupos:

a. Crímenes que tienen como objetivo redes de computadoras; ejemplo: instalación de Códigos, gusanos y archivos maliciosos, spam, ataque masivo a servidores de Internet y generación de virus.

b. Crímenes realizados por medio de ordenadores y de internet, ejemplo:

Espionaje, fraude, robo, pornografía infantil, pedofilia, chantaje, falsificación, etc.

1.4. Legislación en otros países

1.4.1. **Argentina.**

La ley vigente, sanciono el cuatro de junio de dos mil ocho la Ley veintiséis punto trescientos ochenta y ocho, que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso

ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

1.4.2. **Alemania.**

Para hacer frente a la delincuencia relacionado con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de mil novecientos ochenta y seis en la que se contemplan los siguientes delitos:

- Espionaje de datos.
- Estafa Informática.
- Falsificación de datos probatorios.
- Alteración de Datos.
- Sabotaje Informático.
- Utilización abusiva de cheques o tarjetas de crédito.

Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria. Alemania también cuenta con una Ley de protección de datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos". La presente ley protege los datos personales que fueren almacenados en registros

informatizados, modificados, cancelados o comunidades a partir de registros informatizados.

1.4.3. **Chile**. Cuenta con una ley relativa a delitos informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Artículo 3. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

1.4.4. **Estados Unidos.**

Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha acta define dos niveles para el tratamiento

de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten solo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión. En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos; específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo.

Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.

Tipos de delitos informáticos reconocidos por la organización de las naciones unidas:

I) Los fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

II) La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

III) La manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

IV) Fraude efectuado por manipulación informáticas de los procesos de cómputo.

V) Falsificaciones informáticas; cuando se alteran datos de los documentos en forma computarizada.

VI) Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

VII) Sabotaje informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII) Los virus; es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

IX) Los gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X) La bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

XI) Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

XII) Piratas informáticos o hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

XIII) Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos.

1.4.5. **México**.

La Ley Federal de Derechos de Autor y Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia del Fuero Federal.

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define

lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etc.

1.4.6. **Guatemala**.

En el capítulo VII del Código Penal Guatemalteco, Artículos 274 al 275 Bis, encontramos todo lo relacionado a los Delitos Informáticos, los cuales ya no son acordes a la realidad nacional, y es por ello la importancia de nuestra investigación.

Artículo 274. "Será sancionado con prisión de cuatro a seis años y multa de cincuenta mil a cien mil quetzales, quien realizare cualesquiera de los actos siguientes:

a) La atribución falsa de calidad de titular de un derecho de autor, de artista, intérprete o ejecutarse, de productor de fonograma o de un organismo de radiodifusión, independientemente de que los mismos se exploten económicamente o no.

b) La presentación, ejecución o audición pública o transmisión, comunicación, radiodifusión y/o distribución de una obra literaria o artística protegida, sin la autorización del titular del derecho, salvo los casos de excepción establecidos en las leyes de la materia.

c) La transmisión o la ejecución pública de un fonograma protegido, sin la autorización de un productor, salvo los casos de excepción establecidos en las leyes de la materia.

d) La reproducción o arrendamiento de ejemplares de obras literarias, artísticas o científicas protegidas, sin la autorización del titular.

e) La reproducción o arrendamiento de copias de fonogramas protegidos, sin la autorización de su productor.

f) La fijación, reproducción o transmisión de interpretaciones o ejecuciones protegidas, sin la autorización del artista.

g) La fijación, reproducción o retransmisión de emisiones protegidas, sin autorización del organismo de radiodifusión.

h) La impresión por el editor, de mayor número de ejemplares que el convenido con el titular del derecho.

i) Las adaptaciones, arreglos, limitaciones o alteraciones que impliquen una reproducción disimulada de una obra original.

j) La adaptación, traducción, modificación, transformación o incorporación de una obra ajena o parte de ella, sin autorización del titular.

k) La publicación de una obra ajena protegida, con el título cambiado o suprimido, o con el texto alterado, como si fuera de otro autor.

l) La importación, exportación, transporte, reproducción, distribución, comercialización, exhibición, venta u ofrecimiento para la venta de copias ilícitas de obras y fonogramas protegidos.

m) La distribución de ejemplares de una obra o fonograma protegido, por medio de la venta, el arrendamiento o cualquier otra modalidad de distribución, sin la autorización del titular del derecho".

La responsabilidad penal de los dependientes, comisionistas o cualquier otra persona que desempeñe una actividad laboral bajo remuneración o dependencia, será determinada de acuerdo a su participación en la comisión del hecho delictivo.

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 él".

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".

Violación a los derechos de propiedad industrial

Artículo 275. "Será sancionado con prisión de cuatro a seis años y multa de cincuenta mil a cien mil quetzales, quien realizare cualesquiera de los actos siguientes:

a) Fabricar o elaborar productos amparados por una patente de invención o por un registro de modelo de utilidad, sin consentimiento de su titular o sin la licencia respectiva.

b) Ofrecer en venta o poner en circulación productos amparados por una patente de invención o de modelo de utilidad, a sabiendas de que fueron fabricados o elaborados sin consentimiento del titular de la patente o sin licencia respectiva.

c) Utilizar procesos patentados sin consentimiento del titular de la patente o sin la licencia respectiva.

d) Ofrecer en venta o poner en circulación productos, que sean resultado de la utilización de procesos patentados, a sabiendas que fueron utilizados sin el consentimiento del titular de la patente o de quien tuviera una licencia de explotación.

e) Reproducir diseños industriales protegidos, sin consentimiento de su titular o sin la licencia respectiva.

f) Revelar a un tercero un secreto industrial que conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para un tercero o con el fin de causar un perjuicio a la persona que guarda el secreto.

g) Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarda o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarda el secreto.

h) Usar la información contenida en un secreto industrial que conozca por virtud de su trabajo, cargo, puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo guarda o de su usuario autorizado o que le haya sido revelado por un tercero, a sabiendas de que este no contaba para ello con el consentimiento de la persona que guarda el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarda el secreto industrial o su usuario autorizado".

Violación a los derechos marcarios

Artículo 275 BIS. "Será sancionado con prisión de cuatro a seis años y multa de cincuenta mil a cien mil quetzales, quien realizare cualquiera de los actos siguientes:

a) Usar en el comercio una marca registrada, o una copia servil o imitación fraudulenta de ella, en relación a productos o servicios iguales o similares a los que la marca se aplique.

b) Usar en el comercio un nombre comercial o un emblema protegidos.

c) Usar en el comercio, en relación con un producto o un servicio, una indicación geográfica falsa o susceptible de engañar al público sobre la procedencia de ese producto o servicio, o sobre la identidad del producto, fabricante o comerciante del producto o servicio.

d) Ofrecer en venta o poner en circulación productos a los que se aplica una marca registrada, después de haber alterado, sustituido o suprimido ésta, parcial o totalmente.

e) Continuar usando una marca no registrada parecida en grado de confusión a otra registrada, después de que se haya emitido resolución ordenando el cese total o parcialmente".

En Guatemala, existe la Ley para el reconocimiento de las comunicaciones y firmas electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, que regula todo lo relacionado al comercio electrónico, obliga a la creación de nuevas figuras delictivas o sea crear una ley especial para poder prevenir, sancionar y erradicar los delitos de naturaleza informática que pudieran afectar el objeto mismo de la ley de comercio electrónico, y todos aquellos actos ilícitos de naturaleza informática, y con ello cumplir con los convenios internacionales sobre la ciberdelincuencia, que fue suscrito en Budapest con fecha veintitrés de noviembre del año dos mil uno, que se considera como una ley modelo para la regulación de cibercrimen. En consecuencia para el desarrollo de la investigación debe respetarse la fisonomía peculiar de que se encuentra

investida esta materia: como el aspecto jurídico, atendiendo a la naturaleza de la investigación en cuanto a la propuesta de la regulación de los delitos informáticos en el Código Penal; y el científico, dada la forma en la cual se ha desarrollado el trabajo de investigación, desarrollando cada una de las etapas que comprende el método científico.

La ciberdelincuencia fue tema tratado en la Organización de las Naciones Unidas, en la Convención Budapest del veintitrés de noviembre del año dos mil uno.

CAPÍTULO II

2. Reseña histórica

El derecho constituye una materia en extremo cambiante, que evoluciona y se desarrolla de la mano con las transformaciones y necesidades de la sociedad. Los avances de la civilización, la globalización, los constantes descubrimientos son factores que influyen en la necesidad de regular por parte de las normas legales aspectos y bienes jurídicos que el Estado señala como merecedores de proteger de acuerdo al clamor de los tiempos. En ese sentido, los avances tecnológicos y dentro de estos los de orden informático determinan imperativamente necesidades de orden social, que impulsan la obligación de tutela estatal a través de la reforma o creación de leyes específicas.

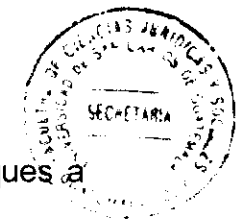
El derecho penal no constituye la excepción, y se ha visto en la necesidad de normar ámbitos de protección a bienes jurídicos tutelados que anteriormente no existían o no se consideraban merecedores de defensa estatal. En ese sentido se puede ubicar cronológicamente el siglo veinte, como el del origen y evolución de los delitos de carácter informático.

Las primeras conductas que tenían como finalidad el ataque a un sistema o equipo informático no tenían la cualidad de ser consideradas como delito, ya que el

principio de legalidad exige que para que una acción sea considerada como delictiva debe estar expresamente determinada como tal por el legislador, y ante la necesidad de ampliar el ámbito de protección a este tipo de bienes jurídicos, las legislaciones han regulado sanciones de orden penal a los responsables de este tipo de acciones.

Es válido afirmar que los ataques al programa o sistema operativo de un computador pueden ser considerados como las primeras conductas merecedoras de regulación y sanción de carácter penal. Debe reconocerse que una de las primeras acciones de este tipo se da a manera de juego, documentándose en el año de 1959 el caso de Robert Thomas Morris, Douglas McIlory y Víctor Vysottsky, tres programadores de la compañía Bell Computer quienes en una competencia idearon un sistema al que denominaron Corewar, consistiendo este en crear programas que paulatinamente disminuían la memoria de la computadora, ganando el mismo quien lograse la eliminación total de esta.

Uno de los primeros virus que afecta los sistemas informáticos aparece en el año de 1972, y se le denominó Creeper (enredadera en idioma inglés), que afectó a las computadoras de la compañía IBM e hizo necesaria la aparición del primer antivirus conocido como "cegadora". Posteriormente en el año 1980 el Arpanet, (sistema de comunicación vía computadoras usado por el departamento de



defensa de los Estados Unidos y precursor de Internet), experimentó ataques a través de un virus informático que necesitó de 3 días de trabajo para eliminarlo.

En el plano internacional al año de 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio para aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas de computadoras. Fruto de ello en el año 1986, se publica el documento titulado: "Delitos de informática análisis de la normativa jurídica" en el que se recopilan detalles de normas penales vigentes y propuestas de reforma de legislación en sus países miembros así como las conductas que era necesario sancionar penalmente, en lo que se denominó lista mínima.

En la actualidad las conductas se han diversificado y el grado de ataques cada vez han sido mayores y más originales; la jurisprudencia francesa registra el caso del empleado a cargo de los registros informáticos de una compañía, que programó su computadora de tal manera que se borraran todos sus archivos al momento que este fuera despedido, y el modo de activarlo consistía en que cuando su nombre se borrara de la nómina de pagos se desencadenaba el programa que borraba los registros.

Con respecto a la legislación guatemalteca, es en el año de 1996 que se regula los delitos informáticos entre los que se puede mencionar la destrucción de registros informáticos, alteración de programas y la reproducción de instrucciones o programas de computación entre otros.

2.1. Delitos informáticos

El término informática se obtiene de la transposición de las palabras información automática, que fue utilizado por primera vez en el idioma francés con las acepciones information automatique. La informática es definida en el Diccionario de la Real Academia de la Lengua Española como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. Ahora bien con respecto al delito informático Tiedemann ([4]) señala: "Con la expresión criminalidad mediante computadoras se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente dañosos y por eso penalizables en el futuro) realizados con el empleo de un equipo automático de procesamiento de datos".

Por su parte la Organización de las Naciones Unidas al referirse a la delincuencia informática lo hace de la siguiente manera: "A menudo, se le considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias

[4]Tiedemannn Klauss. **Poder económico y delito.** Pág. 122

tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos"

De estas definiciones se desprende que no solamente la propagación de virus u otros ataques a sistemas operativos de los ordenadores deben ser considerados como delitos informáticos, ya que se debe incluir dentro de estas todas aquellas acciones que atentan contra el bien jurídico merecedor de protección y que se valen o utilizan para su comisión de una computadora.

En ese sentido puede definir el delito informático como toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático, o a producir un resultado de daño en ésta o de los sistemas que la misma hace operar.

Como se podrá analizar, el ámbito de actuación en este tipo de conductas implica el ataque o intencionalidad de daño a un sistema operativo de la computadora, la intromisión o acceso a bases de datos o archivos que las mismas contengan, o bien la utilización de este aparato tecnológico y de comunicación como medio o instrumento para la realización de delitos.

2.2 Elementos del delito informático

El análisis de los ilícitos a través de la teoría del delito, diremos que el elemento descriptivo de los delitos lo sería la computadora, las bases de datos o registros informáticos o bien los bienes materiales e intelectuales afectados a través de un sistema informático u ordenador para citar algunos. Con respecto al elemento normativo Zaffaroni: señala: "aparecen cuando los tipos acuden a valoraciones jurídicas o éticas. Normalmente el tipo se vale de descripciones para individualizar pragmas, pero en ocasiones lo hace mediante estas remisiones a elementos de carácter valorativo"[5].

Debe entenderse entonces que dicho elemento se aprecia intelectualmente, en el caso en particular de los delitos informáticos es necesario auxiliarse de la informática u otra ciencia para comprenderlos, en ese sentido dentro de los elementos normativos de este tipo de ilícitos tenemos los daños producidos a los equipos, a los programas o bases de datos, la pérdida patrimonial, la indemnidad sexual, etc.

2.3. Bien jurídico tutelado

En el entendido que el bien jurídico tutelado lo constituyen todos aquellos derechos, valores o atributos de la persona que el Estado encuentra merecedores

[5]Zaffaroni. Eugenio Raúl. **Derecho penal parte general.** Pág. 461

de protección a través del Derecho Penal, se puede afirmar que en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro.

Por un lado las acciones que van dirigidas al sabotaje, el daño, la destrucción o pérdida de equipos de computación afectan, lesionan o ponen en peligro el bien jurídico patrimonio, Por otro, los delitos que se sirven o utilizan de un equipo informático para su realización pueden de igual manera afectar diversos bienes, como lo serían la indemnidad sexual (caso de la pornografía infantil), la privacidad o el mismo patrimonio en los casos de fraudes informáticos cometidos por internet.

También debe tomarse en cuenta que el uso de ordenadores para la reproducción no autorizada de libros, películas música, etc., afecta valores de propiedad intelectual pero implícitamente éstas acciones tienen una motivación económica por lo que a su vez redundan en la afectación al bien jurídico patrimonio. Es por eso que al hablar de delitos informáticos es válida la afirmación que los mismos afectan una diversidad de bienes legalmente tutelados por lo que puede considerarse pluriofensivo.

2.4. Clases de delitos informáticos

Al definir los delitos informáticos se hacía referencia a acciones antijurídicas con una finalidad que podría ser el ataque, daño o acceso no autorizado a un aparato

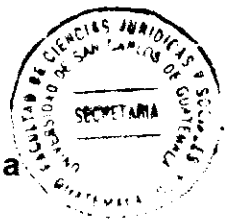
o sistema de computadoras o sus programas, o bien se sirve de éstas como medio operativo para realizar actos ilícitos; además de acuerdo a la real afectación al bien jurídico tutelado estos pueden ser dirigidos a vulnerar el patrimonio, propiedad intelectual o bien la privacidad o indemnidad de las personas. Estas reflexiones sirven de base para proponer por parte del autor la siguiente clasificación de los delitos informáticos, distinguiéndose entonces dos tipos a saber:

a) Delitos Informáticos contra el patrimonio y la propiedad intelectual.

b) Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual.

2.4.1. Delitos informáticos contra el patrimonio y la propiedad intelectual;

Se pueden citar dentro de esta clasificación delitos como: La copia ilegal de software, películas y música; defraudaciones a través de publicidad engañosa; fraudes cometidos por medio del acceso y manipulación a sistemas informáticos bancarios o financieros; sabotaje a sistemas informáticos; uso no autorizado de sistemas informáticos ajenos; espionaje informático; falsificación de documentos por medio de la computadora.



2.4.2. Delitos informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual;

En este grupo se clasifican las acciones u omisiones en que incurre el sujeto activo y que lesionan o ponen el bien jurídico tutelado privacidad, entendida ésta, como el ámbito de la vida privada y del cual se tiene derecho a proteger de cualquier intromisión. Al respecto Bustamante señala: "Los delitos informáticos contra la privacidad constituyen un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos"[6].

En esta clasificación se aprecian las siguientes conductas:

2.4.3. Violación a la privacidad de la información personal o a las comunicaciones;

2.4.4. La revelación indebida de información personal;

2.4.5. Pornografía infantil a través de internet;

2.5. De la actividad de hackers, crackers y los delitos informáticos

La palabra hacker viene del inglés hack que equivale a cortar a tajos o derribar, y se utiliza generalmente para distinguir a cierto sector de expertos en redes de computadoras, informática, programas y los sistemas relacionados a estos. Se

[6] Bustamante Alcina, Jorge. **La informática y la protección del secreto de la vida privada**. Pág. 826

afirma que un hacker es un especialista, alguien que ha llegado a dominar de tal manera el ámbito informático que está por encima de la generalidad. Regularmente el término hacker se asocia con el de pirata informático, sin embargo para estos grupos sus actividades no son constitutivas de los hechos delictivos que se atribuyen a los piratas.

Un cracker como ya se ha mencionado se sirve de sus capacidades y conocimientos para su beneficio personal, acciones como violar la seguridad de un sistema informático, propagar virus, boicotear redes sociales, etc. Por consiguiente muchas de sus conductas recaen en el ámbito de bienes jurídicos que el derecho penal busca tutelar. El término cracker también viene del inglés en este caso de la palabra crack que puede ser traducida como rajar, crujir, romper.

2.6. Delitos informáticos y la legislación guatemalteca

En la década de los años ochenta en nuestro país se empieza a acentuar la utilización de las computadoras tanto en el ámbito comercial como gubernamental, aparecen las primeras computadoras personales así como carreras específicas en la materia tanto a nivel vocacional como universitario. Para inicios de la década siguiente se dan los primeros pasos sobre todo en materia investigativa de las universidades para la comunicación global a través del correo electrónico e internet.

La utilización de nuevas tecnologías y las relaciones que de las mismas dependían, los fenómenos sociales con ellos relacionadas y dentro de estos la vulneración a nuevos bienes jurídicos merecedores de tutela, así como innovadoras modalidades de comisión de hechos delictivos hizo necesaria en esa década reformas al Código Penal a efecto de prohibir y sancionar las conductas relacionadas.

De esa forma el Congreso de la República introduce modificaciones a la Ley Sustantiva Penal a través del Decreto 33-96 publicado en fecha 21 de Junio de 1996. En la normativa ya referida como motivación de la misma se expone: "Que los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado". En ese sentido en materia de delitos informáticos se regulan los tipos siguientes:

a) Artículo 274 "A" Destrucción de registros informáticos

b) Artículo 274 "B" Alteración de programas

c) Artículo 274 "C" Reproducción de instrucciones o programas de computación

d) Artículo 274 "D" Registros prohibidos.

e) Artículo 274 "E" Manipulación de información

f) Artículo 274 "F" Uso de información

g) Artículo 274 "G" Programas destructivos

No obstante no estar clasificadas específicamente dentro de los delitos informáticos el Código Penal señala otras conductas de las que podrían incluirse dentro de este tipo, (por qué se sirven de un computador para realizarlas o bien van dirigidas a producir daños en el mismo), de las cuales enumeraremos a continuación:

a) Violación a derechos de autor contenida en el Artículo 274 del Código Penal.

b) Violación a los derechos de propiedad industrial contenida en el Artículo 275 del Código Penal.

c) Pánico financiero contenido en el Artículo 342 "B" del Código Penal.

d) Ingreso a espectáculos y distribución de material pornográfico a personas menores de edad contenida en el Artículo 189 del Código Penal.

e) Violación a la intimidad sexual contenida en el Artículo 190 del Código Penal.

f) Producción de pornografía de personas menores de edad contenida en el Artículo 194 del Código Penal.

g) Comercialización o difusión de pornografía de personas menores de edad contenida en el Artículo 195 Bis

h) Posesión de material pornográfico de personas menores de edad contenido en el Artículo 195 ter.

j) Comercialización de datos personales ilícito penal contenido en la Ley de Acceso a la Información Pública, Artículo 64.

k) Alteración fraudulenta contenido en el Artículo 275 Bis del Código Penal.

2.7. Bienes jurídicos tutelados en los delitos informáticos de la legislación guatemalteca y el ejercicio de la defensa técnica

Al referirnos a las generalidades de los delitos informáticos se hizo mención con respecto a la diversidad de bienes jurídicos tutelados que son por ellos afectados. Los ilícitos antes citados lesionan o ponen en peligro los distintos valores materiales o inmateriales que el Estado considera merecedores de protección. La importancia que para el defensor público o para el profesional del derecho en general implica la claridad en su comprensión radica en que le proveerá de herramientas de análisis para determinar en el caso concreto: primero: Si se está ante la comisión de un hecho delictivo, segundo: Su adecuada tipificación o calificación jurídica y en su caso si existe o no una apropiada estimación de que existe una real afectación o puesta en peligro al bien jurídico tutelado y tercero: Si la investigación que fundamenta una persecución penal es la idónea y pertinente. Esto con el propósito de proveer de una defensa efectiva y eficaz a nuestro patrocinado.

Por lo anterior se propone para efectos del análisis la agrupación de los delitos informáticos de acuerdo a la consideración de afectación o puesta en peligro de determinado bien jurídico tutelado, de igual manera se generan ideas generales con respecto a la obligación de sustento de los medios de investigación que con una imputación de este tipo debería de realizar el ente investigador, así como criterios básicos de la imputación sobre casos concretos, de la manera siguiente:

2.8. Delitos informáticos del Código Penal que afectan el patrimonio y la propiedad intelectual.

El patrimonio es definido por Manuel Ossorio de la siguiente manera: "representa una universalidad constituida por el conjunto de derechos y obligaciones que corresponden a una persona y que pueden ser apreciables en dinero." Cuando un ilícito lesiona o pone en peligro los valores tangibles o intangibles que pertenecen a una persona individual o colectiva se clasifica dentro de los delitos patrimoniales, en el caso de afectación o utilización de sistemas informáticos dentro de las conductas que el legislador guatemalteco ha encontrado merecedoras de protección tenemos las siguientes:

2.8.1. Violación a derechos de autor.

Las obras producto del intelecto y los derechos sobre estas pueden encontrar vulneración a través del uso de las computadoras ya sea para reproducirlas,

atribuirse falsamente su autoría, modificarlas o usarlas sin pagar los respectivos derechos. En la práctica se puede observar que la reproducción de discos compactos de música y películas constituye una actividad por demás lucrativa. La ley sustantiva penal determina en el Artículo 274 que comete esta acción delictiva quien:

- Identifique falsamente la calidad de titular de un derecho de autor, artista intérprete o ejecutante, productor de fonogramas o un organismo de radiodifusión.

- La reproducción de una obra, interpretación o ejecución, fonograma o difusión sin la autorización del autor titular del derecho correspondiente.

- La adaptación, arreglo o transformación de todo o parte de una obra protegida sin la autorización del autor o del titular del derecho.

- La comunicación al público por cualquier medio o proceso de una obra protegida o de un fonograma sin la autorización del titular del derecho correspondiente.

- La distribución no autorizada de reproducciones de todo o parte de una obra o fonograma por medio de su venta, arrendamiento de largo plazo, arrendamiento, arrendamiento con opción a compre, préstamo o cualquier otra modalidad.

- La fijación, reproducción o retransmisión de una difusión transmitida por satélite, radio, hilo o cable, fibra óptica o cualquier otro medio sin la autorización del titular del derecho.

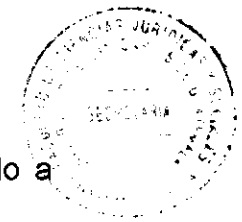
- Manufacture, ensamble, modifique, importe, exporte, venda, arrende o de cualquier forma distribuya un dispositivo o sistema tangible o intangible, sabiendo o teniendo razón para saber que el dispositivo o sistema sirve o asiste principalmente para decodificar una señal de satélite codificada, que tenga un programa sin la autorización del distribuidor legal de dicha señal, o la recepción y distribución intencionada de una señal que lleva un programa que se originó como señal satelital codificada sabiendo que fue decodificada sin la autorización del distribuidor legal de la señal.

- Con respecto a las medidas tecnológicas efectivas lo siguiente: acto que eluda o intente eludir una medida tecnológica efectiva que impida o controle el acceso o el uso no autorizado a toda obra, interpretación o ejecución o fonograma protegido.

2.8.2. Destrucción de registros informáticos

Realiza esta figura delictiva quien destruya, borre o de cualquier modo inutilice registros informáticos tanto públicos como privados; según lo normado en el Artículo 274 "A" del Código Penal se infiere que la intención del legislador recae en la necesidad de proteger los archivos, bases de datos y en general todo registro informático que se encuentre en un ordenador tanto en la esfera gubernamental pública como la empresarial o personal.

La doctrina se refiere a este delito como Sabotaje Informático y describe su realización desde dos puntos de vista, el primero de ellos la destrucción o daño



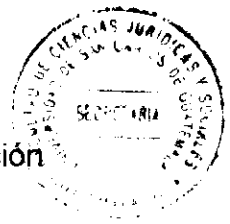
físico a la computadora que implica obviamente su inutilización y el segundo a través de las conductas dirigidas a causar "daños lógicos".

Las mismas consideraciones anteriormente referidas se aplican a los delitos de Alteración de Programas y Programas Destructivos contenidos en los Artículos 274 "A" y "G" del Código Penal que buscan proteger de la alteración, borrado o inutilización de las instrucciones o programas que utilizan las computadoras así como de la distribución o puesta en circulación de programas o instrucciones destructivas que causen un daño a los programas o equipos.

2.8.3. Reproducción de instrucciones o programas de comunicación

Comete este delito conforme al Artículo 274 "C" del Código Penal el que sin autorización del autor copia o de cualquier modo reproduzca las instrucciones o programas de computación. De estrecha relación con respecto al delito de violación a los derechos de autor y dirigida específicamente a su protección en el ámbito informático, esta figura delictiva busca proteger los bienes jurídicos tutelados de carácter patrimonial, así como el reconocimiento de la calidad de autor o inventor de instrucciones o programas informáticos.

La imputación de este ilícito penal debe entonces ir dirigida a la construcción histórica de un hecho y lógicamente su comprobación a través de los medios de investigación y en su momento de prueba idóneos sobre los siguientes aspectos fácticos como mínimo:



a) Que el imputado copió o reprodujo instrucciones o programas de computación

b) Que dichas acciones las realizó sin el consentimiento del autor de la instrucción o programa en ese sentido se excluye que la conducta sea ilícita cuando recae sobre un programa de acceso libre o gratuito.

c) Dado que uno de los bienes jurídicos tutelados lo constituye el patrimonio del autor debería analizarse si es menester comprobar que ha existido un desmedro o pérdida de este en el autor de la instrucción o programa.

Dado que la imputación debe referirse a modo tiempo y lugar es lógico suponer que el medio de investigación y de prueba debe hacer referencia directa a la fecha en que se copiaron o reprodujeron los programas, el lugar en que se encontraba el posible autor del delito, así como los medios empleados para esto generalmente es necesaria la participación de un perito en la materia a efecto de demostrar estos extremos.

2.8.4. Manipulación de información

Se perfecciona esta conducta ilícita cuando se utilizan registros informáticos o programas de computación para 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. Se aprecian entonces de los elementos tipo de la figura los siguientes supuestos:

a) La utilización de un registro o programa para cambiar la información que se requiere a efecto cumplir con los requisitos necesarios de una actividad comercial.

b) Las mismas acciones con el objeto de incumplir una obligación con respecto al Estado y,

c) El cambio de estados contables o situación patrimonial de una persona física o jurídica.

Se entiende con respecto al sujeto activo de este ilícito que podría estar constituido por un empleado, el propietario de una empresa o el particular que distorsiona o falsea la información con un propósito en particular que podría ser aparentar que una empresa cumple con los presupuestos y requisitos legales de operación, eludir una obligación en relación al Estado o bien modificar la realidad con respecto a la situación patrimonial y/o estados contables de una persona individual o jurídica.

El sujeto pasivo del delito analizado lo constituye entonces el particular o bien el Estado que encuentra un desmedro en su patrimonio o bien en los tributos como consecuencia de estas acciones. Aunque cabe también analizar que de acuerdo a como se encuentra conformada esta figura delictiva no se exige que exista una efectiva lesión al bien jurídico tutelado si no que basta la simple acción en sus diferentes modalidades para que el delito se perfeccione. La teoría del delito se

refiere a este tipo de ilícitos clasificándolos dentro de los que se conocen como de "mera actividad" ([7])

2.8.5. Registros prohibidos

Según lo normado en el Artículo 274 "D" del Código Penal esta conducta se perfecciona por la persona que crea un banco de datos o un registro informático con datos que pudieran afectar la intimidad de las personas. A manera de ejemplo se puede citar el caso de quien crea una página, un blog un foro de opinión en la red y en ella registra información íntima, privada o confidencial, en concreto información que afecte el bien jurídico la intimidad personal.

De su análisis se debe tomar en cuenta que los datos de registro deben ser íntimos y de esa cuenta vale la pena profundizar sobre el ámbito de lo que debe entenderse como tal para diferenciarlo de lo privado. De igual manera debe valorarse el extremo que si los datos son recopilados o recabados de archivos o registros públicos no podría tipificarse esta conducta delictiva.

Por último ha de considerarse que la norma busca desarrollar la protección constitucional referente al derecho a la dignidad, la integridad y la intimidad (Artículos 3 y 4). En ese sentido debería valorarse que la acusación y los medios de investigación que la sustentan establezcan una relación de causalidad entre la creación del registro informático o banco de datos y el grado de afectación del bien jurídico tutelado intimidad de las personas.

---

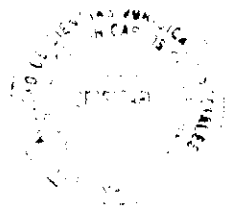
[7] Girón, Pallés. **Módulo teoría del delito**. Pág. 34.

2.8.6. Delito de pánico financiero

El delito de pánico financiero tipificado conforme al Artículo 342 "B" del Código Penal está ubicado en la legislación dentro de los ilícitos que atentan contra el bien jurídico economía nacional en primer orden, ya que su comisión implica un ataque directo al sistema bancario en términos generales que repercute en el acontecer económico y financiero del país. Sin embargo como se podrá apreciar sus efectos también atentan directamente contra el patrimonio de los particulares; podría pensarse a manera de ejemplo que el pánico financiero provoque lo que se conoce como una "corrida bancaria" que es el acto por el cual los depositantes acuden en masa a la institución bancaria a retirar sus ahorros (generalmente como consecuencia de un rumor cierto o falso de la falta de liquidez del banco,) con lo cual esta se descapitaliza y obviamente no puede cubrir con las obligaciones para con todos sus clientes.

2.8.7. Comercialización de datos personales

Según lo regulado en el Artículo 64 del Decreto 57-2008 del Congreso de la República, Ley de Acceso a la Información Pública; quien comercializa o distribuya por cualquier medio archivo de información o datos personales, datos sensibles o personales sensibles protegidos por dicha ley comete esta acción delictiva. En ese sentido el espíritu de la norma va dirigido a la prohibición de venta o distribución de registros o archivos que contengan referencias o detalles personales o considerados sensibles.



CAPÍTULO III

3. El proceso penal guatemalteco

Es el procedimiento de carácter jurídico que se lleva a cabo para que un órgano estatal aplique una ley de tipo penal en un caso específico. Las acciones que se desarrollan en el marco de estos procesos están orientadas a la investigación, la identificación y el eventual castigo de aquellas conductas que están tipificadas como delitos por el Código Penal.

La finalidad de los procesos penales, es última instancia, es la conservación del orden público. Las características de su desarrollo dependen de cada jurisdicción. Lo habitual es que un proceso penal se inicie con una instrucción preparatoria que consiste en la etapa investigativa. En esta parte del proceso, se recogen las pruebas que sustentarán la acusación contra una persona.

Algunos autores definen el derecho procesal penal de la siguiente manera:

Hugo Alsina: "El derecho procesal penal es el conjunto de normas que regulan la actividad jurisdiccional del Estado para la aplicación de las leyes de fondo, y su estudio comprende: la organización del poder judicial y la determinación de la competencia de los funcionarios que lo integran y la actuación del juez y las partes en la sustanciación del proceso"[8]

[8] Alsina, Hugo. **Tratado teórico-práctico del derecho procesal civil y comercial.** Pág. 37.

Alberto Binder: "Conjunto de actos realizados por determinados sujetos (jueces, fiscales, defensores, imputados, etc.) con el fin de comprobar la existencia de los presupuestos que habilitan la imposición de una pena y, en el caso de que tal existencia se compruebe, establecer la cantidad, calidad y modalidades de la sanción".[9]

3.1. Sistemas procesales

3.1.1. Formas del proceso penal

Para el estudio de la forma del proceso penal tenemos que atender a la historia y distinguir ésta de los principios rectores del proceso con independencia de la forma procesal adoptada. Históricamente y en el derecho comparado los sistemas procesales que destacan son: el acusatorio, el inquisitivo y el mixto.

Se dice que cuando las funciones de acusar, defender y decidir son encomendadas a tres órganos independientes, un acusador, un defensor y un juez, la forma del proceso es acusatorio. Si las tres funciones anteriores se reúnen en un solo órgano, el juez, la forma del proceso es inquisitiva.

Del estudio de las características propias de los sistemas absolutos que se constituyen por los dos primeros estaremos en condiciones de aclarar la naturaleza del sistema mixto que como corolario es el más admitido en la actualidad.

---

[9]Binder, Alberto. **Introducción al derecho procesal penal.** Pág.49

3.1.2. El proceso penal

3.1.2.1. Sistema acusatorio

En este sistema, el juez, ni aun teniendo conocimiento de la comisión de un delito, puede proceder de oficio y perseguir al delincuente. Es necesario que el ofendido presente acusación y solo entonces el juzgador podrá citar u obligar a comparecer al supuesto delincuente a su presencia; es entonces cuando se traba la Litis en forma oral y las partes alegan lo concerniente a la acusación y a la defensa, siendo oídos los testigos y presentadas las pruebas consideradas oportunas a efecto de hacer valer sus derechos.

Las ventajas y defectos de este sistema saltan a la vista. En primer lugar el acusado casi no se ve envuelto en acusaciones falsas y los medios de defensa que se le otorgan son equitativos e iguales a los de la acusación.

Por otra parte, bastará que el ofendido ignore la persona del ofensor para que el delito no pueda perseguirse. Es de destacar que si bien el ofendido no puede remitir la pena impuesta al ofensor, su perdón es eficaz si se abstiene de acusar. El juez se ve imposibilitado de producir pruebas, por lo que la posibilidad de castigar al supuesto infractor se reduce a la capacidad del acusador en la producción de las mismas.

El proceso acusatorio que observa principalmente las garantías del acusador, se caracteriza por la separación de las tres funciones básicas de acusar, defender y juzgar; toma relevancia la libertad de la defensa y libre apreciación de la prueba,

pocas facultades del juez, inapenabilidad de la sentencia porque ésta no está fundada y especialmente por constituir un sistema oral, público y contradictorio.

3.1.2.2. Sistema inquisitivo

Los defectos del sistema acusatorio llevó a los legisladores a la adopción de un sistema nuevo; se empezó por establecer junto al proceso acusatorio, un proceso judicial ex oficio, para los casos de flagrancia. En éstos, el juez iniciaba de oficio el proceso prescindiendo de acusador y en virtud del propio impulso oficial dirigía el proceso y dictaba sentencia.

Las ventajas de este sistema provocaron que fuera aplicado no solo a los delitos in fraganti sino se hizo extensivo a todos los delitos; se buscaba defender más los intereses sociales con el secreto; este estaba orientado a impedir que el delincuente desapareciera las pruebas del hecho punible y como el proceso se desarrollaba en varios actos, se sustituyó la oralidad por la escritura lo que impidió la inmediación y la contradicción procesal; se implementó el sistema de pruebas legales (tasadas) y la confesión como prueba reina, lo que trajo como resultado el empleo de la tortura; por las características propias de este sistema se abrió la posibilidad de apelar las sentencias, tarea que se tornaba por demás fatigosa tomando en cuenta que los fallos del juzgador no eran motivados.

El proceso inquisitivo se convirtió muchas veces en un arma mortal contra los enemigos políticos o sociales por la concentración de su ejercicio en manos de la

clase privilegiada. No olvidemos que la función de acusar, defender y decidir estaba concentrada en una sola persona u órgano.

3.1.2.3. Sistema mixto

Con la intención de subsanar los defectos de los sistemas absolutos, surgió, en Francia, el sistema mixto, el cual adoptan todos los ordenamientos positivos. Este sistema busca reunir las bondades de los sistemas anteriores buscando el beneficio social y del imputado. Se caracteriza por la división que hace del proceso; una fase de instrucción en donde predomina la forma inquisitiva, el secreto, la escritura y el impulso oficial; y otra fase llamada de plenario o del juicio en donde rigen los principios del sistema acusatorio y prevalece la publicidad, oralidad, libre apreciación de la prueba, concentración contradicción procesal.

Para hacer viable el sistema se crea la figura del acusador público y para garantizar la imparcialidad del juicio y de la sentencia, el tribunal que juzga y aplica la pena no interviene en la fase de instrucción.

En nuestro Código Procesal Penal anterior destacaba la oralidad toda vez que se utilizaba la palabra como vehículo conductor de la actividad procesal en la segunda etapa del proceso, sin menoscabo de las constancias escritas que por disposición de la ley debían recoger las incidencias del mismo.

3.2. Partes y sujetos procesales

Fenech, refiere que las partes en sentido procesal es "Persona rem in iudiciumdeducens, de un lado, y de otro, is contra quem res in iudiciumdeducitur. Esto es, son partes la persona que pide y aquella frente a quien se pide al titular

del órgano jurisdiccional la actuación de la pretensión penal y la de resarcimiento, en su caso."[10]

3.2.1. El juez

Jorge R. Moras Mom: "Juez penal es el representante del poder judicial para el ejercicio de la función penal, esto es la potestad estatal de aplicar el derecho objetivo a casos concretos. Actúa de forma unipersonal o colegiada, en juzgados o en tribunales o cámaras. Se separa del juzgamiento (juicio) en instancia única. O sea lo hace todo junto ante el juez".[11]

3.2.2. El Ministerio Público

Guillermo Cabanellas: "La institución y el órgano encargado de cooperar en la administración de justicia, velando por el interés del Estado, de la sociedad y los particulares mediante el ejercicio de las acciones pertinentes, haciendo observar las leyes y promoviendo la investigación y represión de los delitos".[12]

El Artículo 1°. Del Decreto 40-94 del Congreso de la República de Guatemala, Ley Orgánica del Ministerio Público establece: "El Ministerio Público es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública, además de velar por el estricto cumplimiento de las leyes del país. En el ejercicio de sus función, el Ministerio Público perseguirá la realización de la justicia y actuará con objetividad,

---

[10]Frenech, Miguel. **Derecho procesal penal.** Pág. 131

[11]Moras Mom, Jorge R. **Manual de derecho procesal penal.** Pág. 43.

12Cabanellas, Guillermo. **Diccionario enciclopédico de derecho usual.** Pág. 424

imparcialidad y con apego al principio de legalidad, en los términos que la ley establece."

El querellante

Jorge R. Moras Mom: "Es un sujeto privado acusador que, asumiendo voluntariamente el ejercicio de la acción penal emergente de un delito cometido en su contra en forma directa, impulsa el proceso, proporciona elementos de convicción, argumenta sobre ellos y recurre de las resoluciones en la medida que le concede la ley".[13]

Nuestro Código Procesal Penal acoge la figura del querellante bajo distintas denominaciones, así:

3.2.4. Querellante adhesivo

- El querellante adhesivo individual. Art. 116 del Código Procesal Penal.
- Querellante adhesivo colectivo. Las asociaciones de ciudadanos pueden constituirse en querellantes (simples) o en querellantes adhesivos en los casos relativos a violaciones de derechos humanos a condición de que los sujetos activos sean funcionarios o empleados públicos y que éstos directamente fueren responsables de tales violaciones o bien con ocasión o en el ejercicio de sus funciones o cuando se trate de funcionarios públicos que abusen de sus cargos.

13 **Ibid**. Pág. 46

Estos sujetos procesales no pueden ejercer con entera autonomía sus pretensiones dentro del proceso penal debido al principio de oficialidad; es decir, intervienen como terceros coadyuvantes del Ministerio Público. Vale señalar, van de alguna manera "detrás" de las acciones del ente oficial. No obstante, una vez admitido en el proceso, pueden intervenir en todas sus fases hasta que se dicte la sentencia definitiva.

- Querellante exclusivo. Es el titular del ejercicio de la acción penal en los casos en que la persecución penal es de carácter privado. Se rige por las reglas relativas a los juicios por delitos de acción privada. Al respecto el Artículo 122 del Código Procesal Penal establece: "Querellante exclusivo. Cuando, conforme a la ley, la persecución fuese privada, actuará como querellante la persona que sea titular del ejercicio de la acción."

3.2.5. El actor civil

Jorge R. Moras Mom: "Es un sujeto procesal que dentro del proceso penal juega su rol accionario relacionado con el objeto de este, como causa de obligación, pero limitado al campo civil reparatorio e indemnizatorio".[14]

14 **Ibid**. Pág. 49

La calidad de actor civil en el proceso penal solamente puede ser invocada por quien ostenta la calidad de damnificado por el hecho punible, también puede invocarse por quien comparece a título de heredero del damnificado o como mandatario judicial o representante legal del mismo. En los casos en que el Estado sea el damnificado tal calidad recae en la Procuraduría General de la Nación.

3.2.6. El imputado

Carlos Creus: "El imputado es toda persona de existencia física que es indicada, en un acto del proceso, como partícipe en el hecho que se investiga, o se va a investigar, nominándola o individualizándola de otro modo en los actos iniciales o disponiendo contra ella medidas de coerción (por ejemplo, detención, citación)".[15]

Señala el Artículo 70 del Código Procesal Penal que "Se denominará sindicado, imputado, procesado o acusado a toda persona a quien se le señale de haber cometido un hecho delictuoso, y condenado a aquel sobre quien haya recaído una sentencia condenatoria firme."

---

15 Creus, Carlos. **Derecho procesal penal**. Pág. 267

3.2.7. El tercero civilmente demandado

Alfredo Vélez Mariconde: "Las personas que responden por el imputado del daño causado directamente por el delito, en virtud de la ley civil, y no a consecuencia de un contrato, es decir, a la responsabilidad por el hecho ajeno derivado de una presunción legal de culpa, in vigilando o in negligendo".

3.2.8. El abogado defensor

Jorge Claría Olmedo: "Todo profesional del derecho que pone al servicio de quien tienen intereses comprometidos en un proceso, su actividad profesional y sus conocimientos jurídicos".[16]

Nuestro Código Procesal Penal en su Artículo 71, primer párrafo; "Los derechos que la constitución y este Código otorgan al imputado, puede hacerlos valer por sí o por medio de su defensor, desde el primer acto del procedimiento dirigido en su contra hasta su finalización".

3.3. Fases del proceso

3.3.1. Procedimiento preparatorio

Alberto Binder: "Consiste en un conjunto de actos fundamentalmente de investigación orientados a determinar si existen razones para someter a una

16 Claria Olmedo, Jorge. **Derecho procesal penal.** Pág. 127

persona a juicio. El pedido del fiscal, consistente en que se inicie juicio respecto de una persona determinada y por un hecho determinado, se denomina acusación".[17]

El Código Procesal Penal en su Artículo 309, primer párrafo, refiriéndose al objeto de la investigación, establece que "en la investigación de la verdad, el Ministerio Público deberá practicar todas las diligencias pertinentes y útiles para determinar la existencia del hecho, con todas las circunstancias de importancia para la ley penal. Asimismo, deberá establecer quiénes son los partícipes, procurando su identificación y el conocimiento de las circunstancias personales que sirvan para valorar su responsabilidad o influyan en su punibilidad. Verificará también el daño causado por el delito, aun cuando no se haya ejercido la acción civil".

Podemos indicar entonces, que la finalidad del procedimiento preparatorio es conjuntar los elementos del juicio indispensables para acusar durante el desarrollo del proceso a la persona debidamente individualizada como autor del delito, ya que cuando sea manifestado que el hecho no es punible o cuando no se pueda proceder, el órgano encargado de la persecución penal debe solicitar al juez contralor de la instrucción el archivo de las diligencias practicadas, evitando a los que resulten inocentes los inconvenientes de verse sujetos a un proceso penal.

17Binder, Alberto. **Introducción al derecho procesal penal.** Pág. 213

3.3.2. Fase intermedia

César Barrientos Pellecer: "La etapa intermedia es de naturaleza crítica; su función es la de evaluar y decidir judicialmente sobre las conclusiones planteadas por el Ministerio Público con motivo de la investigación preparatoria. No hay pase automático del procedimiento preparatorio al debate, ya que para evitar abusos o la salida indebida de casos del sistema penal se establece este procedimiento filtro".[18]

Se establece en el párrafo segundo del Artículo 332 del Código Procesal Penal que "la etapa intermedia tiene por objeto que el juez evalúe si existe o no fundamento para someter a una persona a juicio oral y público, por la probabilidad de su participación en un hecho delictivo o para verificar la fundamentación de las otras solicitudes del Ministerio Público."

Podemos establecer que la función esencial del procedimiento intermedio consiste en la determinación jurisdiccional sobre la procedencia de la solicitud planteada por el Ministerio Público. Si este acuso, el juez revisa si se dan los presupuestos para llevar a juicio oral y público a una persona, decide si de la investigación

18Barrientos Pellecer, César. **Código procesal penal.** Pág. 65

practicada se refiere la existencia del delito señalado en la acusación y si dichos elementos de prueba apuntan a presumir la responsabilidad criminal del acusado.

3.3.3. El juicio

César Barrientos Pellecer: "Es la etapa plena y principal del proceso porque en ella se produce el encuentro personal de los sujetos procesales y de los órganos de prueba; se comprueban y valoran los hechos y se resuelve, como resultado del contradictorio, el conflicto penal."[19]

El Artículo 356 del Código Procesal Penal establece que "el debate será público; pero esta publicidad tiene algunas excepciones cuando a juicio del tribunal concurran razones para realizarlo total o parcialmente a puertas cerradas".

3.4. Impugnaciones

Los recursos o impugnaciones son los medios procesales a través de los cuales las partes solicitan la modificación de una resolución judicial, que consideren injusta o ilegal ante el juzgado o tribunal que dictó la resolución o ante uno superior. Tiene como objetivo corregir errores de los jueces o tribunales y unifica la

19 **Ibid.** Pág. 67

jurisprudencia o la interpretación única de la ley, con el fin de dotar de seguridad jurídica.

La fase de impugnaciones esta constituida de los medios legales mediante los cuales las partes pueden oponerse o manifestar su inconformidad con las resoluciones dictadas durante el desarrollo del proceso penal, cuando sean contrarias a sus intereses y pueden ser presentados ante el mismo o el tribunal de mayor jerarquía con el fin de que revoque o modifique la resolución de que se trate, por medio del examen de la decisión judicial. Según lo estipulado por nuestra legislación, para que proceda plantear los medios de impugnación, en contra de las resoluciones emanadas de un órgano jurisdiccional, se debe observar ciertas condiciones entre las que podemos mencionar: a) Ser el agraviado quien hace uso de uno de los medios de impugnación, expresando los motivos que le afecta; b) se debe de cumplir con los requisitos de forma establecidos y plantearlos dentro de los plazos legales; y c) Determinar que la resolución sea impugnable.

Entre los medios de impugnación que contiene nuestra legislación procesal están: Recurso de reposición, recurso de apelación, recurso de queja, recurso de apelación especial, recurso de revisión y el recurso de casación.

3.4.1. Recurso de reposición

Es un recurso que se puede plantear frente a cualquier resolución de juez o tribunal, que se haya dictado sin audiencia previa, siempre y cuando no quepa frente el mismo recurso de apelación o de apelación especial, con el objetivo de que se reforme o se revoque. Asimismo, este recurso se interpone ante el mismo órgano jurisdiccional que dicto la resolución en un plazo de tres días y el tribunal lo resolverá en el mismo plazo.

3.4.2. Recurso de apelación

Este recurso es el medio de impugnación que se interpone frente a las resoluciones del juez de primera instancia, para que la sala de apelaciones, examine lo resuelto y revoque o modifique la resolución recurrida. Este es un recurso amplio en cuanto a sus motivos que procede contra un número limitado de autos señalados en el Artículo 404, del Código Procesal Penal.

En cuanto a los motivos por los que procede el recurso de apelación, se dice que son motivos amplios porque pueden discutirse cuestiones referidas a la aplicación del derecho (tanto penal como procesal) o cuestiones de valoración de los hechos y la prueba que funda la decisión. Este recurso deberá de interponerse por escrito dentro del término de tres días, indicándose el motivo en que se funda, bajo sanción de inadmisibilidad, si el recurrente no corrige en su memorial los defectos

u omisiones establecida en el Código Procesal Penal específicamente en el Artículo 407.

3.4.3. Recurso de queja

Cuando interponemos un recurso de apelación o de apelación especial, ante el juez ya sea de primera instancia, de paz, de sentencia, o de ejecución, dependiendo de quien haya dictado la resolución o resuelto la misma, y si el escrito en el que planteamos el recurso contiene las exigencias de forma que plantea la ley, y el tribunal lo rechace, se habilita el recurso de queja, con el objeto de que la Sala de Apelaciones solicite las actuaciones y resuelva su procedencia y, en su caso sobre el fondo de la cuestión.

Este recurso lo encontramos regulado en el Artículo 412. Asimismo, en el Artículo 413, encontramos su tramitación en el cual se establece que "se le solicitara informe al juez respectivo, quien lo expedirá en un plazo de veinticuatro horas, y el presidente pedirá el envió de las actuaciones cuando lo considere conveniente".

En el Artículo 414, encontramos "que la resolución de la queja será dentro de las veinticuatro horas de recibido el informe y las actuaciones en su caso. Si este se desestimare, las actuaciones serán devueltas al tribunal de origen sin más trámite. En caso contrario, se concederá el recurso y se procederá conforme a lo prescrito

para el recurso de apelación". Todos los Artículos anteriormente mencionados, son del Código Procesal Penal.

3.4.4. Recurso de apelación especial

De acuerdo con el Artículo 415 del Código Procesal Penal, "la apelación especial es un recurso restringido en cuanto a sus motivos, que procede contra: a) Las sentencias del tribunal de sentencia; b) Las resoluciones del tribunal de sentencia que declaren el sobreseimiento o el archivo y; c) Las resoluciones del juez de ejecución que pongan fin a la pena, a medida de seguridad y corrección o denieguen la extinción, conmutación o suspensión de la pena".

Este recurso que es semejante a los recursos de casación, tiene por objeto controlar las decisiones de los tribunales que dictan sentencia, asegurando de esta forma el derecho al recurso reconocido por la Convención Americana sobre Derechos Humanos, Artículos 8, 2. El hecho de que este recurso sea semejante a la casación, no implica que deban aplicarse todas las normas formales que tradicionalmente se exigieron para la casación. Tanto solo se podrá admitir, un recurso cuando no respete lo preceptuado en el Código Procesal Penal.

El objeto del recurso de apelación especial es: la sentencia o la resolución que pone fin al procedimiento. Asimismo, podrá ser impugnada el acta del debate, cuando se trate de impugnar la forma en que se ha conducido el debate. Los

legitimados a impugnar son los mismos y en las mismas condiciones para impugnar en los otros recursos.

El motivo de procedencia del recurso, restringido legalmente, es la infracción a la ley. Conforme a este criterio el Código Procesal Penal distingue en el Artículo 419, entre infracciones de fondo y de forma. "La primera de ellas, es la incorrecta o errónea aplicación de la ley que, interpretado contextualmente debemos entender que se trata de la ley sustantiva, y la segunda, un error o inobservancia que constituya un vicio del procedimiento".

3.4.4.1. Apelación especial de fondo

El Artículo 419 en el inciso primero, indica "que podrá interponerse recurso de apelación de fondo cuando exista:

Inobservancia de la ley: Inobserva la norma sustantiva quien hace caso o miso de ella y no la aplica. Por ejemplo, en un relato de hechos se señala que el imputado produjo heridas que tardaron en curar más de veinte días y no tipifica ese hecho como lesiones leves.

Interpretación indebida. Se dará la interpretación indebida cuando se realice una errónea tarea de subsunción, es decir los hechos analizados no coinciden con el

presupuesto fáctico. Por ejemplo, en un delito contra el patrimonio, interpretar que un edificio es un bien mueble.

Errónea aplicación de la ley. Habrá errónea aplicación de la ley cuando ante unos hechos se aplique una norma no prevista entre sus presupuestos fácticos. Por ejemplo, tipificar parricidio cuando el acusado mate a su hermano. El examen de la sentencia que puede hacerse mediante el recurso de apelación especial de fondo es estrictamente, es una revaloración jurídica de los hechos descritos en la sentencia". Asimismo, los efectos que señala el Artículo 431, son los siguientes; "anular la sentencia recurrida y dictar nueva sentencia. En la misma deberá, razonando jurídicamente indicar la correcta aplicación de la ley, fijando la pena a imponer".

El Artículo 433 del Código Procesal Penal señala que "no será necesario anular la sentencia cuando los errores no influyan en su parte resolutiva o sea errores materiales en la designación o en el cómputo de la pena. En esos casos la sala se limitara a corregir el error".

3.4.4.2. Apelación especial de forma

Lo que se busca con este recurso, es que se respete el rito establecido por la ley, es decir, las normas que determinan el modo en que deben de realizarse los actos, el tiempo, el lugar y en general, todas aquellas normas que regulan la actividad de los sujetos procesales.

El Artículo 419 del Código Procesal Penal, establece: "que procede el recurso de apelación especial contra una sentencia o resolución, cuando se haya operado una inobservancia o errónea aplicación de la ley que constituya un defecto del procedimiento".

La Ley Procesal cuya aplicación se alega, será tanto del Código Procesal Penal, como la Constitución y Tratados Internacionales. El vicio que puede alegarse para la procedencia del recurso tiene dos características: a) El vicio ha de ser esencial, ya que este debe de repercutir directamente en la parte resolutiva de la sentencia y debe de afectar la decisión en concreto y; b) El recurrente debe de haber reclamado oportunamente la subsanación o hecho protesta de anulación, ya que el Artículo 403 del Código Procesal Penal establece "que durante el debate, el planteo del recurso de reposición equivale a la protesta de anulación".

El Artículo 420 del Código Penal, especifica "en que materias el vicio el vicio debe de considerarse absoluto: a) Lo concerniente al nombramiento y capacidad de los jueces y a la constitución del tribunal; b) Los casos de ausencia del Ministerio Público en el debate o de otra parte cuya presencia prevé la ley; c) Lo relativo a la intervención, asistencia y representación del acusado en el debate, en los casos y formas que la ley establece; d) Lo relativo a la publicidad y continuidad del debate, salvo los casos de reserva autorizada; e) Casos de injusticia notoria; f) el Artículo 394 del Código Procesal Penal establece los vicios de la sentencia: Que el

acusado o las partes civiles no estén suficientemente individualizados. Que falte la enunciación de los hechos imputados a lo enunciado de los daños y la pretensión de la reparación del actor civil. Si falta o es contradictoria la motivación de los votos que haga la mayoría del tribunal, o no se hubieren observado en ella las reglas de la sana critica razonada con respecto a medios o elementos probatorios de valor decisivo".

Asimismo, encontramos que: a) Falte o sea incompleta en sus elementos esenciales la parte resolutiva. b) Que falte la fecha o la firma de los jueces, según lo dispuesto en los Artículos anteriores. La inobservancia de las reglas previstas para la redacción de la sentencia.

Asimismo, encontramos los efectos del recurso de apelación especial de forma el cual establece que el principal es el de anulación del acto recurrido, y en el cual distinguimos dos situaciones distintas: a) El recurso admitido impugnaba la redacción de la sentencia, aduciendo un vicio en la misma, por ejemplo encontramos en el Artículo 394 inciso tercero, el cual establece que "la sentencia no esta motivada, ya que la sala de apelaciones ordenara el reenvió y el mismo tribunal que la redacto tendrá que repetirla, corrigiendo los defectos señalados".

No procederá el reemplazo del tribunal, ya que obviamente, solo los jueces que redactaron la sentencia podrán corregir los vicios. Y; b) El vicio señalado seda en el procedimiento, ya que en este caso, habrá que renovar el acto anulado y repetir todos los actos posteriores influidos por dicho vicio. El fallo tendrá que ser dictado por distintos jueces a los que reconocieron el fallo impugnado. Por ello la admisión de dicho recurso genera necesariamente la repetición del debate, pues, independientemente de la normativa sobre interrupciones.

Asimismo, el trámite para la interposición de este recurso, lo encontramos en los Artículo del Código Procesal Penal así: El Artículo 423, "se interpone por escrito en el plazo de 10 días, ante el tribunal que dicto la resolución recurrida, el tribunal debe de notificar a todas las partes, después de notificado a los interesados remitirá las actuaciones, a la Corte de Apelaciones correspondiente, quien debe de emplazar a las partes para que comparezcan ante el mismo". El Artículo 424 del mismo cuerpo legal establece que: en el plazo de cinco días del emplazamiento, las partes deben de comparecer ante la sala y en su caso señalaran nuevo lugar para recibir notificaciones, y si no comparece se tendrá por abandonado el recurso". Asimismo, dentro del plazo de los 10 días, cualquiera de las partes podrá adherirse al recurso, planteado por otra parte, esto lo establecemos en base al Artículo 417 del Código Procesal Penal. Artículo 425 del mismo cuerpo legal establece que: "recibido las actuaciones y vencido el plazo y vencido el plazo de cinco días, la sala analizara el recurso y las adhesiones y

revisara si contiene los requisitos de tiempo, argumentación, fundamentación y protesta".

De existir defecto la sala lo hará saber al interponerte, explicándole los motivos, para que en el plazo de tres días lo amplié o corrija. Si no lo presenta corregido en plazo o no subsane los defectos señalados, la sala lo declarara inadmisible y devolverá el recurso. Frente a la resolución no cabe ningún recurso. El Artículo 426 del Código Procesal Penal establece que: "Admitido el recurso, las actuaciones quedaran por seis días en la oficina del tribunal, para que los interesados puedan examinarlas. Vencido el plazo el presidente fijara audiencia para el debate, con un intervalo de diez días y notificado a las partes".

Y, finalmente el Artículo 427 del Código Procesal Penal señala que: "la audiencia se celebrara con las formalidades de ley" cuando el recurso planteado sea de forma, se podrá presentar prueba para demostrar el vicio de procedimiento", esto lo encontramos en el Artículo 428 del Código Procesal Penal. "Asimismo, finalizada la audiencia se reunirán los magistrados de la sala para deliberar y posteriormente dictar sentencia", Artículo 429 del Código Procesal Penal.

"Cuando el objeto del recurso sean las resoluciones interlocutorias del tribunal de sentencia o de ejecución" señaladas en el Artículo 435 inciso primero del Código

Procesal Penal, o "lo relativo a la acción civil siempre que no se recurra la parte penal de la sentencia", se modificara el procedimiento de acuerdo al Artículo 436 del Código Procesal Penal.

3.4.5. La revisión

Este es un medio extraordinario que procede por motivos taxativamente fijados, para rescindir sentencias firmes de condena. Asimismo, supone un límite al efecto de cosa juzgada de las sentencias, por cuanto se plantea en procesos ya terminados. La seguridad jurídica impide, como norma general, que los procesos finalizados pueden ser reabiertos en cualquier momento. Sin embargo la sentencia, como acto humano que es, puede estar equivocada.

Por ello, el Código Procesal Penal ha previsto la posibilidad de rescindir sentencias manifiestamente injustas, pero siempre y cuando sean de condena. La seguridad jurídica se entiende como valor prioritario y tan solo el respeto a la persona humana, injustamente condenada, permite una revisión de sentencia.

De acuerdo al Artículo 455 del Código Procesal Penal, "para que haya revisión es necesario: a) Que exista una sentencia condenatoria firme; b) Que aparezcan nuevos hechos o nuevos medios de prueba. Asimismo, cabe la revisión cuando se modifique la legislación y; c) Los nuevos hechos o reformas legales produzcan la absolución o reducción de la condena o medida de seguridad. Por lo tanto es

necesario que la nueva situación produzca un efecto en la pena o medida de seguridad".

"No es necesario que la pena se esté cumpliendo en el momento en el que se plantea la revisión. Esta puede promoverse incluso después de la muerte del injustamente condenado". Los motivos especiales por los que podemos plantear el recurso de revisión los regulados el Artículo 455 del Código Procesal Penal, el cual establece que:

- "La presentación, después de la sentencia, de documentos que no hubiesen podido ser valorados en la sentencia, nuestra ley exige que esos documentos sean decisivos.

- La demostración de que un elemento de prueba decisivo, apreciado en la sentencia carece de valor probatorio asignado, por falsedad, invalidez, adulteración o falsificación.

- Cuando la sentencia condenatoria ha sido pronunciada a consecuencia de prevaricación, cohecho, violencia u otra maquinación fraudulenta, cuya existencia fue declarada en fallo posterior firme.

- Cuando la sentencia penal se basa en una sentencia que posteriormente ha sido anulada o ha sido objeto de revisión.

- La aparición de nuevos hechos o elementos de prueba que solos o unidos a los ya examinados en el proceso, hacen evidente que el hecho o una

circunstancia agravante no existió o que el reo no lo cometió. Este inciso engloba en líneas generales cualquier supuesto no contenido en los incisos anteriores.

- La aplicación retroactiva de una ley penal más benigna que la aplicada en la sentencia. En este inciso se agrupan todos los supuestos de una modificación legislativa favorece al reo. El cambio puede darse en la cuantía de la pena, como en la tipificación de la conducta". Por ejemplo que se despenalice la posesión de droga para el consumo.

De acuerdo al Artículo 454 del Código Procesal Penal, tienen la facultad para impugnar e interponer el recurso de revisión:

- "El condenado o aquel a quien se le hubiere aplicado medida de seguridad.
- En caso de ser incapaz, sus representantes legales y en caso de haber fallecido sus familiares.
- El Ministerio Público, aplicando el principio de objetividad que establece su propia, Ley orgánica".

Asimismo, establece el Artículo 457 del Código Procesal Penal, "que el condenado podrá designar un defensor que mantenga la revisión. En caso de que reo

falleciere el proceso podrá ser continuado por el defensor o por los familiares. En aquellos casos en que se modifique la ley, el juez de ejecución podrá de oficio iniciar el proceso para la aplicación de la ley más benigna".

La forma de tramitar el recurso de revisión la encontramos regulada en los Artículos 456, 458 y 459 del Código Procesal Penal, y establecen lo siguiente:

- "El recurso de revisión, para ser admitido, debe de ser promovido por escrito ante la Corte Suprema de Justicia, señalándose expresamente los motivos en los que se funda la revisión de los preceptos jurídicos aplicables. No existe ninguna limitación temporal en cuanto a su admisión. Si los motivos de revisión no surgen de una sentencia o reforma legislativa, el impugnante deberá indicar los medios de prueba que acrediten la verdad de sus afirmaciones", Artículos 456 del Código Procesal Penal.
- "El, establece que recibida la impugnación la Corte Suprema de Justicia decidirá sobre su procedencia. Si faltaren requisitos, podrá otorgar un plazo para que estos se cumplan".
- "Una vez admitida la revisión, la Corte Suprema de Justicia le dará intervención al Ministerio Público o al condenado, según el caso y dispondrá, si fuere necesario la recepción de medios de prueba solicitados por el recurrente. Corte Suprema de Justicia podrá ordenar la recepción de pruebas de oficio", esto lo encontramos regulado en el Artículo 458 del Código Procesal Penal.

El Artículo 459 del Código Procesal Penal regula: "finalizada la instrucción se dará una audiencia para oír a los intervinientes, pudiéndose entregar alegatos por escrito. Finalizada la misma, el tribunal declarara si da lugar o no a la revisión".

"Los efectos del recurso de revisión pueden dar lugar: A la remisión para la repetición del juicio, este nuevo juicio ha de tramitarse conforme las normas contenidas en el Código Procesal Penal. En este nuevo juicio, en la presentación de prueba y en la sentencia, han de valorarse los elementos que motivaron la revisión", Artículo 461 del Código Procesal Penal.

El Artículo 462 del Código Procesal Penal, establece que "al dictar nueva sentencia, por parte de la Corte Suprema de Justicia, la nueva sentencia ordenara la libertad, el reintegro total o parcial de la multa y la cesación de cualquier otra pena". "En su caso podrá aplicarse nueva pena o practicarse nuevo cómputo de la misma. Asimismo, se establece que la admisión de la revisión puede dar lugar a indemnización", conforme a lo señalado en los Artículos 521 al 525 del Código Procesal Penal. La indemnización solo podrá darse al imputado o a sus hermanos. La indemnización de la revisión no imposibilita peticionar de nuevo, fundada en elementos distintos.

3.4.6. Recurso de casación

Este es un recurso limitado en sus motivos, que puede plantearse ante la Corte Suprema de Justicia, frente alguno de los autos y sentencia que resuelvan, recursos de apelación y apelación especial. "Este recurso cumple una función de unificación de la jurisprudencia de las distintas salas de la Corte de Apelación". De acuerdo con el Artículo 437 del Código Procesal Penal, el objeto del recurso de casación es que procede contra las sentencias o autos definitivos dictados por las salas de apelaciones que resuelvan: a) el recurso de apelación especial de los fallos emitidos por los tribunales de sentencia; b) Los recursos de apelación especial, contra los autos de sobreseimiento dictados por el tribunal de sentencia; c) Los recursos de apelación contra las sentencias emitidas por los jueces de primera instancia, en los casos de procedimiento abreviado; y d) Los recursos de apelación contra los resoluciones de los jueces de primera instancia que declaren el sobreseimiento o clausura del proceso. Y los que resuelvan excepciones u obstáculos a la persecución penal.

En la casación solo se entrarán a conocer los errores jurídicos contenidos en el auto o sentencia emitidos por la sala de la Corte de Apelaciones. Los errores pueden surgir en la resolución de la sala o venir arrastrándose desde la primera resolución. Por ejemplo, se puede recurrir una sentencia que resuelva apelación especial, que deniegan la misma y confirma una sentencia del tribunal.

"Asimismo, encontramos que el recurso de casación se divide en dos: el primero que encontramos es el recurso de casación de forma el cual versa sobre violaciones esenciales del procedimiento" tal como lo establece el Artículo 439 del Código Procesal Penal. En el Artículo 440 del mismo cuerpo legal, establece "taxativamente los motivos de forma por los que puede plantearse el recurso de casación:

- Cuando la sentencia no resolvió todos los puntos esenciales que fueron objeto de la acusación formulada o que estaban contenidos en las alegaciones del defensor.

- Cuando la sentencia no expreso de forma concluyente los hechos que el tribunal de sentencia tenía como probados o los fundamentos de la sana critica que se tuvieron en cuenta en la misma.

- Cuando la resolución se den por probados dos o más hechos manifiestamente contradictorios.

- Cuando la resolución se refiere a un hecho punible distinto del que se atribuye al acusado.

- Cuando en el fallo del tribunal de sentencia o de la sala de apelaciones ha existido incompetencia por razón de la materia que no haya sido advertida.

- Cuando en la sentencia no se cumplan las formalidades exigidas para su validez" contenidas en el en el Artículo 389 del Código Procesal Penal.

"Si se admite un recurso de casación de forma, la Corte Suprema de Justicia remitirá el expediente a la sala de la Corte de Apelaciones para que dicte nuevo auto o sentencia" esto lo encontramos regulado en el Artículo 448 del Código Procesal Penal.

El segundo seria el recurso de casación de fondo, el cual hace referencias a las infracciones a la ley sustantiva que influyan o influyeron decisivamente en la parte resolutiva de la sentencia o auto recurrido. Asimismo, el Artículo 441 del Código Procesal Penal señala "los motivos por los cuales puede interponerse el recurso de casación:

- Cuando en la nueva sentencia se produce una errónea tipificación de los hechos, al calificar como delito hechos que no lo son, o calificar un hecho delictivo de forma incorrecta. Por ejemplo si calificamos como estafa un simple incumplimiento contractual o como hurto un robo.

- Cuando hubo condena y era manifiesto que no era manifiesto que no había antijuridicidad, culpabilidad o punibilidad, por existir una circunstancia eximente. Por ejemplo del relato de hechos queda manifiesto que hubo legítima defensa.

- Cuando la sentencia en apelación especial tenga por acreditado un hecho decisivo para absolver, condenar, atenuar o agravar la pena, sin que el

tribunal de sentencia haya declarado probado el hecho. Lo que se pretende en este inciso es evitar que en la apelación especial se viole el principio de intangibilidad de prueba.

- Cuando en la resolución se haya vulnerado preceptos constitucionales o legales y ello haya influido en la resolución o auto".

Si se declara procedente el recurso de casación de fondo, se casara la sentencia o resolución recurrida y la Corte Suprema de Justicia, dictara una nueva. En cuanto su forma y trámite, lo encontramos en los Artículos siguientes: el Artículo 443 del Código Procesal Penal establece que, "solo se tendrán debidamente fundados los recursos de casación cuando se expresen de manera clara y precisa los Artículos e incisos que autoricen el recurso, indicando si es de casación de forma o de fondo, así como si contiene los Artículos e incisos que se consideren violados por las leyes respectivas".

El mismo podrá interponerse ante la Corte Suprema de Justicia o ante la sala que resolvió la resolución recurrida. En este ultimo supuesto, la sala elevara inmediatamente el recurso a la Corte Suprema de Justicia. Una vez recibido el recurso, la Corte Suprema de Justicia analizará si el mismo cumple los requisitos de forma. Si se interpusiera fuera de plazo o no cumpliera con los requisitos del

Artículo 443 del Código Procesal Penal, "la Corte Suprema de Justicia lo rechazara sin más trámite, en caso contrario, lo admitirá, pedirá los autos y señalara día y hora para la audiencia. El día y hora señalado se celebrará vista pública a la que se citará a las partes", procediéndose de acuerdo con los señalado en el Artículo 446 del Código Procesal Penal. "En un plazo de quince días desde la audiencia, la Corte Suprema de Justicia deberá dictar sentencia".

CAPÍTULO IV

4. Convenios internacionales en el ámbito de delitos informáticos

La especial naturaleza de los delitos informáticos, que como ya se ha mencionado trasciende fronteras y continentes hace necesaria la unificación de criterios y esfuerzos en el ámbito de persecución penal; de esa cuenta que son cada vez más los países llamados a uniformar legislaciones en el ámbito de investigación y enjuiciamiento de este tipo de ilícitos.

Al respecto la Organización de las Naciones Unidas señaló: "La creciente densidad de tecnologías de la información y las comunicaciones también aumenta la frecuencia de la delincuencia informática nacional, obligando a las naciones a establecer legislación nacional. Puede que se requieran leyes nacionales adaptadas a la delincuencia cibernética para responder eficazmente a las peticiones externas de asistencia o para obtener asistencia de otros países. Cuando se elabora legislación, la compatibilidad con las leyes de otras naciones es una meta esencial; la cooperación internacional es necesaria debido a la naturaleza internacional y transfronteriza de la delincuencia informática. Se necesitan mecanismos internacionales formales que respeten los derechos soberanos de los Estados y faciliten la cooperación internacional. Para que la asistencia judicial recíproca funcione con éxito, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de otras."

No obstante este consenso general a la fecha son pocos los instrumentos que en esta materia se han regulado a nivel internacional. A continuación se describen brevemente los más importantes:

4.1. Convenio sobre Cibercriminalidad

En fecha 23 de Noviembre del año 2001 en Budapest Hungría se suscribió el Convenio sobre Cibercriminalidad entre los Estados miembros del Consejo de Europa y otros países entre los que se cuentan Estados Unidos de América. El instrumento cobra vigencia en junio del 2004 y tiene como objetivo principal coordinar esfuerzos que permitan hacer efectiva la persecución penal en el ámbito de los delitos informáticos a nivel Internacional.

Regula en su texto disposiciones sobre uniformidad de la terminología en el ámbito de la informática. En lo referente a los delitos informáticos describe elementos tipo a ser tomados en cuenta en las legislaciones propias de los países suscriptores; hace un particular énfasis en la necesidad de perseguir criminalmente delitos tales como la pornografía infantil, fraude informático y delitos contra la propiedad intelectual. De igual manera contiene aspectos referentes al proceso penal en ámbitos como la competencia para la persecución de este tipo de ilícitos, Acuerdos relacionados a la Asistencia Jurídica Internacional para el juzgamiento y procura de medios de prueba así como reglas para definir las cuestiones de extradición.

En conclusión se materializó un instrumento de gran importancia en el marco de los esfuerzos internacionales para prevenir y sancionar la comisión de este tipo

de ilícitos; sin embargo es importante acotar que el alcance del mismo se limitó a Los países suscriptores no obstante estar abierto a la adhesión. En el ámbito Latinoamericano se ha mostrado buena voluntad y disposición para hacer propios los lineamientos del Convenio sobre Cibercriminalidad sin embargo a la fecha han sido pocas las disposiciones que se han tomado para hacer esto realidad. Concretamente al Convenio se han suscrito los Estados de Costa Rica, República Dominicana, México, Argentina y Chile.

4.2. La Organización de las Naciones Unidas y la prevención del delito informático, undécimo congreso.

La temática "Medidas para prevenir delitos informáticos" constituyó una de las tratadas en el marco de este Congreso; en ese sentido se citó la resolución de asamblea general número 56/121 que señala con respecto a los Estados: "Al elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, tuvieran en cuenta la labor y los logros de la Comisión de prevención del delito y justicia penal y de otras organizaciones internacionales y regionales" Asimismo, la resolución número 56/261citada también señaló: " La Asamblea tomó nota de los planes de acción para la aplicación de la Declaración de Viena, en cumplimiento de los cuales los Estados se esforzarían por apoyar diversas medidas, entre ellas la penalización del uso indebido de la tecnología de la información, la formulación y aplicación de normas y procedimientos para que los delitos relacionados con la informática y las telecomunicaciones pudieran investigarse eficazmente".

Una de las conclusiones a las que se llegó en el referido congreso es que: ".....dentro de las jurisdicciones nacionales, deberían cumplirse cuatro condiciones básicas para responder eficazmente a casos relacionados con delitos informáticos: expertos dedicados al estudio de la delincuencia informática; expertos disponibles 24 horas al día; una capacitación continua, incluida la capacitación de especialistas de otros países; y equipo actualizado. El cumplimiento de esos requisitos mejoraría también la calidad de la cooperación entre los Estados."

Como se podrá apreciar la implementación de estas recomendaciones garantiza contar con herramientas adecuadas para el combate a los delitos informáticos, sin embargo la realidad nos dice que éstas implican la inversión de recursos que escapa a las posibilidades de muchos Estados. En ese sentido la cooperación internacional resulta más que trascendente para fortalecer a los gobiernos locales, en el entendido que el combate a delitos informáticos debe ser un esfuerzo mundial ya que dada su especial naturaleza los ámbitos de ejecución de estos ilícitos trascienden las fronteras y por eso su persecución debe ser un interés que trascienda también a los países.

4.3. Convención de Palermo

La Convención de las Naciones Unidas contra la delincuencia organizada transnacional adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000 mediante Resolución A/RES/55/25 más conocida como Convención de Palermo tiene como finalidad según su Artículo 1: "promover la

cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional. Los métodos utilizados para combatir la delincuencia organizada transnacional mediante computadoras, redes de telecomunicaciones u otras formas de la tecnología moderna".

En ese sentido debe tomarse en cuenta que ésta convención busca uniformar criterios de capacitación y asesoría a los funcionarios judiciales, fiscales y policiales en el ámbito del combate a delitos de delincuencia organizada a través de herramientas informáticas o bien de internet.

Los elementos para la creación de una cultura mundial de seguridad cibernética:

En el marco del quincuagésimo séptimo período de sesiones se aprobó por parte de la Asamblea General de las Naciones Unidas en fecha 31 de Enero del 2003 este instrumento. Parte de la base de reconocer que la necesidad de la seguridad cibernética aumenta cada día a medida que los países aumentan su participación en la sociedad de la información. Establece en un anexo los Elementos para la creación de una cultura de seguridad cibernética sobre aspectos como:

Conciencia: De los Estados, individuos e instituciones de la necesidad de la seguridad de los sistemas y redes de información.

Responsabilidad: Para examinar periódicamente las propias políticas de los participantes así como evaluar estas.

Respuesta: Debe darse ésta de manera pronta y oportuna ante cualquier ataque a la seguridad de los sistemas y redes de información, así como compartir

información sobre amenazas y vulnerabilidad de los sistemas, aplicar procedimientos ágiles de cooperación interestatal.

Ética: Para el respeto de los legítimos intereses de los demás.

Democracia: Las medidas de seguridad deben atender a los principios de un Estado Democrático, respeto de la libertad de expresión, acceso a la información, la transparencia, etc.

Evaluación de riesgos: Implica la obligación de evaluar periódicamente los riesgos amenazas y vulnerabilidades.

Diseño y puesta en práctica y gestión de la seguridad: En ese sentido pretende el consenso de creación y aplicación de mecanismos de seguridad informática.

Reevaluación: Implica el análisis de los sistemas de seguridad examinando su eficacia e incorporar las modificaciones necesarias para hacer frente a las amenazas y vulnerabilidades en la medida que éstas se presentan.

4.4. Manual de las Naciones Unidas para la prevención y control de los delitos informáticos

En términos generales este instrumento señala que los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada, establece como causales de éstas necesidades una realidad caracterizada por la falta de acuerdos globales acerca de qué conductas tipo deben constituir delitos informáticos, falta de leyes

especializadas en materia procesal, sustantiva así como de investigación. El carácter transnacional de delitos cometidos mediante el uso de computadoras, ausencia de tratados de extradición, de acuerdos y de mecanismos sincronizados que permitan la plena eficacia de la cooperación internacional.

4.5. La Organización de Estados Americanos y los delitos informáticos

4.5.1 Estrategia de la OEA sobre seguridad informática

Por medio de la resolución AG/RES.1939 (XXXIII-0/03) aprobada en la cuarta sesión plenaria celebrada el 10 de Junio de 2003, la Asamblea General de la Organización de Estados Americanos aprobó las pautas para el desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. La misma resuelve:

a. Encomendar al Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA) que se aseguren de que la Conferencia de la Organización de los Estados Americanos (OEA) sobre Seguridad Cibernética, propuesta por la Argentina, empiece a trabajar en el desarrollo de un proyecto de estrategia integral de la OEA sobre seguridad cibernética que aborde los aspectos multidimensional y multidisciplinario de la seguridad cibernética y que: informen sobre los resultados de la reunión, y sobre el trabajo de seguimiento que se considere apropiado, a la Comisión de Seguridad Hemisférica para su consideración.

b. Encomendar al Consejo Permanente que, a través de la Comisión de Seguridad Hemisférica, desarrolle un proyecto de estrategia de seguridad cibernética para los Estados Miembros en coordinación y colaboración con la CITEL, el CICTE, el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la REMJA y cualquier otro Órgano de la OEA que se considere apropiado, sin perjuicio de sus respectivos mandatos, misiones y requerimientos existentes sobre presentación de informes, teniendo en consideración cualquier actividad pertinente en los Estados Miembros relativa a la protección de infraestructura crítica, y que presente este proyecto de estrategia sobre seguridad cibernética al Consejo Permanente para su consideración.

c. Solicitar al Consejo Permanente que informe a la Asamblea General en su trigésimo cuarto período ordinario de sesiones sobre la implementación de esta resolución.

CONCLUSIÓN DISCURSIVA

Los delitos informáticos, son figuras delictuales que con la globalización mundial se han convertido en delitos de carácter transnacional; es por ello, que es urgente que el legislador regule específicamente dichos delitos, pues la legislación vigente ya no es acorde a este tipo de ilícitos que cada día se comenten, tanto en lo particular como en la administración pública. Delitos que han sido tratados en el seno de la Organización de Naciones Unidas y en la Organización de Estados Americanos, puesto que afecta a toda la sociedad en general a nivel mundial.

De conformidad al Artículo 2 de la Constitución Política de la República de Guatemala, es deber del Estado garantizar a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona, es bajo este precepto constitucional que no se puede dejar de legislar y tipificar estos delitos en el Código Penal.

Se debe castigar severamente a los infractores de los delitos informáticos, protegiendo de esta manera el bien jurídico tutelado de los usuarios del sistema informático, y se deben crear mecanismos de control para prevenir estos ilícitos por parte del Organismo Legislativo.

BIBLIOGRAFÍA

ALSINA, Hugo. **Tratado teórico-practico del derecho procesal civil y comercial.** t. I. Buenos Aires, Argentina: Ed. Ad-Hoc, 1941.

BARRIENTOS PELLECER, César. **Código Procesal Penal.** Guatemala, Guatemala: Ed. Llerena, 1997.

BINDER, Alberto. **Introducción al derecho procesal penal.** Buenos Aires, Argentina: Ed. Ad-Hoc, 1993.

BUSTAMANTE ALSINA, Jorge. **La informática y la protección del secreto de la vida privada.** Buenos Aires, Argentina: Ed. 122-826, 1987.

CALLEGARI, Lidia. **Delitos informáticos y legislación en revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana.** Medellín, Colombia: (s.Ed.) 1985.

CABANELLAS, Guillermo. **Diccionario enciclopédico de derecho usual.** 14ª. ed. Buenos Aires, Argentina: Ed. Heliasta SRL, 1979.

CLARIA OLMEDO, Jorge. **Derecho procesal penal.** t. 3. Argentina: Ed. Marcos Lerner Cordova, 1984.

CREUS, Carlos. **Derecho procesal penal.** Buenos Aires, Argentina: Ed. Astrea, 1996.

DE LEÓN VELASCO, Héctor Aníbal y José Francisco de Mata Vela. **Curso de derecho penal guatemalteco, parte general y parte especial.** 4ª ed. Guatemala, Guatemala: Ed. Offset, Imprenta y Encuadernación, 1989.

FRENECH, Miguel. **Derecho procesal penal.** Vol. I. Barcelona, España: Ed. Labor, S.A. 1960.

MORAS MOM, Jorge R. **Manual de derecho procesal penal.** 1ª. ed. Buenos Aires, Argentina: Ed. Abeledo-Perrot, 1993.

TÉLLEZ VALDÉS, Julio. **Derecho informático.** 2ª. ed. México: Ed. Mc Graw Hill, 1996.

TIEDEMANNN, Klauss. **Poder económico y delito.** 1ª. ed. Barcelona, España: Ed. Ariel, 1985.

VÉLEZ MARICONDE, Alfredo. **Código procesal penal y leyes complementarias.** Buenos Aires, Argentina: Ed. Astrea, 1994.

ZAFFARONI. Eugenio Raúl. **Derecho penal parte general.** 2ª. ed. Buenos Aires, Argentina: Ed. Ediar, S.A. 2001.

Legislación:

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

Código Civil. Decreto Ley 106, Enrique Peralta Azurdia, Jefe de Gobierno de la República de Guatemala, Decreto Ley 106, Guatemala. 1964.

Código Penal. Congreso de la República de Guatemala, Decreto número 17-73, 1992.

Código Procesal Civil y Mercantil de Guatemala. Decreto Ley número 107, Enrique Peralta Azurdia, Jefe de Gobierno de la República de Guatemala, 1971.

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

Ley del Organismo Judicial. Congreso de la República de Guatemala, Decreto número 2-89, 1989.