

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



ROMEO ANDREÉ MOLINA ORTIZ

GUATEMALA, MARZO DE 2024

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

**CRIMINOLOGÍA COMO HERRAMIENTA ESENCIAL EN LA PREVENCIÓN DE
DELITOS INFORMÁTICOS**



Guatemala, marzo de 2024

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

DECANO:	M.Sc. Henry Manuel Arriaga Contreras
VOCAL I:	Licda. Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic. Rodolfo Barahona Jácome
VOCAL III:	Lic. Helmer Rolando Reyes García
VOCAL IV:	Lic. Javier Estuardo Sarmiento Cabrera
VOCAL V:	Br. Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Lic. Wilfredo Eliú Ramos Leonor

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente:	Lic. Jorge Eduardo Isaías Aguilar Soto
Vocal:	Lic. Marvin Hernández
Secretario:	Licda. Ingrid Nohelia Villatoro Natareno

Segunda Fase:

Presidente:	Licda. Rosa Elida Guevara Pineda
Vocal:	Lic. Abner Fernando Castillo Delgado
Secretario:	Lic. Alex Franklin Méndez Vásquez

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, diez de marzo de dos mil veintiuno.

Atentamente pase al (a) Profesional, ANNABETHSY ZURAMA LEONARDO SOTO
_____, para que proceda a asesorar el trabajo de tesis del (a) estudiante
ROMEO ANDREÉ MOLINA ORTÍZ, con carné 201502321,
intitulado CRIMINOLOGÍA COMO HERRAMIENTA ESENCIAL EN LA PREVENCIÓN DE DELITOS INFORMÁTICOS.

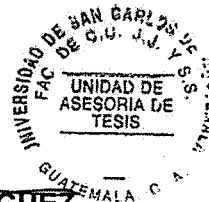
Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

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.



ASTRID JEANNETTE LEMUS RODRÍGUEZ
Vocal en sustitución del Decano



Fecha de recepción 20 / 3 / 2021

Asesor(a)
(Firma y Sello)

Heda. Annabethsy Zurama Leonardo Soto
ABOGADA Y NOTARIA



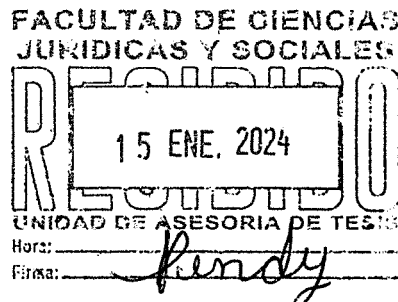


Licda. Annabethsy Zurama Leonardo Soto
Abogada y Notaria
Colegiado No. 6755
Cel: 50196007

Licda. Annabethsy Zurama Leonardo Soto
ABOGADA Y NOTARIA

Guatemala, 01 de agosto del 2022

Dr. Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su despacho



Doctor Herrera Recinos:

En atención a providencia de esa dirección, de fecha diez de marzo de dos mil veintiuno, se me nombra Asesora de tesis del Bachiller Romeo Andreé Molina Ortiz, con el que no existe ningún parentesco dentro de los grados de ley y quien se identifica con el carné 201502321, quien elaboró el trabajo de tesis titulado **"CRIMINOLOGÍA COMO HERRAMIENTA ESENCIAL EN LA PREVENCIÓN DE DELITOS INFORMÁTICOS"**. Habiendo asesorado el trabajo encomendado, me permito seguir el siguiente:

DICTAMEN:

A. CONTENIDO CIENTÍFICO Y TÉCNICO:

Durante el desarrollo de la tesis empleó adecuadamente la información científica mediante recolección de datos doctrinarios y jurídicos que fueron recabados y los cuales se adaptan a los lineamientos exigidos. La tesis se enfoca principalmente en la aplicación de la Criminología para el estudio de los delitos informáticos para su correcta tipificación y prevención.

B. MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN:

Durante el desarrollo de tesis se emplearon métodos y técnicas de investigación necesarias para determinar la realidad actual del país, siendo los métodos utilizados, el sintético, deductivo, inductivo, consultas doctrinarias, recolección de expedientes judiciales y análisis de los mismos.

C. APOORTE CIENTÍFICO:

El aporte científico del presente trabajo de investigación se desarrolla en la rama del Derecho Penal, Derecho Informático y en la Ciencia de la Criminología, específicamente en determinar la ayuda que brinda la Criminología para prevenir la comisión de delitos informáticos.

D. CONCLUSIÓN DISCURSIVA:

La conclusión discursiva es acorde a la investigación y resultados obtenidos.

E. BIBLIOGRAFÍA:

Apruebo totalmente la bibliografía utilizada, ya que es de gran importancia la doctrina utilizada, así como la legislación.



Licda. Annabethsy Zurama Leonardo Soto
Abogada y Notaria
Colegiado No. 6755
Cel: 50196007

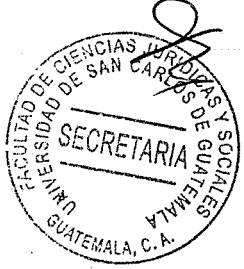
La presente tesis cumple con todos los requisitos exigidos, principalmente lo preceptuado en el artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público. En tal virtud y después de haber satisfecho las exigencias del suscrito asesor, emito **DICTAMEN FAVORABLE** para que el presente trabajo de tesis continúe el trámite respectivo.

Sin otro particular, me suscribo de usted, deferentemente,

Licda. Annabethsy Zurama Leonardo Soto
ABOGADA Y NOTARIA



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala



D. ORD. 122-2024

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, doce de febrero de dos mil veinticuatro.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **ROMEO ANDREÉ MOLINA ORTIZ**, titulado **CRIMINOLOGÍA COMO HERRAMIENTA ESENCIAL EN LA PREVENCIÓN DE DELITOS INFORMÁTICOS**. Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

HMAC/JIMR





DEDICATORIA

- A DIOS:** Por darme la inteligencia y capacidad de afrontar los obstáculos de la vida y brindarme energías para lograr mis éxitos.
- A MI MADRE:** Por darme su amor y apoyo incondicional a lo largo de mi vida, por ser mi consejera y más fuerte ejemplo de superación.
- A MI PADRE:** Por brindarme apoyo en mis estudios y consejos que emplearé en mi profesión.
- A MIS HERMANOS:** Gracias por su apoyo incondicional durante mi carrera académica, han sido mi más grande ejemplo de superación profesional.
- A MIS DOCENTES:** Por su conocimiento profesional que me permitió llegar a este momento; en especial a los profesionales académicos Lic. Barahona Jácome y Licda. Annabethsy Leonardo.
- A MIS AMIGOS:** Por los buenos momentos y conocimientos compartidos en las aulas universitarias.
- A:** La Universidad de San Carlos de Guatemala.
- A:** La Facultad de Ciencias Jurídicas y Sociales.

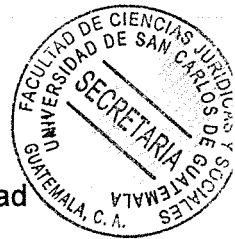


PRESENTACIÓN

El delito informático es una categoría especial de los delitos, los cuales se cometen por el ciberespacio y mediante la utilización de las tecnologías de información y comunicación, teniendo como objetivo a los derechos e información digital o a los componentes informáticos de los distintos dispositivos tecnológicos. Este tipo de delito es complejo al ser desarrollado y cometido por una mente con conocimientos complejos y procesos técnicos en informática, los cuales requieren de un correcto estudio para su combate y prevención.

Este tipo de delitos se pueden prevenir mediante distintas acciones por parte del poder público, tomando en cuenta que la prevención tiene un carácter general (al ser testigo la sociedad de que el Estado está capacitado para sancionar estos delitos) y especial (al sancionar adecuadamente al ciberdelincuente, logrando una rehabilitación adecuada para evitar que vuelva a delinquir), los cuales deben de estar formulado por programas y políticas públicas guiadas por un estudio criminológico que plantea la formulación de una política cibercriminal.

Una política criminal enfocada en delitos informáticos ha ayudado internacionalmente a distintos países para combatir y prevenir el delito informático, debido a que se realiza un estudio detallado de la actividad criminal, con base a sus modos de comisión, los objetivos adecuados, los delincuentes digitales y la ausencia de guardianes capaces que se identifican para poder plasmar una custodia digital, la cual va acompañada de propuestas de reforma legal, fortalecimiento institucional y detalles que ayudarán a



identificar cómo y por qué se dan este tipo de delitos; todo ello enfocado en la realidad nacional.

Por lo tanto, es indispensable abordar un estudio criminológico en los delitos informáticos para poder identificar los delitos actuales y sus modos de comisión que se dan en Guatemala para formular una política criminal enfocada en delitos informáticos para lograr un avance institucional y legal la materia, logrando un mejor manejo del tema para su combate y prevención.



HIPÓTESIS

Criminología como herramienta esencial en la prevención de delitos informáticos, surge por el problema de la alta comisión de ciberdelitos, su mala tipificación en la práctica y la falta de estrategias criminológicas y legales para combatir y prevenir los delitos informáticos en Guatemala; los cuales surgen a causa del cambio tecnológico, económico y social que ha tenido el país, agregado a ello, la falta de estudio, actualización y regulación dirigido a estos delitos por parte del Estado.



COMPROBACIÓN DE LA HIPÓTESIS

Guatemala los delitos informáticos no han sido de importancia, por no tener estudios criminológicos, reformas y planes de acción para prevenir y combatir el cibercrimen. El Estado de Guatemala, no cuenta con políticas criminales que tengan un enfoque de delitos informáticos, y por ello no cumple el mandato constitucional de brindar seguridad y asegurar el bien común de los guatemaltecos.

No hay un estudio criminológico de los delitos informáticos deja desprotegida la integridad, patrimonio y seguridad de los guatemaltecos. Agregado a ello, al no contar con una política cibercriminal no se han creado iniciativas de ley y reforma de delitos adecuados a la realidad nacional, por lo cual se ha vulnerado los derechos de los procesados al aplicar por analogía delitos que fueron creados para regular una actividad criminal que se realiza en el medio físico.

La metodología de investigación para comprobar la hipótesis consistió en el uso de los siguientes métodos: Sintético, al extraer los elementos más importantes del delito informático; deductivo, para obtener conocimientos generales para lograr entender los cibercrimen y la teoría de la actividad cotidiana; inductiva, para establecer la clasificación de los delitos informáticos y diferenciarlos de los biodelitos. La técnica de investigación bibliográfica, sirvió para recolectar y analizar la información que fundamenta la tesis y, la documental, la cual se usó para verificar la legislación extranjera y los expedientes judiciales.



ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Nociones fundamentales del derecho penal	1
1.1. Antecedentes.....	2
1.2. Concepto	7
1.3. Características.....	9
1.4. Principios	11
2. Nociones fundamentales del derecho informático.....	14
2.1. Antecedentes	15
2.2. Concepto	16
2.3. Naturaleza jurídica	17
2.4. Relación con el derecho penal	18

CAPÍTULO II

1. El cibercrimen y el delito informático	19
1.1. Precedentes	20
1.2. Clasificación de los delitos informáticos	23
1.3. La prevención de delitos informáticos	24
1.3.1 La persecución, averiguación y juzgamiento de los delitos informáticos y su influencia en la prevención del delito	28

CAPÍTULO III

1. Generalidades de la criminología	33
1.1. Concepto.....	34
1.2. Relación de la criminología y el derecho penal	35

2. Cuasi-teoría de las criminologías específicas	36
2.1. Criminología informática	36
3. Factores de estudio para la criminología	37
3.1. Factores criminógenos	39
3.1.1. Factores endógenos	40
3.1.2. Factores exógenos	41
4. Política criminal	43
4.1. Política criminal democrática del Estado de Guatemala 2015-2035	43
4.2. Estrategia nacional de seguridad cibernética	45
5. Convenio de Budapest y el compromiso de Guatemala	47

CAPÍTULO IV

1. Teoría de las actividades cotidianas	49
1.1. Ofensor motivado o cibercriminal	51
1.2. Objetivo adecuado o cibervíctima	53
1.3. Custodia digital	54
2. Aplicación de la teoría de las actividades cotidianas en el estudio de los delitos informáticos	56
3. La práctica, su tipificación y su influencia en la prevención	58
3.1. Delitos condenados	61
3.2. Delito atípico mencionado	63
3.3. Conclusión y aspectos relevantes de la práctica y su influencia en la prevención	64
4. Propuesta de solución a la problemática planteada	66
CONCLUSIÓN DISCURSIVA	69
BIBLIOGRAFÍA	71





INTRODUCCIÓN

En Guatemala la criminología como ciencia, ha estado presente en el estudio de la actividad criminal que cada día denuncia la población, de los cuales el Estado se ha encargado de velar por investigar, juzgar y sancionar. El conocimiento técnico y especializado de los investigadores criminológicos es de suma importancia en el análisis de la actividad criminal, mediante los registros que están conservados en las distintas dependencias del Estado, los datos estadísticos y la comprensión de la mente criminal para poder brindar una solución que provea estándares que ayuden a la disminución de comisión de ilícitos.

Está comprobado y aceptado por estándares internacionales y científicos que la aplicación de la criminología para prevenir y combatir el crimen es vital. Es por ello que su aplicación debe de ser constante y aún más si es en hechos delictivos más complejos y propensos a ser dinámicos, tal como sucede con los delitos informáticos. Estos tienden a variar con la innovación de las nuevas tecnologías y el aprovechamiento del conocimiento de las tecnologías de información y comunicación para delinquir. Por esta misma razón el uso de esta ciencia es vital para formular una política cibercriminal, que fortalezca la estructura del Estado y brinde aspectos a considerar para la creación o reforma de leyes penales adecuadas a la realidad nacional.

La hipótesis se comprobó, ya que en Guatemala no existe un estudio criminológico enfocado en delitos informáticos, lo cual ha conllevado a que los tipos penales se encuentren siendo utilizados por analogía por abogados, fiscales y jueces, sancionando delitos informáticos que requieren otro tipo de tipificación y sanción para lograr una correcta rehabilitación del delincuente, incitándolo a no volver a delinquir cumpliendo con la prevención especial y general, al ser visto el Estado de Guatemala como un país capaz de investigar, juzgar y sancionar este tipo de delitos demostrando que está organizado de forma correcta con guardianes capaces y que tiene la legislación adecuada para proteger los derechos tutelados.



Se cumplieron los objetivos esperados, debido a que se pudo determinar la importancia que tiene la criminología en el estudio de los delitos informáticos para brindar las bases de una ley especial y políticas criminales enfocadas a la prevención de este tipo de ilícitos, comprobando que Guatemala no tiene una política criminal enfocada en delitos informáticos. Asimismo, se comprobó que los delitos que actualmente están vigentes están siendo aplicados por analogía por medio de revisión de expedientes judiciales, lo cual influye directamente en lograr una correcta sanción, rehabilitación y prevención.

La tesis queda contenida en cuatro capítulos siendo de la forma siguiente: El primer capítulo, desarrolla lo referente a la generalidad del derecho penal y el derecho informático y su relación; el segundo capítulo, sobre las generalidades de la cibercriminalidad y los delitos informáticos; el tercero, establece las generalidades sobre la criminología y aspectos que deben de ser tomados en cuenta al momento de estudiar los delitos informáticos y los estudios criminológicos que ha hecho Guatemala, y; el cuarto, desarrolla la teoría de las actividades cotidianas y brinda aspectos sobre la práctica judicial que conlleva a malas tipificaciones.

La metodología de investigación para comprobar la hipótesis consistió en el uso de los siguientes métodos: Sintético, al extraer los elementos más importantes del delito informático; deductivo, para obtener conocimientos generales para lograr entender los cibercrimitos y la teoría de la actividad cotidiana; inductiva, para establecer la clasificación de los delitos informáticos y diferenciarlos de los biodelitos. La técnica de investigación bibliográfica, sirvió para recolectar y analizar la información que fundamenta la tesis y, la documental, la cual se usó para verificar la legislación extranjera y los expedientes judiciales.



CAPÍTULO I

1. Nociones fundamentales del derecho penal

Se tiene conocimiento que el derecho penal es un área del derecho público, el cual está enfocado en la creación y regulación de los delitos, faltas, medidas de seguridad y penas. Este se encarga de la persecución penal de los infractores de la ley penal, mediante la aplicación del derecho adjetivo de esta materia, procediendo a la determinación de la responsabilidad penal, su participación, la intensidad del daño causado y la pena a imponer para reparar la vulneración realizada a bienes jurídicos tutelados y ayudar a la debida rehabilitación del delincuente para ser reincorporado a la sociedad.

Esta ciencia es usada por los Estados para crear leyes penales, encaminadas a prevenir, sancionar y erradicar todas aquellas conductas humanas que por acción u omisión provocan un daño a derechos tutelados dentro de un territorio determinado cuya aplicación se extiende a todas las personas que se encuentren dentro de él, no importando que sean nacionales o extranjeros.

De conformidad con nuestra Constitución Política de la República de Guatemala en su artículo 153, establece que: "El imperio de la ley se extiende a todas las personas que se encuentre en el territorio de la República"; En la parte conducente del artículo 4 del Código penal Decreto 17-73 del Congreso de la República, establece: "...este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en



lugares o vehículos sometidos a su jurisdicción”; Y atendiendo al Código Procesal Penal Decreto 51-92 del Congreso de la República en su artículo 38: “la jurisdicción penal se extenderá a los hechos delictivos cometidos en el territorio nacional en todo o en parte...”.

El estudio de esta materia es de suma importancia para poder regular de forma objetiva, actualizada y específica, todas las conductas que a lo largo del tiempo se han visto que afectan los derechos de los habitantes de un Estado, asimismo aquellos que surgen derivados de la creación de nuevos instrumentos tecnológicos que se utilizan para realizar actos delictivos, los cuales no se podrían llevar a cabo sin estos.

Tomando en consideración lo expuesto, se debe reconocer el dinamismo del derecho penal, el cual se debe de adecuar a una población en un tiempo determinado, basándose en la objetividad de la realidad social, del reconocimiento de las nuevas tecnologías y la evolución de la mente criminal y sus formas de planificación, organización y ejecución de nuevas figuras delictivas reconocidas internacionalmente por otros Estados.

1.1. Antecedentes

Los antecedentes del derecho penal son de importancia para el estudio del delincuente, la víctima y el ente sancionador, con el cual se puede demostrar el dinamismo que tiene esta ciencia jurídica y cómo influye una sociedad y su avance tecnológico en cuanto a la regulación del actuar criminal y la forma de sancionarlo, la cual ha

cambiado desde el momento en que no existía un Estado y hasta que este se empezó a formalizar mediante la organización social.

El primer punto relevante a mencionar sobre los antecedentes, es la época de la venganza privada. Es menester mencionar lo que establece de Mata Vela y de León sobre los antecedentes, en el cual afirman que: “la época de la venganza privada es la época bárbara, puesto que accede al impulso de un instinto de defensa, ante la reacción provocada por un ataque que se considera injusto”¹, por lo cual se puede decir que fue un período de justicia bajo el dicho común “diente por diente, ojo por ojo”, donde cada particular tomaba venganza y justicia por su propia mano.

Esta etapa es de mucha importancia debido a que todavía no está estructurado un Estado y la justicia es repartida y aplicada por los particulares, por lo cual, existía el riesgo de aplicar un castigo a una persona por un acto considerado injusto, pero ¿qué era realmente lo injusto?, dejaba abierta la posibilidad de valorar un acto leve como gravísimo y aplicar una sanción inadecuada, vulnerando lo que hoy en día se conoce como un debido proceso, la proporcionalidad y por supuesto, el derecho de la duda.

La segunda etapa es la época de la venganza divina, a lo cual mencionan que: “se sustituye la voluntad individual del vengador por una voluntad divina”², por lo cual es importante resaltar que es un paso importante en cuanto a quién iba a valorar un acto como injusto y le daría su sanción, la cual procede a ser la iglesia mediante sus líderes

¹ De Mata Vela, José Francisco y H. de L. **Derecho Penal Guatemalteco**. Pág. 14.

² *Ibíd.* Pág. 15.

religiosos. En consecuencia, no se puede hablar de una forma eficaz de juzgar, ya que intervenía la moral religiosa de una sociedad y muchos de los actos eran sancionados con torturas, penas capitales y mutilación de extremidades que se realizaban en nombre de un dios justo y castigador hacia el pecador (criminal).

Seguido, se encuentra la época de la venganza pública, en este momento se le es delegado al Estado conocer, valorar, juzgar y sancionar a los actos considerados injustos. Pero es necesario establecer que dichos actos no estaban preestablecidos en norma en su totalidad y que sus penas no estaban normadas, sino que quedaban a consideración del juzgador, por lo cual "La represión penal que pretendía mantener a toda costa la tranquilidad pública, se convirtió en una verdadera venganza pública que llegó a excesos, caracterizándose por la aplicación de penas inhumanas y totalmente desproporcionadas con el daño causado, la pena era sinónimo de tormento."³

La categorización de los delitos, su juzgamiento y sanción fueron de proporciones inhumanas, dejando cada vez más que desear por parte de la población, en donde el Estado mediante sus gobernantes impartían justicia de forma subjetiva, dando sanciones gravísimas a la población, las cuales atentaban contra su dignidad, honor, libertad y su vida, esto sucedía mientras que a aquellos que ostentaban el poder que eran señalados de abuso de poder y por los demás delitos comunes eran sancionados con penas mínimas, vulnerando cada vez el acceso a ser juzgado de forma igualitaria, justa, proporcional y racional. Esto sin duda creó un descontento en esa época y dejando un vacío de justicia social.

³Ibid.

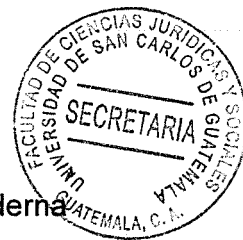


Producto de todos estos acontecimientos anteriormente mencionados, surge el período humanitario, debido al enojo y descontento social de la población de los abusos de poder, juzgamientos injustos y desproporcionados en cuanto a sus sanciones; temiendo incluso, a perder la vida incluso por ver mal a un gobernante. Esta etapa comienza con el iluminismo en la revolución francesa del año 1789, cuando empezaron a surgir grandes pensadores que se oponían a la monarquía de aquel entonces por medio de sus obras y discursos de conciencia social sobre el deber ser del Estado y exigiendo el respeto a los derechos del hombre en igualdad.

Teniendo éxito en el reconocimiento de los derechos humanos, se procede a dar importancia a la rehabilitación y educación del delincuente y en educar a la población para prevenir nuevos actos ilícitos. Siendo este un pilar fundamental para lo que luego se conoció como la etapa científica del derecho penal, que mediante distintos autores y estudiosadores del derecho, llegaron a la conclusión y formulación de que el derecho penal debía de ser estudiado y enseñado como una ciencia.

Comprendiendo que una ciencia es el “conocimiento sistemático que el hombre construye sobre una realidad en condiciones históricas y sociales concretas y determinadas”⁴, siendo este un gran paso para normar la actividad criminal mediante un estudio riguroso que asegure prevenir, reprimir, sancionar y erradicar los actos ilícitos dentro de un territorio y tiempo determinado. Este sin duda es el elemento más básico que rige al derecho, el cual debe de ser sumamente estudiado.

⁴ Castillo, Dina. Documento de Exposición de los Temas: La Realidad, su Conocimiento, Enfoques Epistemológicos y Paradigmas en la Teoría y el Método de la Ciencia. Pág. 23.



Logrando categorizar al derecho penal como una ciencia, procede la época moderna en la que se estableció que el “derecho penal es una ciencia eminentemente jurídica, para tratar los problemas relativos al delito, al delincuente, a la pena y a las medidas de seguridad; mientras que las ciencias penales o criminológicas, que tienen el mismo objeto de estudio, lo deben hacer desde el punto de vista antropológico y sociológico.”⁵ Por lo cual es bueno recordar que esta área del derecho está completamente ligada al principio de legalidad, estudiando y aplicando únicamente lo normado en la ley penal.

Tomando en cuenta todos los antecedentes llegamos a plantear nuestro contexto social actual en Guatemala, lo que muchos juristas en la doctrina han catalogado como la crisis del derecho penal guatemalteco. Es un momento preocupante, debido a que muchas personas han comenzado a perder su confianza en cuanto a la eficiencia y eficacia que debería de tener el Estado para poder investigar, enjuiciar y debatir sobre la responsabilidad penal, su participación y la pena proporcional a aplicar según el daño causado.

La desconfianza aumenta cada día, tomando en cuenta por una parte la falta de aplicación del principio de objetividad por parte del Ministerio Público, el cual se encuentra regulado en nuestro Código Procesal Penal Decreto 51-92 en su artículo 108 el cual establece que: “en ejercicio de su función, el Ministerio Público adecuará sus actos a un criterio objetivo, velando por la correcta aplicación de la ley penal... Deberá formular los requerimientos y solicitudes conforme a ese criterio, aún en favor del imputado”, lo cual no se cumple, ligando a proceso a sindicados que son denunciados

⁵ De Mata Vela, José Francisco y H. de L. **Op. Cit.** Págs. 18 y 19.

sin indicios suficientes y no realizan las gestiones necesarias para averiguar la realidad de los hechos.

Se debe de tener en cuenta que otro factor que llama la atención de los juristas es la mora y retardo judicial en la tramitación de los casos penales, siendo esto completamente lesivo al interés particular y colectivo, porque mientras más tardan los procesos, más sufren los inocentes y las víctimas, y, además abre una brecha para que la evidencia fundamental de un caso desaparezca, pudiendo dejar impunes a todas las personas que han cometido un ilícito penal. Esto corrompe el espíritu de una sociedad y evita una reparación digna material y moral.

Considerando estas circunstancias, se ha llegado al punto de que varios particulares comiencen a retroceder hacia la época de la vengia privada, tomando justicia por su propia mano a falta de la confianza y eficacia que se tiene del sector justicia. Se puede decir que “es consecuencia de situaciones jurídicas propias que se han resultado inadecuadamente y que muchas veces ni siquiera se han intentado resolver”⁶. Esto provoca que no solamente corrompa un estado de derecho, sino que se cometan nuevos hechos delictivos.

1.2. Concepto

Para Samantha López el derecho penal es el: “conjunto de normas jurídicas (de derecho público interno), cuya función es definir los delitos y señalar las penas y

⁶Ibíd. Pág. 19.

medidas de seguridad impuestas al ser humano que rompe el denominado contrato social, y daña con su actuación a la sociedad.”⁷

Zaffaroni, Alagia y Slokar definen que: “el derecho penal es la rama del saber jurídico que, mediante la interpretación de las leyes penales, propone a los jueces un sistema orientador de decisiones que contiene y reduce el poder punitivo, para impulsar el progreso del estado constitucional de derecho.”⁸

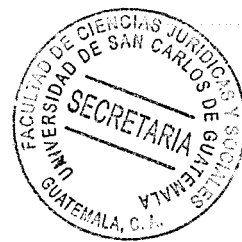
Y para Amuchategui: “el derecho penal es el conjunto normativo perteneciente al derecho público interno, que tiene por objeto al delito, al delincuente y la pena o medida de seguridad, para mantener el orden social mediante el respeto de los bienes jurídicos tutelados por la ley. De la noción anterior se colige que el derecho penal pretende preservar un equilibrio que dé seguridad a los miembros de la sociedad.”⁹

Por conclusión se puede definir al derecho penal como el área del derecho público interno, sistematizado de forma lógica por teorías, doctrinas, principios, instituciones y normas jurídicas que regulan al delito, las faltas, al delincuente, la pena o medida de seguridad, para mantener el orden social y reducir el poder punitivo para la conservación de un estado de derecho. Siendo esta una ciencia moderna y evolutiva de juzgamiento, regulación, prevención y rehabilitación de la actividad humana, creando normas enfocadas a conservar la paz y propagar la comisión del bien común en beneficio de la sociedad.

⁷ López, Samantha. **Derecho Penal I**. Pág. 12.

⁸Zaffaroni, Eugenio, A.A y A.S. **Derecho Penal, Parte General**. Pág. 5.

⁹Amuchategui, Griselda. **Derecho Penal**. Pág. 13.



1.3. Características

Las características del derecho penal son importantes para determinar la esencia de la ciencia, para lo cual de Mata Vela y de León, han determinado en su obra Derecho Penal Guatemalteco, que son las siguientes:

- A) Es una ciencia social y cultural: Porque estudia a una población en territorio y tiempo determinado para la formulación y creación de sus tipos penales y procesos penales más adecuados.
- B) Es normativo: Está ligado principalmente al principio de legalidad, donde los delitos, faltas, medidas de seguridad y las penas deben de estar plasmadas en una ley penal emanada por el poder soberano.
- C) Es de carácter positivo: Se basa en la vigencia e imposición que tiene la norma penal al ser creada por el órgano encargado de la función legislativa mediante el procedimiento de creación de leyes, el cual pasa a ser de observancia general.
- D) Pertenece al derecho público: Debido a la intervención que tiene el Estado en velar por la persecución penal y asegurar la ejecución de lo dictado. Mediante el derecho penal el Estado se encarga de administrar la justicia ante actos o hechos que hayan lesionado derechos tutelados de particulares o colectivos mediante una reparación y una pena, siendo el Estado el único capaz de sancionar. Esta sin duda es una característica muy relevante en esta materia.



E) Es valorativo: Realiza una valoración entre derechos, los cuales son fundamentales para establecer causas que eximen la responsabilidad penal, y circunstancias que modifican la misma, y el análisis jurídico entre el supuesto jurídico y la sanción a aplicar.

F) Es finalista: Porque tiene la finalidad de prevenir, regular, reprimir, controlar y erradicar las actividades delictivas dentro de un territorio determinado. Asimismo, tiene como fin crear las bases para juzgar los delitos y faltas y asignarles una sanción adecuada para la rehabilitación del delincuente y la reparación de la víctima y terceros civilmente interesados.

G) Es fundamentalmente sancionador: Es la potestad coercitiva que ejerce el Estado para sancionar los delitos dentro los límites legales establecidos en la ley penal.

H) Debe ser preventivo y rehabilitador: La prevención es la primera etapa que debe de fijar el derecho penal para poder cumplir con su función, porque no es mejor un Estado que más condena, sino aquel que menos índices de crimen tiene. Por ello la prevención es la primera etapa y la rehabilitación la última, para que el criminal pueda ser reincorporado a la sociedad para que sea de utilidad para ella y colabore con el avance social, cultural y tecnológico del país.

I) Fragmentario: También llamado de ultima ratio o de última instancia, debido a que hay otros medios de control que tiene el Estado para solventar controversias y estos deben de ser agotados antes para poder pedir la intervención de la fuerza coercitiva del

derecho penal mediante los órganos de justicia penal para solventar las situaciones.

1.4. Principios

Los principios son los “fundamentos o rudimentos de una ciencia o arte”¹⁰, siendo todas las directrices guía que brindan un camino a seguir en la aplicación del espíritu del derecho penal. Son los que crean la base de toda la normativa aplicada en el área penal cuya observancia y aplicación es obligatoria. Los cuales están regulados en el Código Penal Decreto 17-73 del Congreso de la república, siendo los siguientes:

A) Principio de legalidad: La Constitución Política de la República de Guatemala establece en su artículo 17: “No son punibles las acciones u omisiones que no estén calificadas como delito o falta y penadas por ley anterior a su perpetración” y acorde al artículo 1 del Código Penal, establece que: “nadie podrá ser penado por hechos que no estén expresamente calificados, como delitos o faltas, por ley anterior a su perpetración; ni se impondrán otras penas que no sean las previamente establecidas en la ley.” Asimismo, en el artículo 1 y 2 del Código Procesal Penal establecen que: “no hay pena sin ley” y “no hay proceso sin ley”. Por lo cual podemos establecer que este principio exige una norma penal que lo regule y que esté vigente antes de la comisión del hecho para poder procesarlo y sancionarlo.

B) Principio de extractividad: de conformidad con la Constitución Política de la República de Guatemala en su artículo 15 establece que: “la ley no tiene efecto

¹⁰ Cabanellas, Guillermo. *Diccionario de Derecho Usual*. Pág. 381.

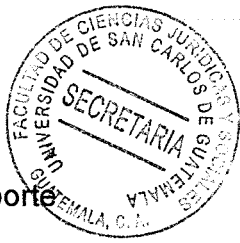


retroactivo, salvo en materia penal cuando favorezca al reo”; tal como establece la norma constitucional, este principio está basado en la aplicación de una norma penal fuera de su período de vigencia, pero debe de ser aplicado únicamente en beneficio del reo, pudiendo ser con aplicación de la norma con efectos hacia el pasado (retroactividad) o mediante la aplicación de la norma con efectos hacia el futuro (ultractividad).

C) Principio de ley excepcional o temporal: de conformidad con el artículo 3 del Código Penal Decreto 17-73 del Congreso de la República: “la ley excepcional o temporaria se aplicará a los hechos cometidos bajo su vigencia, aun cuando ésta hubiere cesado al tiempo de dictarse el fallo...”, por lo cual se deduce que existen leyes penales que son creadas para tener vigencia en un período corto o en un plazo fijo, para regular una situación de urgencia o conveniencia social.

D) Principio de territorialidad de la ley penal: Consiste en el imperio de la ley, el cual se extiende a todo el territorio nacional donde el Estado ejerce su soberanía, estableciendo que es de conocimiento y observancia obligatoria para todo aquel que se encuentre dentro del país. De conformidad con el artículo 4 del Código Penal Decreto 17-73 del Congreso de la República: “... este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción.”

E) Principio de extraterritorialidad de la ley penal: Regula las circunstancias en las cuales la ley penal guatemalteca va a ser aplicada en cuanto a la comisión de delitos



realizados en el extranjero, por la característica de tratarse de medios de transporte aéreos, marítimos y terrestres guatemaltecos o bien porque el autor de los delitos sean agentes diplomáticos o funcionarios en ejercicio.

F) Principio de sentencia extranjera: Este principio reconoce la autoridad de otros estados para juzgar delitos de guatemaltecos cometidos en el extranjero, asimismo le da el valor de veracidad de los hechos planteados en sus resoluciones, los cuales reconoce el Estado mediante el Código Penal Decreto 17-73 del Congreso de la República en su artículo 6 en el cual establece que: "...la sentencia extranjera producirá cosa juzgada."

G) Principio de exclusión de la analogía: También llamada analogía *ad malam partem*. De conformidad con el artículo 7 del Código Penal Decreto 17-73 del Congreso de la República: "por analogía, los jueces no podrán crear figuras delictivas ni aplicar sanciones." Este principio está relacionado con el de legalidad, obligando a los jueces a aplicar la normativa de forma gramatical.

H) Principio de extradición: Regula lo concerniente al movimiento migratorio de una persona para ser sometida a juicio penal en otro país que le reclama hechos en los que tuvo participación delictiva, para ello se debe de tomar en cuenta que para que esto sea procedente se debe de cumplir con: 1) debe de existir tratado internacional en materia de extradición; 2) el acto ilícito debe de ser delito en ambos Estados; 3) debe de ser en delitos sancionados con más de 1 año de prisión; y 4) aplica únicamente para delitos comunes, no políticos ni conexos.



I) Principio de leyes especiales: Establece que “la ley especial tiene vigencia preferente sobre la ley general, salvo ser ésta posterior e incompatible en alguna cuestión.”¹¹ Esto se aplica debido a que el carácter esencial de una ley penal especial es normar de forma adecuada un tema en específico que ha pasado por un riguroso estudio social, económico y criminológico.

2. Nociones fundamentales del derecho informático

Esta ciencia del derecho, es reciente, la cual nace de la necesidad de regular las actividades que realizan las personas en el ciberespacio mediante la utilización de nuevas tecnologías que permiten el acceso y divulgación de información de forma rápida y sencilla, la cual puede ser sensible y comprometer los derechos fundamentales, particulares y culturales dentro de una sociedad.

El derecho informático es utilizado por los Estados para regular procedimientos administrativos innovadores y para actualizar procesos judiciales de distintas materias con el uso de la tecnología, sin embargo, también es utilizado para el estudio, regulación y persecución de delitos informáticos, los cuales son cometidos en el ciberespacio y tienen un impacto directo en el mundo exterior.

Actualmente tiene gran relevancia esta área del derecho, debido que cada vez más personas tienen acceso a dispositivos inteligentes con los cuales pueden interactuar en el ciberespacio, el cual se encuentra englobado en el internet; cuyo acceso fue

¹¹Ossorio, Manuel. **Diccionario de Ciencias Jurídicas, Políticas y Sociales**. Pág. 544.

reconocido como un derecho humano por el Consejo de Derechos Humanos de las Naciones Unidas por medio de la resolución “promoción, protección y el disfrute de los derechos humanos en internet.”

2.1. Antecedentes

Desde el surgimiento de la computadora que comienza a partir del año 1940, se da el surgimiento de la informática y, con la creación del internet en 1969 al ser el resultado de un experimento del Departamento de Defensa de Estados Unidos, a solicitud del pentágono, que se materializó en el desarrollo de ARPAnet, la cual era una red que enlazaba a distintas universidades de Estados Unidos con centros de alta tecnología y contratistas militares.

Mediante su desarrollo se fueron uniendo distintas sedes de Europa y del resto del mundo formando lo que hoy se conoce como la gran telaraña mundial (Word Wide Web) y suple a ARPAnet en 1990, surgiendo la transmisión de datos informáticos a nivel mundial, lo cual brinda un mundo de información tanto pública como sensible que corre el riesgo de ser afectada al ser destruida, modificada o extraída para ocasionar un avance o un perjuicio a una persona o a una sociedad.

Tomando en cuenta la historia y la evolución que ha tenido la informática en su desarrollo, tanto en *Software* como en *Hardware*, es el momento en que surge la informática jurídica para hacer uso de tal avance informático, la cual es “el conjunto de aplicaciones de la informática (ciencia del tratamiento lógico y automático de la

información) en el ámbito del derecho”¹², es decir, es la técnica que permite que la información jurídica sea automatizada a través de sistemas informáticos.

Es por ello que al crearse los medios tecnológicos (computadoras, celulares, tabletas, etc.), y al estar conectados a internet, se le ha brindado al mundo una nueva modalidad para comunicarse, e interactuar en el comercio informático, redes sociales, banco de datos, finanzas, servicios, entretenimiento, entre otros. Siendo esto el origen del derecho informático, el cual nace para regular todos los acontecimientos nuevos que se derivan de la utilización de nuevas tecnologías que se relacionan con el ciberespacio.

2.2. Concepto

Para Jonatán es definido como: “el conjunto de normas jurídicas, principios y doctrinas, las cuales tiene como objeto regular toda la actividad informática dentro de la sociedad, yendo desde la regulación para los aparatos electrónicos físicos, como desarrollo e implementación de software dentro del entorno social.”¹³

De conformidad con Julio Téllez: “el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).”¹⁴ Por lo cual se puede decir que el derecho informático es una ciencia del derecho nueva y dinámica, que abarca su estudio en el área privada como pública. Está conformada por un conjunto de normas

¹²Telléz, Julio. **Derecho Informático**. Pág. 25.

¹³ Marroquín, Jonatán. **Informática Jurídica**. Pág. 8.

¹⁴**Ibíd.** Pág. 22.



jurídicas, principios, teorías, doctrinas e instituciones legales que estudian la relación e implementación de la informática en la diversidad de relaciones interpersonales, laborales y comerciales.

Para entender su objeto de estudio y diferenciarlo del derecho informático, se entiende que la informática “un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones”¹⁵ y aplicándolo al ámbito jurídico, mediante la informática jurídica, la cual es “el conjunto de aplicaciones de la informática (ciencia del tratamiento lógico y automático de la información) en el ámbito del derecho”¹⁶, es decir, es la técnica que permite que la información jurídica sea automatizada a través de sistemas informáticos, no siendo un área del derecho, ya que si nos referimos a dicha área reguladora nos adentramos con el derecho informático el cual surge ante la necesidad de regular la actividad informática de una sociedad.

2.3. Naturaleza jurídica

El derecho informático es un derecho autónomo, que cuenta con su propio objeto de estudio, el cual no se puede encasillar únicamente en el derecho privado o derecho público, porque atiende a aplicarse en ambas dependiendo del objeto de estudio en el que se desenvuelva en la práctica. Depende del modo de su utilización y estudio, dependiendo del medio para el cual es utilizado y por el motivo que se emplea.

¹⁵Ibíd. Pág. 5.

¹⁶Ibíd. Pág. 25.



En el campo del derecho privado se dedica a estudiar la utilización de la informática y su aplicación en actividades y contratos entre particulares en sus relaciones interpersonales, laborales y comerciales. Mientras que, en el área del derecho público, el derecho informático se dedica al estudio de las relaciones y aplicación de la informática entre los gobernantes y gobernados; además, se encarga del estudio de los delitos informáticos, sus formas de averiguación, persecución y sanción.

2.4. Relación con el derecho penal

Siendo el derecho penal el encargado de regular los delitos, las penas y la actividad criminal y, el derecho informático el encargado de estudiar y regular la actividad informática de una sociedad, se concluye en que ambas áreas del saber jurídico están relacionadas en el estudio, regulación, prevención, averiguación, persecución y sanción de los delitos informáticos, los cuales son actos ilícitos cometidos por medios informáticos, comprometiendo los datos personales, sensibles, el habeas data y economía de particulares y los Estados.

Capítulo II

1. El cibercrimen y el delito informático

De conformidad con Miró, el cibercrimen puede ser visto desde dos sentidos, los cuales son el normativo y el tipológico, para lo cual establece que el primero es el “conjunto de delitos del CP caracterizados por llevarse a cabo en el ciberespacio”¹⁷ y el segundo es el “comportamiento criminal en el ciberespacio, bien como categoría que incluye a todos (o algunos de) ellos.”¹⁸

El delito informático es definido por Alvarado y Morales como: “acción u omisión típica, antijurídica y culpable, que se realiza por medio de un sistema que haga uso de las tecnologías de la información o un componente de éste, o que lesione la integridad, disponibilidad o confidencialidad de la información.”¹⁹

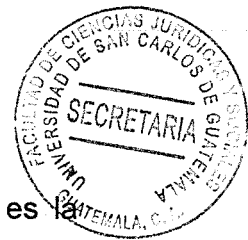
Para tener un concepto más amplio también incluimos otra definición que enriquecerá el conocimiento para poder entender más el objeto de estudio, por lo cual para Hans es: “toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener 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.”²⁰

¹⁷ Miró, Fernando. *El Cibercrimen. Fenomenología y Criminología de la Delincuencia en el Ciberespacio*. Pág. 40.

¹⁸ *Ibid.* Pág. 41.

¹⁹ Alvarado, José y R.M. *Cibercrimen*. Pág. 16.

²⁰ Noriega, Hans. *Delitos Informáticos*. Pág. 23.



Por lo cual se concluye que el cibercrimen es el género y el delito informático es la especie, entendiendo que el primero engloba a la totalidad de los delitos tipificados en una ley penal vigente y a la actividad que realiza el criminal en el ciberespacio; por el contrario, el delito informático es una acción típica, antijurídica y culpable que se lleva a cabo en el ciberespacio por medios informáticos, la cual es sancionada con una pena por comprometer los datos personales y sensibles, el honor y la economía de las personas.

1.1. Precedentes

El derecho penal se dedica al constante estudio y regularización de delitos y penas, sin embargo, su estudio se ha ido expandiendo por distintas áreas y derechos protegidos por el Estado, tales como los delitos enfocados al comercio, a la hacienda pública, al ambiente, al narcotráfico y grupos criminales organizados, entre otros, haciendo su estudio y aplicación cada vez más complejo.

Por tanto, es indispensable mencionar que el surgimiento de la regularización de los delitos informáticos es a causa de la creación de la computadora y el acceso a una interacción virtual por la cual se puede almacenar información y acceder a ella desde sitios remotos, generando una comunicación global y archivo de información privada de contenido comercial y personal que muchas veces no se quiere ser compartida y es vulnerada por un tercero, por ello la necesidad de contar con un ordenamiento legal adecuado y técnico para regular esta tecnología y la actividad informática que se ejecuta con la misma.



La vida de las personas y la sociedad en general comienza a cambiar desde ese momento, muchos comienzan a expandir sus horizontes para emprender en distintas áreas del actuar humano, y, asimismo, comienza el pensamiento del aprovechamiento del delincuente de cuello blanco, llamado así por ser un criminal que tiene amplios conocimientos en computación e informática.

“Uno de los primeros virus que afecta los sistemas informáticos aparece en 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 la 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.”²¹

A finales de la década de los 2000 se inició con la creación, distribución y venta de teléfonos inteligentes a nivel mundial, pero no fue hasta el año 2010 cuando se popularizaron tanto en el mundo como en Guatemala, de la misma forma surgieron las distintas redes sociales tales como Hotmail, Messenger, Facebook, entre otras; las cuales fueron cambiando los medios de comunicación y de comercio de una forma completamente radical, al igual que la creación de páginas informáticas mediante las cuales se hacia la compra y venta de productos a distancia, tal como lo es Amazon,

²¹Ibíd. Págs. 21 y 22.

EBay, AliExpress, entre otras, las cuales abrían una nueva venta para cometer ciberdelitos.

Por estos motivos países como Estados Unidos, Colombia, España, Perú y México se han preocupado por su constante estudio criminal, haciendo uso de la criminología para entender al cibercriminal, la víctima en potencia y los medios más susceptibles para la comisión de estos ilícitos, creando así sus propias leyes informáticas, regulando derechos informáticos y a la vez sus delitos, sanciones y medidas de seguridad.

En Guatemala, el tema del derecho informático y los delitos informáticos comenzó a ser tratado a partir del año 1996, mediante la aprobación del Decreto 33-96, el cual incluye reformas al Código Penal relativo a la inclusión de los delitos informáticos, asimismo cuenta con la Ley de Acceso a la Información Pública Decreto 57-2008, mediante el cual se establecen definiciones que son importantes para el derecho informático tales como los datos personales, datos sensibles y el habeas data.

Del mismo modo, existe la Ley de Equipos y Terminales Móviles Decreto 8-2013, la cual regula a los terminales móviles de comunicación, la cual brinda definiciones importantes para el estudio y tipificación de los delitos contenidos en dicha ley. También está regula la Ley de Implementación del Control Telemático en el Proceso Penal Decreto 49-2016, mediante el cual regula la aplicación del control a distancia de personas ligadas a proceso penal y que gozan de esta medida sustitutiva para poder verificar su ubicación y regular delitos que atenten contra la seguridad jurídica que implica la utilización del dispositivo tecnológico.



Actualmente Guatemala cuenta con estas últimas leyes en relación al delito informático, sin embargo, se ha cometido el error de no estudiar criminológicamente bajo estándares internacionales para actualizar los delitos informáticos contenidos en el Código Penal Decreto 17-73, ni se ha preocupado el Estado por regular la gran diversidad de nuevos actos cibercriminales que han surgido debido a las nuevas tecnologías.

Esto ha conllevado muchas veces a violar el principio de exclusión por analogía, adecuando los cibercrimenes a una variedad de delitos, cuando realmente se trata de uno, lo cual crea penas desproporcionadas y una mala prevención de delitos informáticos, debido a que la política criminal del estado y políticas públicas se ven reflejadas en estudios realizados a los biodelitos, no incluyendo a los informáticos, provocando que cada día sigan siendo vulnerados los derecho tutelados por medios tecnológicos mediante estafas, difamación, extorsión, hurto y otros delitos por medios electrónicos.

1.2. Clasificación de los delitos informáticos

Para poder entender mejor los delitos informáticos es necesario comprender que estos se clasifican para poder realizar un estudio más adecuado, tomando en cuenta la categoría a la que pertenecen.

Hans Noriega clasifica a los delitos informáticos en dos grupos de conformidad con nuestra legislación penal:



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."²²

Julio Téllez establece la siguiente clasificación de los ciberdelitos:

A) Como instrumento o medio: "En esta categoría tenemos a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito."²³

B) Como fin u objetivo: "En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física."²⁴

Son clasificados con base a si su finalidad es causar daño a un aparato tecnológico o su contenido, o bien, utilizarlo para ocasionar un mal a un tercero, asimismo tenemos que pueden clasificarse dependiendo del tipo de bien jurídico tutelado que vulnera.

1.3. La prevención de delitos informáticos

La prevención del delito es una de las características fundamentales del derecho penal, cuya esencia radica en estudiar la actividad criminal que afecta a un territorio y

²²Ibíd. Pág. 24.

²³ Téllez, Julio. *Op. Cit.* Pág. 105.

²⁴Ibíd. Pág. 106.



sociedad en un tiempo determinado con estudios criminológicos, seguidos de la planificación de programas que tiendan a coordinar acciones para ejecutar políticas públicas orientadas a brindar bases de prevención y mecanismos de custodia para evitar la comisión de delitos.

Cabanellas define a la prevención como: “finalidad atribuida a la ley para contener con su amenaza los impulsos delictivos”²⁵, de lo cual podemos establecer que la ley penal influye en la prevención de delitos mediante la regulación normativa de la actividad criminal por medio del tipo penal. El que un Estado se organice para crear delitos y establecer penas crea un estado de conciencia en la población sobre la relación de causa-efecto que puede provocar cometer un acto ilícito el cual está regulado y es sancionado por el poder punitivo del país.

De lo anterior Cabanellas establece una división en cuanto a la importancia de la ley penal en cuanto a prevención, estableciendo: “En este último aspecto, la prevención es de dos clases: una general, integrada por la conminación dirigida al conjunto social, en cuanto la pena significa un mal o privación de derechos aplicable al que quebrante el orden jurídico; o especial, la que obra sobre el delincuente al cumplir la sanción, como escarmiento que le disuade de la reincidencia, al comprobar que las penas no son simples amenazas verbales.”²⁶ De esto se establece que la prevención va enfocada a dos grupos de personas, siendo las que no han cometido un delito y los que ya han sido condenados por los mismos.

²⁵ Cabanellas, Guillermo. *Op. Cit.* Pág. 377.

²⁶ *Ibíd.*



Al hacer referencia a los delitos informáticos y su regulación para prevenir su comisión también se debe de tomar en cuenta lo que establece Miró al respecto: “la categoría del cibercrimen, más que por dar nombre a un grupo de tipos penales, resulta útil como categoría de base criminológica que sirve como referencia de un ámbito de riesgo que incluiría a todas las tipologías de comportamientos que utilicen la Red para la realización de comportamientos que atenten contra bienes considerados esenciales y que, en todo caso, puede posteriormente ser comparada con la categoría normativa en aras a descubrir si los tipos penales dan o no una respuesta adecuada al problema criminológico del delito en el ciberespacio.

El cibercrimen, cumple su función principal, por tanto, con la descripción y sistematización de las nuevas formas de afectación de los bienes más importantes en el ámbito de las nuevas tecnologías de la información y la comunicación, y, a partir de ahí, la valoración de las soluciones político-criminales adoptadas frente a las mismas, partiendo de la revisión de los tipos penales existentes y de la necesidad (o no) de modificación de los mismos. Las necesidades de intervención político-criminal frente al cibercrimen, sin embargo, no se agotan en la tipificación de nuevos preceptos penales, sino que las peculiaridades criminológicas y la incidencia de esa amenaza real en múltiples aspectos sociales es tal, que más importante que la correcta política legislativa sustantiva nacional, es la adaptación de las estructuras procesales y técnicas necesarias, especialmente a nivel internacional, para la prevención de su realización y la mejor investigación procesal de las mismas.”²⁷ Siendo la interpretación de Miró muy acertada.

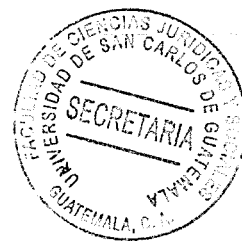
²⁷ Miró, Fernando. *Op. Cit.* Págs. 40 y 41.



De lo expuesto, se puede establecer que es imperativo realizar estudios criminológicos enfocados a ciberdelitos, exponiendo a detalle sus formas de comisión y medios utilizados, lo cual brindará datos que servirán para la modificación o no de los delitos informáticos vigentes o bien, la creación de unos nuevos. Pero también expone que solo la regulación no es suficiente para poder prevenir este tipo de delitos, sino que, además debe existir una estructura en el Estado para poder perseguir este tipo de agresiones, basándose en los modos de averiguación, persecución y juzgamiento.

Agregado a lo anterior y relacionándolo con Cabanellas, se concluye que ambos juristas se relacionan en su pensar. Cabanellas establece que, en la prevención de tipo especial, el condenado se rehabilita y evita la nueva comisión de delitos gracias a que fue debidamente oído y vencido en juicio con métodos eficaces que demostraron su culpabilidad y se da cuenta que el Estado se toma en serio su papel de juzgar a los criminales; mientras, Miró establece que, deben existir de forma necesaria una estructura y técnicas procesales para poder determinar esa culpabilidad, ya que sin métodos eficaces y un sector de justicia especializado sería imposible sancionar a los responsables por el grado de complejidad y conocimientos técnicos que se necesitan, lo cual conlleva a que el delincuente no sea sancionado y se le dé la oportunidad de volver a delinquir.

Hay criterios que argumentan en contra de la prevención ya que establecen que “resulta muy caro llevar a la práctica los planes propuestos, son lentos, se pone en duda su eficiencia y las técnicas aplicadas, dificultades en su realización, preferencias a establecer, así como otros problemas de tipo jurídico, político y derechos de las



personas que se deben respetar.

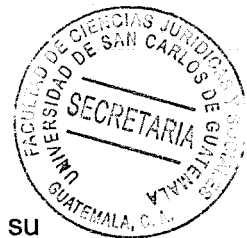
Combatir la criminalidad debe ser algo fundamental en los programas políticos de todos Los Estados; la tranquilidad y seguridad de las personas son los valores más apreciados por el ser humano. Sin embargo, hemos de apuntar que no es frecuente esa preocupación entre los gobernantes.”²⁸

De lo planteado se puede establecer que muchas veces los gobernantes prefieren ocupar sus recursos en otros temas o en combatir los efectos del crimen, sin embargo, esa no es una postura correcta, un Estado no es mejor en índices de lucha contra el crimen porque tiene la mayor tasa de procesos penales condenados, sino en cómo se ha organizado para evitar su comisión y tener el menor índice de criminalidad. Otro aspecto importante es el costo, el cual es aún más elevado reparando los daños causados y persiguiendo y juzgando a los delincuentes, que en prevenirlo.

1.3.1. La persecución, averiguación y juzgamiento de los delitos informáticos y su influencia en la prevención del delito

En materia penal, es obligación del Ministerio Público iniciar la acción penal, la cual puede ser de oficio, de oficio dependiente de instancia particular o de acción privada, dependiendo del tipo penal del que se trate. Esta organización es de las más importantes cuando se trata de materia penal, debido a que se encarga de la investigación y persecución penal.

²⁸ Serrano, Alfonso. *Criminología e Informática*. Pág. 444.



De conformidad con nuestro Código Procesal Penal Decreto 51-95, establece en su artículo 8 lo siguiente: “el Ministerio Público, como institución, goza de plena independencia para el ejercicio de la acción penal y la investigación de los delitos en la forma determinada en este Código, salvo la subordinación jerárquica establecida en su propia ley.

Ninguna autoridad podrá dar instrucciones al jefe del Ministerio Público o a sus subordinados respecto a la forma de llevar adelante la investigación penal o limitar el ejercicio de la acción...”

De conformidad con el artículo 30 de la Ley Orgánica del Ministerio Público existen 22 fiscalías especializadas dentro de las cuales encontramos:

- 1) Fiscalía de delitos administrativos
- 2) Fiscalía de delitos económicos
- 3) Fiscalía de delitos de narcoactividad
- 4) Fiscalía de delitos contra el ambiente
- 5) Fiscalía de asuntos constitucionales, amparos y exhibición personal
- 6) Fiscalía de adolescentes en conflicto con la ley penal
- 7) Fiscalía de la mujer
- 8) Fiscalía de ejecución
- 9) Fiscalía contra la corrupción
- 10) Fiscalía contra el crimen organizado
- 11) Fiscalía de delitos contra el patrimonio cultural de la Nación



- 12) Fiscalía de delitos contra la propiedad intelectual
- 13) Fiscalía de delitos contra la vida y la integridad de las personas
- 14) Fiscalía de derechos humanos
- 15) Fiscalía contra el lavado de dinero u otros activos
- 16) Fiscalía contra el delito de extorsión
- 17) Fiscalía contra la trata de personas
- 18) Fiscalía contra secuestros
- 19) Fiscalía de asuntos internos
- 20) Fiscalía contra el delito de femicidio
- 21) Fiscalía de la niñez y adolescencia
- 22) Fiscalía liquidadora

De lo expuesto, se entiende que es obligación del Ministerio Público organizarse para poder dar inicio a la persecución penal y elaborar las gestiones pertinentes para intimar los hechos en modo, tiempo y lugar y brindar una calificación jurídica del tipo penal, sin embargo, hay un déficit en este tema, debido a que no existe una unidad concreta dentro de esta institución pública que atienda directamente los casos de delitos informáticos, creando un déficit en las acusaciones o entendimiento de los casos para esclarecer los hechos en juicio.

Para la averiguación de los delitos informáticos el Ministerio Público se auxilia de la Policía Nacional Civil mediante la Sección de Delitos Cibernéticos. De conformidad con nuestro Código Procesal Penal Decreto 51-92, en su parte conducente del artículo 112, establece: "los funcionarios y agentes policiales serán auxiliares del Ministerio Público



para llevar a cabo el procedimiento preparatorio, y obrarán bajo sus órdenes en las investigaciones que para ese efecto se realice.”

De igual forma, el mismo cuerpo legal establece en su parte conducente del artículo 113: “Los funcionarios y agentes de policía, cuando realicen tareas de investigación en el proceso penal, actuarán bajo la dirección del Ministerio Público y ejecutarán las actividades de investigación que les requieran...”

Por lo tanto, el Ministerio Público está encargado de la acción y persecución penal, y, de gestionar todas las diligencias necesarias para la averiguación de la verdad, por lo cual se auxilia de la Policía Nacional Civil mediante su Sección de Delitos Cibernéticos, pero el problema radica cuando un fiscal es desconocedor de la informática, este puede solicitar diferente tipo de peritajes forenses digitales, pero si no sabe del tema ni dónde se debe de buscar la información, estamos ante una gran complicación que conlleva a que no se encuentren los medios de prueba electrónicos que son necesarios para demostrar aspectos de tipificación, participación, culpabilidad y daño causado.

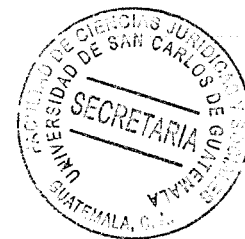
Con relación a lo mencionado, es importante resaltar que en Guatemala no existen tribunales de materia privativa para juzgar este tipo de delitos; estos son conocidos y juzgados por tribunales y jueces penales en sus distintas áreas.

De todo lo expuesto se tienen 2 factores que son obstáculos para lograr una buena prevención mediante el juzgamiento de los delitos informáticos, los cuales se deben de tomar en cuenta para este estudio:



- 1) No hay fiscalía especializada en materia de delitos informáticos: Esto conlleva a que los casos no puedan ser bien investigados por falta de conocimiento de la materia, agregado a ello, la mala litigación que se puede dar dentro del juicio y el planteamiento de la calificación jurídica errónea.
- 2) No hay tribunales especializados para juzgar este tipo de delitos: Lo peor que puede suceder en un proceso penal es que un juez o magistrado no conozca del tema. Puede que no conozcan la terminología informática empleada en juicio o los actos que se realizaron para cometer el delito, todo esto puede influir en una mala tipificación de delitos, una sanción desproporcional y a que criminales puedan salir absueltos.

En conclusión, no contar con fiscales y jueces especializados en la materia es lesivo para la seguridad jurídica de las personas y el Estado. Esto puede conllevar a una mala tipificación, una mala investigación, un mal entendimiento del caso y que criminales salgan absueltos o que nunca sean procesados por el mismo desconocimiento y falta de experticia para establecer los hechos y mostrar los medios de convicción adecuados. He ahí un motivo fundamental de que la prevención no esté funcionando, debido a que no se logra sancionar y por ende el criminal vuelve a reincidir por lograr salirse con su cometido.



Capítulo III

1. Generalidades de la criminología

Se sabe que la criminología es una ciencia utilizada por los estudiosores de la actividad criminal para lograr determinar aspectos que logran activar la mente criminal mediante la comisión de delitos. Estos estudios van dirigidos a estudiar a la mente criminal, la conducta de las víctimas, las razones que permiten que las personas sean vulnerables para ser violentadas en sus derechos y en esclarecer en general, todo aquello que engloba a la conducta delictiva.

Estos estudios van dirigidos con un enfoque social, de educación, prevención y combate contra el crimen. Se realizan mediante la aplicación de técnicas de investigación de primera y segunda mano y mediante el método científico, dependiendo del tema, será mediante el uso de la estadística, la historia, el estudio y razonamiento deductivo e inductivo, experimental y sociológico.

Esta ciencia nace de la antropología, sociología y psicología, la cual es utilizada por los distintos países para formular políticas públicas encaminadas a prevenir y combatir el crimen, de conformidad con los datos estudiados y recabados en cada uno de sus territorios, debido a que, en cada Estado, las modalidades y tendencias delictivas pueden variar por factores sociales y culturales. Es importante tomar en cuenta que la criminología actualmente es una de las ciencias más fundamentales cuando se trata de regir la conducta criminal para poder tener una mayor probabilidad de éxito.

1.1. Concepto

Para Hikal, la criminología: "es el estudio científico del individuo antisocial (criminal), de la conducta antisocial (crimen) de la antisocialidad en general (criminalidad) y de la prevención y tratamiento de estos a través de la política criminológica."²⁹

Rodriguez establece que es: "una ciencia sintética, causal, explicativa, natural y cultural de las conductas antisociales."³⁰

Olivera Díaz, en su obra *Criminología Peruana*, establece que es la "disciplina que a la vez explica y estudia las causas de la conducta delictiva y peligrosa, estudia también la persona del delincuente."³¹

De las anteriores definiciones se puede establecer que la criminología, es una ciencia autónoma por tener su propio objeto de estudio el cual es el criminal, el crimen y la criminalidad, de los cuales pretende descubrir aspectos causales, explicativos y culturales de los fenómenos del crimen para poder prevenir y combatir estas actividades contrarias a la moral y la ley mediante políticas criminales, formuladas, creadas, aplicadas y ejecutadas por los Estados para cumplir con su fin supremo, el cual es el bien común. Es una directriz para poder regular de forma adecuada la conducta criminal, brindando buenos parámetros mediante datos económicos, sociales y estadísticos de la conducta prohibida por la ley y la moral.

²⁹Hikal, Wael. *Introducción al Estudio de la Criminología*. Pág. 83.

³⁰Rodriguez, Luis. *Criminología*. Pág. 3.

³¹Olivera, Guillermo. *Criminología Peruana*. Pág. 50.



1.2. Relación de la criminología y el derecho penal

El derecho penal se encarga desde el punto sustantivo de la regulación de delitos, faltas, penas, medidas de seguridad y sobre la responsabilidad penal del criminal, y desde el adjetivo de su averiguación, persecución y sanción. Por el otro lado la criminología es utilizada para crear los delitos contenidos en la ley penal, para lograr una correcta interpretación y brindar un marco de análisis para su estudio.

La criminología es vista como una ciencia auxiliar del derecho penal, la cual le brinda los estudios antropológicos, sociales y psicológicos del delincuente y las víctimas, sumando aspectos estadísticos y culturales que permiten que los Estados se organicen de una mejor manera para lograr formular políticas criminales para prevenir la comisión de delitos (siendo esta finalidad de ambas ciencias) y además brinda bases sólidas para que el órgano legislativo pueda crear nuevos delitos o reformar los existentes o no, en base a las nuevas modalidades de comisión.

Ambas ciencias pretenden prevenir y combatir el crimen, sin embargo es necesario establecer que la diferencia entre ambas radica en que “El objeto de estudio del Derecho Penal lo constituyen las normas jurídicas de naturaleza punitiva que están vigentes en un lugar determinado, en tanto que el objeto de estudio de la Criminología son las conductas antisociales, estén o no contempladas y penadas por la ley.”³² Por ello se entiende que la criminología es vital para poder crear el tipo penal y para poder aprender de la evolución del delincuente y su nuevo ingenio para vulnerar derechos.

³²Rodriguez, Luis. Op. Cit. Pág. 90.



2. Cuasi-teoría de las criminologías específicas

A la criminología algunos la han categorizado como autónoma y como una verdadera disciplina científica porque tiene su propio objeto de estudio, el cual es el criminal, el crimen y la criminalidad, sin embargo, actualmente esta ciencia ha sido estudiada y se le han clasificado cuasi teorías, de las cuales surge la subdivisión de la criminología enfocada a distintas áreas de estudio, tales como la criminología social, familiar, educativa, laboral, biológica e informática.

De estas cuasi teorías nace lo se le categoriza como la “neocriminología”, la cual establece que el aspecto criminológico debe ser estudiado desde un tema específico y con técnicas de investigación y método adecuado para lograr obtener resultados satisfactorios para prevenir y combatir el crimen, pudiendo ser desde el punto de: el crimen organizado, el narcotráfico, violencia contra la mujer y por supuesto el cibercrimen.

2.1. Criminología informática

Área científica de la criminología que “Implica un estudio bastante extenso sobre los medios electrónicos y las conductas antisociales que se dan por el uso de un sistema electrónico como medio de comunicación. La Criminología Informática se dedica al estudio de las conductas antisociales de los delitos informáticos.”³³ Siendo su finalidad crear estrategias para prevenir y combatir la actividad criminal que surge en el mundo

³³Hikal, Wael. Op. Cit. Pág. 154.



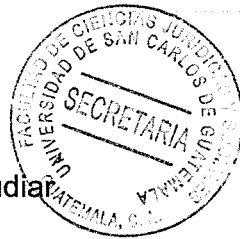
virtual y contrae repercusiones al mundo natural.

Este campo de investigación científica criminal está enfocado en el constante estudio del cibercriminal, el cibercrimen y la cibercriminalidad, la cual se realiza por medios informáticos en el ciberespacio, tendiendo a utilizar la tecnología para afectar y vulnerar los derechos de terceros o bien llevar a cabo acciones que tiendan a dañar equipos informáticos que contienen información personal, sensible o de archivo.

La criminología informática se encarga de estudiar el entorno informático, de los delitos que se cometen por medios digitales, mediante el apoyo de profesionales criminológicos y de expertos en materia informática y procesamiento de datos para lograr indagar a profundidad sobre las causas-efectos y de brindar estrategias de prevención y combate de los mismos, incursionando desde lo que es la seguridad informática corporativa, las redes sociales, los mercados virtuales, videojuegos y toda página o programa por el cual los internautas interactúan.

3. Factores de estudio para la criminología

Para la criminología existen muchísimos enfoques desde los cuales puede ser estudiada la actividad criminal para poder darle una explicación del por qué se realizan los delitos y qué causas lo motivan y ayudan a que sea realizado, y, es mediante este tipo de estudios que se logra entender a profundidad lo que es el criminal, el crimen y la criminalidad que afecta a una sociedad, datos que ayudan a un Estado a regular una adecuada normativa punitiva y preventiva.

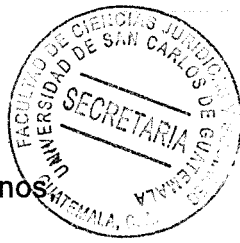


Para Alfonso Serrano algunos aspectos que se deben de observar a la hora de estudiar y crear un plan de prevención para los delitos informáticos son:

- a) "Edad y sexo de los autores
- b) Si nacieron en la ciudad donde delinquieron o proceden de zona urbana o rural, como consecuencia de movimientos migratorios.
- c) Lugar y zona de residencia
- d) Situación socioeconómica
- e) Algunos factores psicopatológicos
- f) Delitos cometidos por extranjeros y su situación (turistas, residentes, etc.)
- g) Peligrosidad y agresividad
- h) Modus operandi, ya estudiado
- i) Lugares más afectados
- j) Tipos de infracciones
- k) Actuación individual, en grupo o banda
- l) Reincidencia"³⁴

Alfonso establece que estos son unos de los muchos aspectos que se deben de investigar en los delitos, sin embargo, también es importante resaltar que estos aspectos van a variar y pueden ser objeto de estudio otros factores dependiendo del tipo de delito informático del que se trate, ya que cada uno tiene modalidades distintas de comisión, algunos necesitan de estudios más profundos y con auxilio de otras ramas científicas, por lo cual de igual forma se deben de considerar los factores que son

³⁴ Serrano, Alfonso. **Op. Cit.** Págs. 444 y 445.



utilizados por la criminología para el estudio criminal, siendo los criminógenos endógenos y exógenos.

3.1. Factores criminógenos

Son estudiados a partir de la criminopatología, la cual utiliza los estudios y auxilio de las ciencias de la psicología, biología, victimología, sociología y psiquiatría para revelar el verdadero origen de los delitos, aclarando el por qué se cometen y por qué se siguen cometiendo, busca una relación causa-efecto que logre descifrar la mente criminal y brindar bases sólidas para prevenir y combatir actos ilícitos.

Para entender la criminopatología y su enfoque de estudio para los delitos, se establece que "La Criminopatología, estudia: las conductas desadaptadas, antisociales y delictuosas en sus causas, consiste en proporcionar una descripción ordenada de todas las irregularidades de la conducta, cualquiera que pueda ser su grado de severidad, clasificándolas y tratando explicar cómo aparecieron. También se le podrá encontrar con el nombre de Criminología Etiológica-Multifactorial."³⁵

Al factor criminógeno debe de entendersele como aquel que es considerado como la causa que origina la conducta criminal, la cual es personal y que puede brindar bases teóricas para entablar una suposición del actuar delictivo, encuadrando un comportamiento o una razón psicológica o biológica que tienda a las personas a cometer delitos. Este factor es el más importante para lograr comprender la actividad

³⁵Hikal, Wael. Op. Cit. Pág. 159.



criminal y en el caso de los delitos informáticos, para lograr comprender el cómo, dónde y por qué se realizan.

Desde la antigüedad los criminólogos han establecido teorías tratando de formular una respuesta al factor criminógeno, tanto desde aspectos biológicos, que son manifestados en el ADN, como aspectos sociales y económicos del entorno en el que se encuentra la persona que comete el delito. Por esta razón de la criminopatología y del estudio del factor criminógeno se derivan los factores endógenos y exógenos.

3.1.1. Factores endógenos

Están considerados como causas provenientes de factores biológicos, los cuales pretenden dar una explicación al factor criminógeno y a la comisión de delitos. Estos se representan de forma externa mediante cambios físicos o alteración mental del sujeto que realiza la actividad criminal, los cuales surgen desde el nacimiento o mediante la vida del mismo, a través de actividades y sucesos que afectan su anatomía.

De este tipo de factores se ha establecido que tienen factores hereditarios, presentes mediante el ADN del sujeto, lo que ha conllevado a pensar que hay sujetos que nacen predispuestos a cometer un delito o es más probable que exista la peligrosidad de que esté tentado a realizarlo; de la misma forma, se establece que la edad es otro factor determinante y que abre la posibilidad de la comisión de ilícitos. Estos estudios se realizan mediante el estudio psicológico y médico, que buscan únicamente una respuesta biológica y científica para dar una explicación a la motivación criminal.

Dentro de los aspectos que se toman en cuenta en este tipo de estudios están: 1) los trastornos bioquímicos, de los cuales calculan cómo la cantidad de carbohidratos y proteínas afectan en el desarrollo emocional y mental de una persona (su alimentación y la serotonina); 2) condiciones congénitas, siendo su estudio durante el período prenatal, sobre como el consumo, por parte de los padres, de medicamentos, drogas u otras sustancias alteran a la persona; 3) el efecto de traumas y golpes, los cuales pueden llegar a alterar el cerebro incrementando la violencia en el sujeto; 4) efectos nutricionales y hormonales, los cuales afectan a las emociones y estados de ánimo; y 5) todos los trastornos mentales y de la personalidad que puede padecer el individuo (paranoia, antisocial, narcisista, dependiente, etc.).

3.1.2. Factores exógenos

Los factores exógenos pretenden dar una orientación y explicación de la actividad del criminal, tomando en cuenta los aspectos sociales, culturales y económicos que lo rodean, siendo influyente en el sujeto el ambiente natural y artificial que gira en torno a su crecimiento, interacción y desenvolvimiento en el mundo físico. Siendo el natural aquel que es creado por la misma naturaleza, que no tiene intervención de la voluntad y mano del ser humano, tomando factores como el frío, el calor, la lluvia, la sequía y cualquier otro aspecto que modifique el ambiente; por otro lado, el artificial, es el creado por intervención de la voluntad humana, tomando en cuenta los barrios donde reside una persona, la paz o perturbación, su núcleo familiar e interacción interpersonal, educación y medios de comunicación, entre otros aspectos que ayudan a formar su personalidad y costumbres.



WaelHikal en su obra introducción al estudio de la criminología establece que en los factores exógenos están: los factores exógenos físicos, factores familiares, economía, factores sociales y la educación.

De esta clasificación es importante resaltar su importancia al momento de estudiar los delitos informáticos analizando al cibercriminal:

- 1) Para determinar su condición de vida dependiendo de su zona de residencia y condiciones de vivienda (factores exógenos físicos).
- 2) Su relación familiar y conocer la educación y destrezas que hay en su entorno familiar que le haya ayudado a aprender de informática o que lo hayan influenciado a interactuar en el ciberespacio (factores familiares).
- 3) Si goza de buena economía para su sustento, educación y entretenimiento, si este es un factor que le impulsó a cometer el crimen o si fue necesario para que lograra adquirir el equipo necesario para delinquir (economía).
- 4) Para entender y analizar su entorno social, si se relaciona en cuestiones entorno a la informática como medio de trabajo, entretenimiento, comunicación, educación, para aislarse o como medio de expresión (factores sociales).
- 5) Determinar si el criminal se ha especializado en conocimiento y uso de tecnologías informáticas que le permitan un nivel más avanzado para lograr cometer crímenes de

esta categoría, debido a que “con mayores conocimientos es más probable que el antisocial salga más fácil de la situación en la que lo podrían descubrir”³⁶ (educación).

4. Política criminal

De León y de Mata Vela establecen que “la Política Criminal se encamina hacia su finalidad, que es la lucha y prevención consciente contra el delito; ella debe ser la maestra y la guía del legislador en la lucha contra el delito.”³⁷

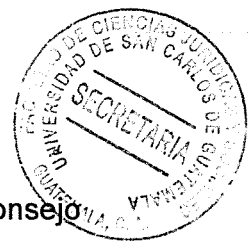
De lo anterior se constituye que la creación de una política criminal es uno de los fines de la criminología, la cual está enfocada en brindar las bases y procedimientos a tomar en cuenta por los Estados para prevenir, combatir y reprimir la criminalidad que los está afectando. Esta política es formulada y creada a partir de grandes estudios exhaustivos sobre la actividad criminal, estudiando el tipo penal normado y la criminalidad atípica, proponiendo estrategias gubernamentales para crear mecanismos de defensa, los cuales a veces, requieren de modificaciones normativas y creación de nuevas instituciones jurídicas o tipos penales para asegurar su efectividad.

4.1. Política criminal democrática del Estado de Guatemala 2015-2035

Guatemala cuenta con su propia política criminal para prevenir y combatir la criminalidad dentro del territorio nacional, la cual fue formulada en el año 2015 y tendrá

³⁶Ibíd. Pág. 185.

³⁷De Mata Vela y H. de L. Op. Cit. Pág. 34.

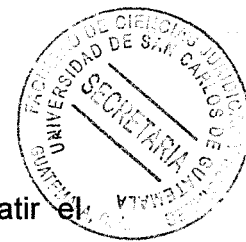


su periodo de aplicación hasta el año 2035. De esta surge la Comisión y Consejo Nacional de Política Criminal, conformada por el Ministerio Público y representantes de los tres organismos del Estado, representantes del sector académico y sociedad civil para estudiar la criminalidad, formular y presentar las políticas criminales y articular acciones interinstitucionales para su aplicación.

En la misma se encuentran estudios estadísticos demuestran la frecuencia de delitos cometidos dentro del país, siendo calculado por su comisión cotidiana en cada departamento, de cuyo estudio en dicha política se han seleccionado como delitos priorizados los siguientes: “delitos contra la vida e integridad de las personas, delitos contra el patrimonio de las personas, delitos contra la integridad y vida de las mujeres (violencia contra la mujer y femicidios), delitos contra la integridad e indemnidad sexual de los niños, niñas y adolescentes; delitos contra la seguridad y libertad de las personas; narcotráfico, contrabando aduanero, crimen organizado, trata de personas, extorsiones, tráfico de armas y delitos de lesa humanidad.”³⁸

De lo expuesto sobre esta política criminal es importante resaltar que su estudio está basado en delitos que suceden en el entorno físico, dejando de lado a los que se cometen por medio del ciberespacio (ciberdelitos), tomando en cuenta que los delitos informáticos son cada vez más comunes e incluso estos están superando su índice de incidencia que los biodelitos, no dejando pasar ni un solo día sin que se cometa un delito de esta categoría en el territorio nacional de conformidad con el Observatorio Guatemalteco de Delitos Informáticos.

³⁸ Ministerio Público. **Política Criminal Democrática del Estado de Guatemala 2015-2035**. Pág. 68.



El plan de prevención expuesto propone estrategias importantes para combatir el crimen, mediante la educación, creación de instituciones, reformulación de la aplicación de las penas y medidas de seguridad para sancionar como medidas alternativas a tratar con estos ilícitos para descongestionar la carga laboral que tienen los juzgados y centros penales, así como la revisión de normativa constitucional y ordinaria para ejecutar el plan propuesto. De esto es importante resaltar que dicho plan de prevención es adecuado para delitos cometidos en el plano físico, sin embargo, deja desprotegido el plano virtual.

Abordando al tema de prevención y combate del delito informático, y, observando el periodo de aplicación de la presente política criminal que es del año 2015 al año 2035, es importante recordar sobre el dinamismo del derecho, en especial del derecho penal y la informática, las cuales cambian con mayor frecuencia debido a la creación de nuevas tecnologías, dejando desprotegidas a las tecnologías de información y comunicaciones (TIC), por el hecho de no realizar estudios constantes en materia informática, por lo cual esta política criminal no es adecuada para la prevención y combate del cibercrimen.

4.2. Estrategia nacional de seguridad cibernética

La estrategia nacional de seguridad cibernética surge en 2018 por medio del Ministerio de Gobernación, debido al compromiso adoptado por Guatemala de dar cumplimiento a la resolución de la Organización de Estados Americanos AG/RES. 2004 (XXXIV-0/04) denominada como "Adopción de una estrategia interamericana integral de seguridad



cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética.”

Este estudio pretende fortalecer la seguridad cibernética en el Estado de Guatemala, además en fomentar la cultura de prevención y seguridad informática en el sector público, privado y la sociedad civil. Comprende estudios estadísticos la cantidad de personas que tienen acceso a aparatos tecnológicos y sistemas informáticos para relacionarse en el ciberespacio, asimismo determina la cantidad de vulneración que sufre la población y el Estado por la comisión de delitos informáticos, siendo un estudio general, no de fondo ni criminológico.

Mediante la presentación de este proyecto han establecido la necesidad de reforzar la seguridad cibernética del país, debido a que “En Guatemala, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales; tampoco existe normativa relacionada con la protección de datos personales.”³⁹Es por ello que pretende brindar una solución al problema proponiendo crear una cultura de seguridad cibernética, abrir espacios de educación en seguridad informática para profesionales y la población, estudiar la actividad criminal y su motivación en relación a delitos informáticos, crear marcos legales que regulen la actividad cibercriminal y sus medios de defensa. Siendo esto sumamente relevante, debido a que incluso un estudio por parte del Estado ha demostrado la deficiencia que tenemos de regulación legal en cuanto se refiere a la protección de la población por el medio informático.

Gracias a este plan, surge por el plazo de 4 años el Comité Nacional de Seguridad

³⁹ Ministerio de Gobernación. **Estrategia Nacional de Seguridad Cibernética**. Pág. 21



Cibernética, el cual está coordinado con la Secretaría técnica del Consejo Nacional de Seguridad, mediante el acuerdo gubernativo 200-2021 del Ministerio de Gobernación. Este está encargado de velar por el cumplimiento de la estrategia nacional de seguridad cibernética y de formular planes de gestión de crisis y amenazas informáticas. Es el encargado de mantener la seguridad informática dentro del Estado de Guatemala y actuar en momentos de ataques cibernéticos.

5. Convenio de Budapest y el compromiso de Guatemala

El Convenio de Budapest, es también llamado como Convenio Sobre la Ciberdelincuencia, el cual es creado por el Consejo Europeo. En el año 2016 Guatemala solicitó adherirse al mismo, ante la necesidad de crear mecanismos de defensa informáticos basados en normativa internacional aplicados a la realidad guatemalteca. Derivado de este compromiso, Guatemala ha presentado diversas iniciativas de ley para poder cumplir con el Convenio, entre las cuales encontramos: 1) Ley de Ciberdelincuencia; 2) Ley contra actos terroristas y; 3) Ley de Prevención y protección Contra la Ciberdelincuencia.

Es importante que logren ser aprobadas estas iniciativas, debido a que son formuladas con las directrices del Convenio de Budapest, el cual fue formulado por un arduo estudio criminológico en distintos países de Europa en cuanto a las modalidades de comisión de los delitos informáticos. Estas contienen definiciones, clasificación de delitos informáticos y medios de protección y prevención de las tecnologías de información y comunicación. Sin embargo, es necesario que las regulaciones de los



tipos penales sean enfocadas en la realidad guatemalteca, con base a un estudio criminológico exhaustivo.

Este convenio ha conllevado a Guatemala a ver la realidad de la importancia de brindar un mecanismo de protección legal para sus habitantes, los cuales se encuentran expuestos todos los días a ser víctimas de los delitos informáticos, los cuales evolucionan y cada vez son más lo que aparecen junto a sus modalidades de comisión. Guatemala tiene el deber y compromiso de enfrentar este vacío y desprotección legal que tiene, por ello cada vez existen más foros y personas estudiantes o profesionales que comienzan a involucrarse en el mundo del Derecho Informático, el cual ya tiene gran relevancia en la práctica y vida cotidiana del abogado y notario.



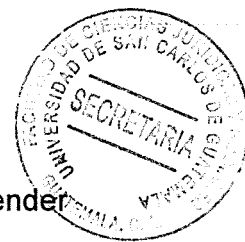
Capítulo IV

1. Teoría de las actividades cotidianas

Dentro de la criminología hay muchas teorías para el estudio de los delitos, las cuales se han formulado para prevenir de forma eficaz la comisión de delitos.

La teoría tradicional de las actividades rutinarias, la cual para Cohen y Felson, establecen que el delito se produce de forma efectiva cuando confluyen tres factores indispensables: 1) Un delincuente motivado a cometer el delito, 2) Una víctima propicia u objetivo alcanzable, 3) Ausencia de guardianes eficaces capaces de evitar el delito. Conforme a lo expuesto, esta teoría fue modificada y adaptada para el estudio del cibercrimen por Choi mediante su libro *Cybercriminology and Criminal Investigation* (Cybercriminología e Investigación Criminal), siendo los nuevos factores de estudio: 1) Ofensor motivado o cibercriminal, 2) objetivo adecuado o cibervíctima y, 3) una custodia digital.

En el año 2011 fue realizada en España una investigación por Fernando Miró, titulada “La Oportunidad Criminal en el Ciberespacio. Aplicación y Desarrollo de la Teoría de las Actividades Cotidianas para la Prevención del Cibercrimen”, en el marco del proyecto de investigación financiado por el Ministerio de Ciencia e Innovación, DER2011-26054, titulado “Cibercriminalidad: detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención

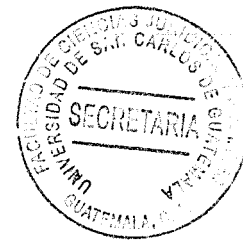


situacional criminológica.” De la cual Miró logró determinar la importancia de entender la conducta criminal y de la necesidad de reconocer que los delitos informáticos por ser cometidos por el ciberespacio necesitan de otro enfoque para su estudio.

Miró concluyó en su estudio que: “La utilización aquí de esta perspectiva criminológica para la recomendación de medidas preventivas frente a la cibercriminalidad, ni supone dejar de lado cualesquiera otras perspectivas más centradas en lo estructural, ni tampoco la consideración de que este enfoque es el central que debe tomarse en materia de prevención del delito. Simplemente, conlleva la afirmación de que, si el delito se produce en un espacio, el que se ejecuta en el ciberespacio debe ser distinto, y comprender el alcance de esta afirmación debe ser el primer paso para poder prevenirlo de forma eficaz.”⁴⁰

De ese modo se plantea que la teoría de las actividades cotidianas para el estudio de los ciberdelitos es adecuada, pero no debe de ser absoluta, ni se debe de dejar por un lado el fortalecimiento estructural del Estado para prevenir el delito. Es por ello que en esta investigación se adopta esta teoría para estudio del ciberdelincuente, la víctima y la custodia digital que va encaminada a la creación y adaptación de una política criminal que incluya un enfoque informático, que promueva bases de reforma, o no de delitos informáticos y brinde las modificaciones estructurales que necesita el Estado para prevenir y combatir estos ilícitos. De igual forma es importante resaltar que una teoría siempre puede ser superada por otra.

⁴⁰Miró, Fernando. **La Oportunidad Criminal en el Ciberespacio. Aplicación y Desarrollo de la Teoría de las Actividades Cotidianas para la Prevención del Cibercrimen.** Pág. 07:50.



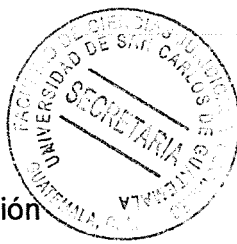
1.1. Ofensor motivado o cibercriminal

El criminal es aquel que pone en crisis la paz y seguridad de las personas dentro de una nación, violentando sus derechos y abusando de sus conocimientos y destrezas para aprovecharse de la debilidad de sus víctimas. De estos se encuentran los delincuentes primarios, reincidentes y habituales, de los cuales algunos planean sus malas acciones con antelación al acto y otros terminan realizándolos sin planificación, de forma espontánea.

Dentro del campo del derecho penal y derecho informático a este se le cataloga con el nombre de cibercriminal, cracker, o delincuente informático o cibernético. Estos además de llevar a cabo actividades ilícitas, también tienen conocimientos complejos en informática debido a que “Los delincuentes deben haber aprendido, además las habilidades apropiadas para delinquir”⁴¹, sin cuyos conocimientos o habilidades sería imposible su comisión.

Cuando se refiere al ofensor motivado, estamos hablando de un cibercriminal que se encuentra con las oportunidades para cometer un delito, los cuales confrontan a la ética y moral del sujeto y tienden a mostrarle los caminos necesarios para aprovecharse de sus víctimas por medio de sus habilidades y conocimientos en informática. Este infractor no solo se aprovecha de sus conocimientos sino también del desconocimiento que tienen sus víctimas, las cuales son vulnerables por no conocer de los métodos y técnicas de protección digital.

⁴¹ Anónimo. **Teoría de las Actividades Rutinarias**. Pág. 2.



Miró establece que “desde la perspectiva del agresor motivado, es que la comprensión del espacio que supone el ciberespacio incrementa las posibilidades de motivación de un potencial agresor motivado. Lo hace al menos por dos razones. La primera porque incrementa los objetivos potenciales sobre los que puede tomar la decisión de cuál es el adecuado, sin que la distancia ni el tiempo sean elementos esenciales de la decisión. La segunda porque reduce el coste espacio-temporal que supone prácticamente siempre cometer un delito, tanto en términos de llegar al objetivo como en el de asegurarse la huida una vez se ha cometido.

El que no exista un desplazamiento espacial y que el sujeto pueda ahorrarse tal coste, no significa que no haya un coste temporal para la realización de un ataque en el ciberespacio. Siempre lo habrá, y será mayor o menor dependiendo del tipo de cibercrimen.”⁴² Estos son unos de los aspectos que resalta en su investigación, la cual evidencia muchos elementos que deben de ser tomados en cuenta a la hora de estudiar a los cibercriminales, siendo estos importantes porque determina modos de motivación y aspectos que determinan la continuidad su actividad delictiva, estos aspectos deben de ser tomados en cuenta por todos los Estado a la hora de estudiar de forma criminológica la actividad cibercriminal.

De lo cual se puede establecer que, lo que se estudiará del mismo serán sus conductas cotidianas en el ciberespacio que lo motivan a cometer un acto ilícito, siendo por los beneficios propios que obtiene el criminal por su conocimiento, habilidad y capacidad de salir impune del acto sin ser identificado o sin que el delito logré ser detectado.

⁴²Miró, Fernando. *Op. Cit.* Págs. 171 y 172.



Asimismo, se tendrá en cuenta la forma de comisión de los delitos en cuanto a su preparación y ejecución y la selección de la víctima.

1.2. Objetivo adecuado o cibervíctima

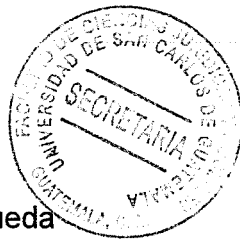
Para Ossorio la víctima es toda “persona que sufre violencia injusta en sí o en sus derechos”⁴³, de lo cual podemos establecer que es la que sufre de forma directa o indirecta de las acciones ilícitas del criminal, dejándola en un estado de afectación total o parcial en sus derechos, afectando su economía y/o estabilidad emocional. Por lo tanto, la cibervíctima, es aquella que es violentada en sus derechos mediante el uso de la informática, desde el ciberespacio.

Para la teoría de las actividades cotidianas es objeto de estudio la cibervíctima, para determinar las conductas habituales que realiza en el ciberespacio, lo cual crea oportunidades de ser objetivo adecuado de un delincuente cibernético, e igualmente para detectar los medios de prevención que toma o deja de tomar la víctima para crear un perfil llamativo para el criminal. “La presencia de objetivos o víctimas apropiados, visibles, descuidados, descontrolados. Son muchas las razones por las cuales se les llega a calificar de víctimas.”⁴⁴

Para que un criminal elija a su víctima, esta se encuentra propensa a ser examinada por él, mediante la información que proporciona de sí misma mediante el ciberespacio,

⁴³Ossorio, Manuel. *Op. Cit.* Pág. 984.

⁴⁴ Anónimo. *Teoría de las Actividades Cotidianas. Op.Cit.* Pág. 2.



debido a que no tiene una interacción física con el sujeto activo donde pueda evidenciar su información visual (objetos de valor que lleva, características físicas, su acompañamiento, etc.), por lo cual “Los usuarios del ciberespacio pueden, por tanto, eliminar del ámbito de ataque aquellos bienes que no incorporen el ciberespacio”⁴⁵, siendo ellos mismos quienes deciden qué información compartir con sus amistades, familia e incluso con los potenciales criminales.

1.3. Custodia digital

La custodia digital hace referencia a la protección informática que tienen los internautas en su navegación por el ciberespacio, resguardando su información personal y habeas data desde las nuevas tecnologías de información y comunicación por el cual se conectan, así como todas aquellas páginas y aplicaciones informáticas por las que mantienen una interacción, para lograr una adecuada defensa de intentos de ataques delictivos en su contra, siendo estos los que aseguran una correcta prevención y ejecución de medidas que eviten las violaciones digitales para evitar la victimización.

De la custodia digital surgen los guardianes capaces, de los cuales se ha establecido que debían de ser amigos, familia, terceros desconocidos, la escuela, entre otros que debían de brindar medidas de seguridad para ellos, su núcleo y terceros. Esto se debía de lograr con educación, brindar las herramientas de defensa, consejos y cualquier otro aspecto que ayudara a alguien para evitar ser objetivo de un criminal. Esta custodia debería de iniciar desde el momento en que un niño toca un dispositivo informático.

⁴⁵Miró, Fernando. Op. Cit. Pág. 181.



De igual forma existen los guardianes autónomos que se implementan en el ámbito informático, entre los cuales se encuentran los antivirus y *firewall* (corta fuegos), siendo los primeros, los que protegen los datos digitales, evitando la instalación y ejecución de virus, gusanos informáticos, troyanos, *adware* y *spyware* por medio de la negación de instalación y la eliminación de los mismos, mientras que los corta fuegos aseguran la seguridad de los datos dentro de la interacción con la red (no de los archivos dentro del dispositivo que fueron instalados, de eso se encarga el antivirus), brindando mecanismos de defensa ante redes de internet de dominio público y privado.

Estos sin dudas son guardianes de suma importancia para lograr una adecuada custodia digital debido a que “los estudios empíricos demuestran que tales sistemas pueden ser muy eficaces para evitar la victimización por el cibercrimen. Así, Yucedal constata que el uso de instrumentos digitales de seguridad, tales como cortafuegos, antivirus o programas *antispyware* como guardianes capaces, determina el riesgo de victimización, y a las mismas conclusiones llega Choi respecto al que él considera como elemento esencial”.⁴⁶

Por otro lado, Fernando Miró establece que “Lo relevante, en todo caso, no es situar los antivirus, cortafuegos y demás en el lado del triángulo del objetivo adecuado o de la ausencia de guardián capaz, sino reconocer que en la conjunción de estos elementos, y por tanto, en la propia prevención del delito, la víctima juega un papel preponderante en el caso del cibercrimen, dado que de ella depende en parte, no sólo su adecuación como objetivo (las dos íes, Introducción e Interacción), sino también su propia

⁴⁶Ibíd. Pág. 188.



autoprotección, pues será ella la que defina los guardianes capaces que la protegerán al tener sistemas antivirus, al actualizarlos, al incorporar otros sistemas de detección de software de riesgo, al actualizar el sistema siempre que se pueda, etc. El guardián capaz, en el ciberespacio, es prácticamente un auto guardián que depende de la propia víctima.”⁴⁷

De lo cual se concluye que para lograr una debida custodia digital deben existir guardianes capaces para proteger a las personas y sus derechos en el espacio digital, donde un factor determinante es el aporte que se brinda por terceros y la utilización de guardianes autónomos digitales, pero siendo la más importante la que realiza la víctima en potencia para poner en marcha las medidas necesarias para prevenir el delito, siendo esto objeto de estudio de la teoría de las actividades cotidianas.

2. Aplicación de la teoría de las actividades cotidianas en el estudio de los delitos informáticos

La teoría de las actividades cotidianas, al ser criminológica debe de ser practicada por criminalistas y profesionales en materia informática, mediante la intervención del Ministerio Público, los tres organismos del Estado, grupos gremiales y sociedad civil.

El estudio debe de ir dirigido a los delitos informáticos ya regulados en el Código Penal, los cuales se encuentran en el libro II, título VI, capítulo VII, delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, los cuales entraron en vigencia

⁴⁷Ibíd. Pág. 189.



mediante el decreto 33-96 del Congreso de la República (siendo estos los únicos catalogados dentro del Código Penal como delitos informáticos), para lograr determinar si su tipificación, juzgamiento y sanción son adecuadas al contexto actual en Guatemala y si se han logrado condenar; lo cual brindará datos estimados para saber si necesitan ser o no reformados.

Considerando que existen delitos informáticos atípicos (referente a los delitos regulados y que no se encuentran catalogados en el Código Penal como delitos informáticos y a los que tienen ausencia de un tipo penal que regule a un delito informático reconocido por estándares internacionales) es necesario que se practique el estudio a los demás delitos que protegen a los derechos tutelados por el Estado contenidos en los 15 títulos del libro II del Código Penal y a los actos denunciados por la población sobre cibercrimitos reconocidos internacionalmente pero que carecen de regulación interna (*pishing, scam, spam, ciberspionaje, sexting, online hatespeech, ciberterrorismo, entre otros*).

Por medio del estudio criminológico mediante la aplicación de la ciberteoría de las actividades cotidianas se podrá estudiar en cada delito informático: a los cibercriminales, enfocado en sus actividades cotidianas y medios que lo motivan a cometer el crimen, seleccionar a su objetivo, su modo de preparación y ejecución; a las cibervíctimas, mediante sus actividades rutinarias y aspectos que lo hacen ser un objetivo adecuado; y la custodia digital, determinando la falta de guardianes capaces (por terceros, el estado, guardianes autónomos y por la misma víctima), y descubriendo las medidas de seguridad y prevención digital adecuadas que se deben de tomar para



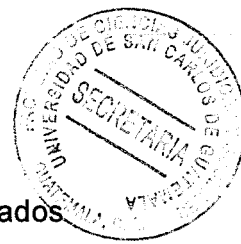
cada categoría de delito informático.

El estudio realizado servirá para plantear, crear y ejecutar una política cibercriminal por parte del Estado de Guatemala, para poder establecer los modos de comisión y averiguación de los delitos informáticos, las estrategias y fortalecimiento institucional para prevenir, combatir y juzgar a la cibercriminalidad y por supuesto, para proponer modificaciones en cuanto a la regulación de los delitos informáticos, planteando la necesidad o no de reformarlos, o bien, de crear nuevos tipos penales.

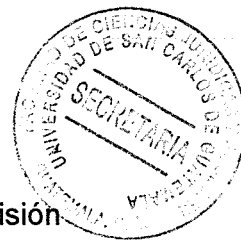
3. La práctica, su tipificación y su influencia en la prevención

Para lograr entender cómo se ha estado interpretando y juzgando a los delitos informáticos, es necesario entrar a conocer como han sido resueltos los mismos por los jueces y magistrados del país, lo cual brindará datos sobre tipificación, valoración de la gravedad del mal causado, la peligrosidad y las penas a imponer. Por lo cual se procede a hacer el siguiente análisis jurídico de la resolución judicial contenida en el expediente: 2352-2019 de la Corte de Constitucionalidad, el cual establece:

“Procede entonces, entrar a analizar si, al conocer el recurso por los motivos de fondo invocados, el Tribunal de Casación, actuó conforme a derecho, o si, por el contrario, incurrió en los vicios denunciados por el postulante. Así las cosas, se advierte que la Corte Suprema de Justicia, Cámara Penal, llevó a cabo el estudio respectivo sobre el fallo de apelación especial, en concordancia con el caso de procedencia invocado, esto a efecto de determinar si, efectivamente, concurrían los vicios *in iudicando* denunciados



y, una vez realizado el análisis correspondiente, partiendo de los hechos acreditados ante el Tribunal de Sentencia, determinó, que en el caso sometido a su conocimiento, contrario a lo alegado por el recurrente, sí se configuró la relación de causalidad entre las conductas desarrolladas por el procesado y los tipos penales por los que fue condenado; toda vez que se acreditaron, ante el sentenciante, los elementos esenciales para encuadrar los delitos de **Estafa propia**, Manipulación de información y Uso de información, todos en forma continuada, toda vez que **el sentenciador acreditó que el procesado envió correos electrónicos a los cuentahabientes de la entidad bancaria, con el objeto de engañarlos y obtener los datos de sus cuentas, con lo cual logró perjudicarlos en su patrimonio.** Asimismo, respecto al delito de Manipulación de información, Cámara Penal indicó que en el proceso penal se tuvo por probado que el procesado utilizó registros informáticos de computación para alterar información requerida por la institución bancaria, con el objeto de verificar el origen lícito del dinero depositado, para dar cumplimiento a una fingida obligación respecto al Estado y, en cuanto al delito de Uso de información, estimó que quedó acreditado ante el Tribunal de Sentencia que el procesado, sin la autorización de la entidad bancaria, utilizó sus recursos informáticos e ingresó a su base de datos y archivos electrónicos de sus clientes a través de la operación fraudulenta denominada *phishing*, con el fin de adquirir información confidencial, concluyendo que se daban las relaciones de causalidad por cada uno de los ilícitos antes mencionados, toda vez que se tuvieron acreditados los elementos esenciales del tipo. Del análisis anteriormente realizado, este Tribunal estima que la Cámara objetada analizó la totalidad de los hechos acreditados ante el sentenciante y los encuadró en los tipos penales correspondientes, inclusive, en lo atinente al tipo regulado en el artículo



274 "E" del Código Penal (Manipulación de información), por lo que la omisión objetada, respecto de que la Sala no advirtió que el Tribunal de Sentencia condenó por un delito inexistente (*"Manipulación en forma continuada"*), queda descartada, debido a que la Cámara encuadró debidamente los hechos delictivos.

Asimismo, partiendo de los hechos acreditados, así como de la integralidad de la sentencia, Cámara Penal determinó que no se vulneró el artículo 65 del Código Penal, en tanto indicó que el Tribunal Sentenciador tuvo por acreditado circunstancias que agravaron el mínimo de las penas impuestas, ya que estuvieron basadas en el principio de elasticidad de las penas reguladas para cada delito, lo cual fue debidamente interpretado en base al artículo 65 del Código Penal, toda vez que se observó los parámetros para cada delito de Estafa propia, Manipulación de información y Uso de información, así como el aumento de dichos parámetros por haberse calificado todos los delitos en forma continuada como se indica en el artículo 66 del citado Código, determinando una pena justa y proporcional para las conductas y circunstancias acreditadas por el Tribunal de Sentencia. Indicó, además, que **fue analizado y justificado la intensidad del daño causado, el cual fue debidamente interpretado en las condiciones que rodearon el hecho teniendo un resultado gravoso para las víctimas y sistema bancario guatemalteco, provocando lesiones en la propiedad privada y el patrimonio.** Determinó que el móvil del delito fue en menoscabo del patrimonio de las víctimas, habiendo actuado el procesado con total irrespeto hacia la sociedad guatemalteca, lo cual se considera debidamente interpretado, toda vez que los delitos cometidos tienen una trascendencia personal y social, dañando a la víctima y la información en registros bancarios; determinó que **la circunstancia agravante de premeditación, se interpretó debidamente**, ya que el procesado al abrir las cuentas



personales en el banco agraviado para el cual trabajaba, lo hizo deliberadamente para de delinquir, y según el Tribunal de Sentencia ya estaba en la mente del procesado, tal como quedó acreditado ante él; **estimó que el procesado no se encuentra dentro de los índice de peligrosidad, contenidos en el artículo 87 del Código Penal, dicho parámetro no fue tomado en cuenta para imponer la pena de prisión, por tanto fue interpretado erróneamente por la Sala;** advierte que fue debidamente interpretado el artículo 65 del Código Penal, con relación a la determinación de pena de prisión, de los artículos 50, 52 y 53 del citado Código, estimando que fue debidamente interpretado el artículo 50 del Código Penal, toda vez que se indica que serán conmutables las penas de prisión que no excedan de cinco años y, siendo que **en el presente caso las penas impuestas por cada delito suman un total de siete años y seis meses de prisión**, esto deriva en que las penas de prisión sean inconvertibles. Asimismo, Cámara Penal señaló que se interpretó apropiadamente por el Tribunal de Apelación Especial los hechos acreditados, estableciendo que **utilizaron conocimientos cibernéticos complicados, manipulando alojamiento en servidores de Francia y Venezuela, utilizando el método *fishing*, perjudicando a personas particulares y, al sistema bancario nacional y, por ende, a la sociedad de Guatemala.**”

3.1. Delitos condenados

En el expediente se encuentra sancionada la acción por los delitos de estafa propia, manipulación de información y uso de información. Estos lograron ser encuadrados en el tipo penal regulado en los artículos 263, 274 “E” y 274 “F” del Código Penal, de los

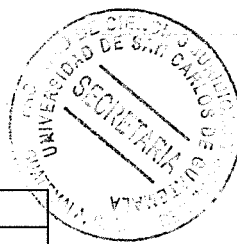


cuales sólo 2 están catalogados como delitos informáticos, dejando al delito de estafa propia como el único que no entra en esta categoría.

El Código Penal en su artículo 263 establece: “Estafa propia. Comete estafa quien, induciendo a error a otro, mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno.” De lo cual se logra verificar que el tipo penal no menciona el medio por el cual se deba de realizar la estafa (únicamente dándole importancia a la acción), dejando libertad a los que intervienen en el proceso penal de utilizar la analogía para encuadrarlo en la acción de engaño por medios informáticos, tal como en el presente caso.

La pena fijada para el condenado fue de 7 años y 6 meses de prisión, por la suma total de los 3 delitos atribuidos en forma continuada, en la cual tomaron en cuenta la premeditación como factor agravante de la pena y la valoración del daño causado al sistema bancario guatemalteco, a los cuentahabientes y a la sociedad guatemalteca.

De la pena se realiza el siguiente cuadro del caso planteado en la sentencia se ha podido verificar la pena mínima y máxima de prisión de cada delito condenado, para brindar una referencia entre mínimo y máximo que se le pudo haber impuesto al imputado y compararla con la pena que se le impuso de conformidad con la valoración de los aspectos para fijar la pena antes mencionados, siendo esto fundamental para entender si los jueces están aplicando de forma proporcional y equilibrada las penas de este tipo de delitos. Es importante determinar si las sanciones están de acuerdo al delito cometido y en la forma de su comisión.



Delito	Pena mínima	Pena máxima
Estafa propia	6 meses	4 años
Manipulación de información	1 año	5 años
Uso de información	6 meses	2 años
	Mínimo total: 2 años	Máximo total: 11 años

Observando la tabla, se puede apreciar que la condena superó por mucho el mínimo que se podía fijar que era de 2 años de prisión, por lo cual se observa que el tribunal que fijó la condena observó aspectos que a su criterio y según lo demostrado en juicio implicó el aumento, de conformidad con los agravantes y la valoración del daño causado, que a criterio personal, fueron interpretados de forma correcta, dejando los 3 años y 6 meses restantes para llegar a la pena máxima total al no tomar en cuenta los factores de peligrosidad, por no encontrarse enlistado en el artículo 87 del Código Penal.

3.2. Delito informático atípico mencionado

En la sentencia en la que resuelve la Corte de Constitucionalidad se logra la identificación del delito informático reconocido internacionalmente como *pishing* o *fishing*, el cual no se encuentran regulado en nuestra ley penal, sin embargo, es mencionado en la resolución para poder darle una mejor interpretación a la actividad criminal que se examina en el expediente por parte de los juzgadores.

Para entender este delito informático es necesario puntualizar qué es, siendo el *Pishing*: "Definido por el grupo mundial *antiphishing* como el mecanismo criminal que



emplea ingeniería social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias.”⁴⁸

El término *fishing* (pescar), está relacionado con la actividad que realiza el ciberdelincuente al colocar los cebos por medios informáticos (mensajes electrónicos solicitando información haciéndose pasar por otro, colocando enlaces que conducen a páginas fraudulentas que recaban información importante como contraseñas, etc.), esperando únicamente a que la persona cometa el error de morderlo y caer en la farsa, convirtiéndola en víctima, perdiendo sus datos y perjudicando su patrimonio.

3.3 Conclusión y aspectos relevantes de la práctica y su influencia en la prevención

Se concluye de la sentencia anteriormente expuesta y del análisis jurídico realizado que el delito de uso de información y manipulación de información fueron tipificados de forma correcta, de conformidad con el derecho positivo y a la rigidez de interpretación de la ley penal, debido a que las acciones fueron ejecutadas por medios y conocimientos informáticos para obtener la información de las víctimas y para tratar de ocultar el delito. Sin embargo, en la aplicación del delito de estafa propia se queda corto ya que regula una acción penal no dirigida específicamente en el espacio digital, recordando el principio de exclusión de la analogía regulado en el artículo 7 del Código Penal que establece: “Por analogía, los jueces no podrán crear figuras delictivas ni aplicar sanciones.”

⁴⁸Ibíd. Pág. 72.



El tipo penal debe de ir encaminado a regular una conducta determinada, no puede dejarse una ventana abierta que de paso a interpretaciones, tal como se está haciendo al querer aplicar el delito informático de *pishing* como estafa propia; no es lo mismo que ese engaño sea realizado por el medio físico que por medios digitales, su forma de comisión, complejidad, preparación, averiguación y daño causado están a niveles completamente distintos, por ende, no se puede pretender aplicar una sanción igual para ambos casos.

En el expediente estudiado se sancionó con pena de prisión y multa, sin embargo, es necesario entender que para lograr una correcta rehabilitación del delincuente y cumplir con la prevención especial es necesario proponer otras sanciones accesorias que estén enfocadas a ciberdelincuentes, tal como privación de acceso a tecnologías de información y comunicación, redes, inhabilitación especial o absoluta dependiendo del delito informático del que se trate.

Los delitos informáticos están siendo condenados en Guatemala, sin embargo, en muchas ocasiones (como en el presente expediente), los tipos penales ya regulados, están siendo interpretados por analogía para poder sancionarlos; esto vulnera a los derechos de los imputados y evita la formulación de sanciones adecuadas para rehabilitar al ciberdelincuente y evitar que vuelva a cometer un delito en el futuro.

Es por estos motivos que es importante la inclusión de los delitos informáticos atípicos en la ley penal guatemalteca, cuya relevancia de comprensión, estudio y regulación quedan evidenciadas en el expediente de la Corte de Constitucionalidad, en el cual



hacen alusión de ellos para que el juzgador pueda entender mejor el delito cometido debido a que muchas veces el tipo penal usado se queda corto en cuanto a su regulación.

Este problema no solo se ve reflejado en este caso, sino en muchos más, y es menester traer el comentario plasmado en la Estrategia Nacional de Seguridad Cibernética formulada en 2018, en la cual establece que: “De la misma forma, el delito relacionado con pornografía infantil, no se encuentra incluido dentro del marco jurídico nacional como delito cibernético, sino que está regulado en el Decreto del Congreso de la República 9-2009 Ley contra la violencia sexual, explotación y trata de personas. Sin la tipificación apropiada de los delitos cibernéticos, el sistema de justicia guatemalteco no puede sancionar de manera adecuada este tipo de delincuencia y se le dificulta la coordinación a nivel internacional sobre este tema, haciendo del país un paraíso para los delincuentes cibernéticos.”⁴⁹

4. Propuesta de solución a la problemática planteada

Para que Guatemala pueda estar a salvo a ataques informáticos y prevenir la comisión de los mismos, de primero debe de estar informado y entender que los delitos realizados por el ciberespacio son actos criminales distintos a los realizados en el espacio físico. Partiendo de esta primicia, se debe de comenzar por realizar estudios criminológicos con la utilización de la teoría de las actividades cotidianas más los factores criminógenos, endógenos y exógenos, en cuanto a los delitos informáticos

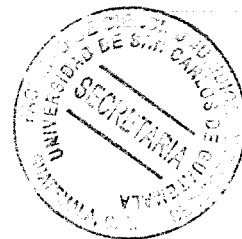
⁴⁹ Ministerio de Gobernación. Op. Cit. Pág. 21

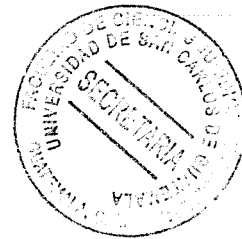


atípicos y típicos que se encuentran en el Código Penal y aquellos que son reconocidos por la comunidad internacional.

Los estudios criminológicos de estos delitos proporcionarán datos de las modalidades de comisión, causas, efectos, la ausencia de guardianes, las condiciones de objetivos adecuados y la necesidad de implementar aspectos que contribuyan a una custodia digital eficaz para prevenir el delito informático, atendiendo a la realidad guatemalteca. Teniendo estos datos se debe de proceder con la formulación de una política criminal del Estado de Guatemala con enfoque de delitos cibernéticos, mediante la cooperación del Ministerio Público, los tres organismos del Estado, grupos gremiales y sociedad civil.

Dentro de la política criminal se deberán abordar los aspectos del estudio criminológico con aplicación de la teoría de las actividades cotidianas, en cuanto al estudio del ciberdelincuente, la cibervíctima y la custodia digital, brindando parámetros que sean de ayuda para los legisladores para crear nuevos delitos informáticos y de reformar o no, los que se encuentran en vigencia dentro del Código Penal Decreto 17-73 del Congreso de la República. Asimismo, basado en el apartado de custodia digital, la política criminal deberá establecer los parámetros de fortalecimiento institucional del Estado para prevenir, combatir, juzgar, condenar y erradicar la cibercriminalidad en Guatemala.



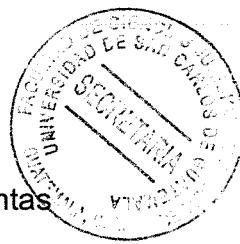


CONCLUSIÓN DISCURSIVA

Es evidente la falta de atención que tienen los delitos informáticos en Guatemala, los cuales se cometen todos los días dentro del territorio nacional. Esto conlleva a una gran vulneración de derechos de los habitantes, debido a que, al no existir estudios constantes y actualizados de los modos de comisión de los ciberdelitos, deja un vacío legal que tanto abogados, fiscales y jueces han estado tratando de acoplar por analogía a tipos penales que sancionan actividades que se realizan por el espacio físico, no por el digital.

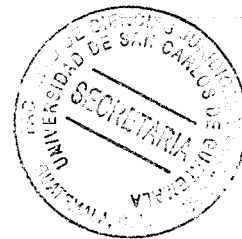
Que el Estado de Guatemala se comprometa a adherirse a convenios internacionales en combate y prevención de la cibercriminalidad es algo positivo, sin embargo, no es suficiente únicamente tener la palabra de decirlo, sino que debe de implementar estudios y crear políticas criminales enfocadas al combate de ciberdelitos, los cuales han sido excluidos de la política criminal democrática del Estado de Guatemala 2015-2035; si no hay estudios criminológicos sobre la comisión de estas modalidades dentro del territorio, el Organismo Legislativo no puede tener bases sólidas para regular un delito informático que esté plenamente adaptado a la realidad nacional y las reformas institucionales para combatir y prevenir estos ilícitos.

Al lograr entender la modalidad de los delitos cometidos en el ciberespacio, se podrán obtener los datos necesarios para establecer el tipo penal junto con sus penas y medidas de seguridad adaptadas al tipo de delito ejecutado, lo cual brindará medidas que ayuden al sector justicia para una correcta interpretación de lo ejecutado y de los



medios probatorios necesarios para esclarecer la verdad, lo que a final de cuentas contribuirá con una adecuada prevención del delito de forma general, al ser testigo la sociedad de que el Estado de Guatemala está capacitado para investigar, juzgar y sancionar los delitos informáticos; y desde un punto especial, mediante la adecuada rehabilitación del ciberdelincuente, logrando que este no vuelva a cometer un delito y sea un ciudadano de provecho para el país.

Por tanto, es importante resaltar que al tener un estudio criminológico de los delitos informáticos cometidos en Guatemala y los reconocidos internacionalmente, se brindará datos para establecer si hay necesidad o no de reformar los delitos contenidos en el Código Penal o, si es necesario la creación de nuevos tipos penales que sancionen nuevas conductas producto de las nuevas tecnologías. Asimismo, ayudará a verificar la ausencia de guardianes capaces para asegurar los derechos en el ciberespacio, y cómo puede el Estado formular cambios dentro de su estructura para combatir, investigar, sancionar y principalmente, prevenir estos ilícitos.



Bibliografía

ALVARADO, Rolando y MORALES, Ronald. **Cibercrimen**. Primera edición. Guatemala: Ed. IUS ediciones, 2012.

AMUCHATEGUI, Griselda. **Derecho Penal**. Cuarta edición. México: Ed. Oxford UniversityPress México, S.A de C.V, 2012.

ANÓNIMO. **Teoría de las Actividades Rutinarias**. (s.l.i.): (s.e.) (s.f.)

CABANELLAS, Guillermo. **Diccionario de Derecho Usual**. Tomo I, II, III y IV. 10ma. Edición. Buenos Aires, Argentina: Ed Heliasta S.R.L, 1976.

CASTILLO, Dina. **Documento de Exposición de los Temas: La Realidad, su Conocimiento, Enfoques Epistemológicos y Paradigmas en Teoría y el Método de la Ciencia**. Séptima edición. Guatemala: (s.e.), 2015.

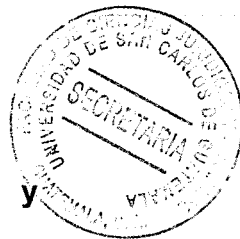
DE MATA VELA, José y DE LEÓN, Héctor. **Derecho Penal Guatemalteco**. Tomo I. Vigésima quinta edición. Guatemala: Ed. Magna Terra editores S.A, 2015.

HIKAL, Wael. **Introducción al Estudio de la Criminología**. Tercera edición. México: Editorial Porrúa, S.A de C.V, 2013.

LÓPEZ GUARDIOLA, Samantha. **Derecho Penal I**. Primera edición. México: Ed. Red Tercer Milenio S.C, 2012.

MARROQUÍN, Jonatán. **Informática Jurídica**. Primer folleto. Guatemala: (s.e.), 2017.

MIRÓ LLINARES, Fernando. **El Cibercrimen. Fenomenología y Criminología de la Delincuencia en el Ciberespacio**. Madrid, España: Ed. Marcial Pons, 2012.



MIRÓ, Fernando. **La Oportunidad Criminal en el Ciberespacio. Aplicación y Desarrollo de la Teoría de las Actividades Cotidianas para la Prevención del Cibercrimen.** España: (s.e.), 2011.

Ministerio Público. **Política Criminal Democrática del Estado de Guatemala 2015-2035.** Guatemala: (s.e.), 2015.

Ministerio de Gobernación. **Estrategia Nacional de Seguridad Cibernética.** Guatemala: (s.e.), 2018.

MOLINA SALGADO, Jesús Antonio. **Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial.** México: Ed. Porrúa, 2003.

NORIEGA, Hans. **Delitos Informáticos.** Primera edición. Guatemala: (s.e.), 2011.

OLIVERA DÍAZ, Guillermo. **Criminología Peruana.** Tomo I. Segunda edición. Lima, Perú: Editorial S.P.E, 1973.

OSSORIO, Manuel. **Diccionario de Ciencias Jurídicas, Políticas y Sociales.** 38va edición. Buenos Aires, Argentina: Ed. Heliasta S.R.L, 2013.

RODRIGUEZ, Luis. **Criminología.** Segunda edición. México: Editorial Porrúa S.A, 1981.

SERRANO, Alfonso. **Criminología e Informática.** Madrid, España: (s.e.), (s.f.).

TELLÉZ VALDÉZ, Julio. **Derecho Informático.** Segunda edición. México: Ed. Impresora OFGLOMA S.A de C.V, 1998.

ZAFFARONI, Eugenio, ALAGIA, Alejandro y SLOKAR, Alejandro. **Derecho Penal.** Parte general. Segunda edición. Buenos Aires, Argentina: Ed. Ediar S.A, 2002.



Legislación:

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

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

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

Ley Orgánica del Ministerio Público. Congreso de la República de Guatemala, Decreto 40-94, 1994.