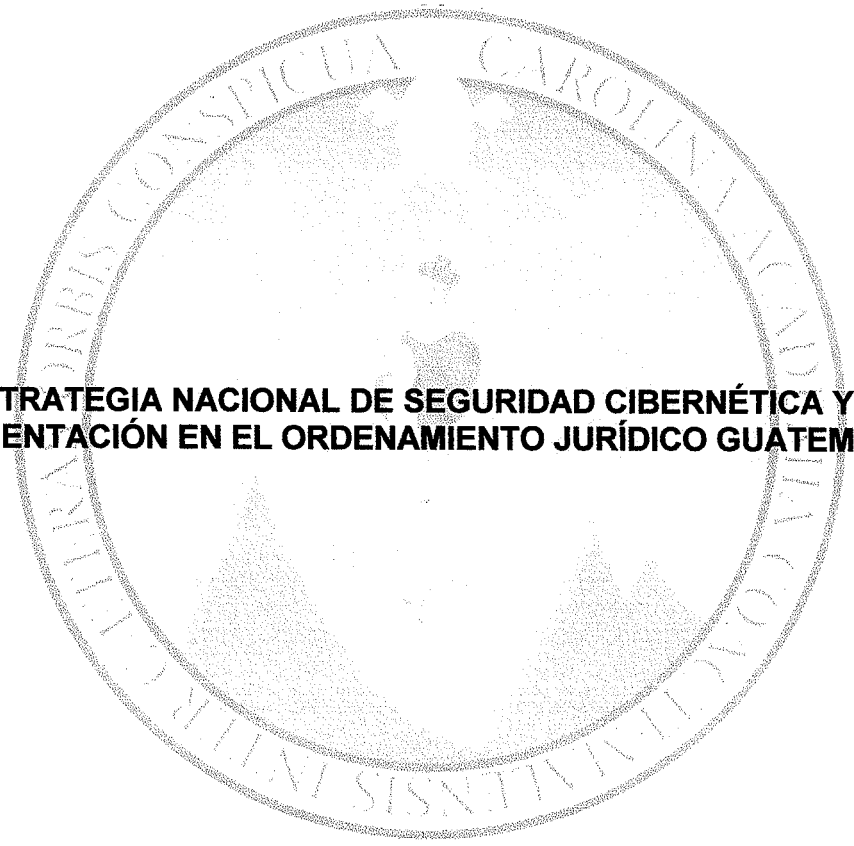
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
CENTRO UNIVERSITARIO DE SANTA ROSA



ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y SU IMPLEMENTACIÓN EN EL ORDENAMIENTO JURÍDICO GUATEMALTECO

ESTEFANI MARÍA WAY GÓMEZ

GUATEMALA, MARZO DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
CENTRO UNIVERSITARIO DE SANTA ROSA

ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y SU IMPLEMENTACIÓN EN EL ORDENAMIENTO JURÍDICO GUATEMALTECO

TESIS

Presentada a la Honorable Junta Directiva

del

Centro Universitario de Santa Rosa

de la

Universidad de San Carlos de Guatemala

Por

ESTEFANI MARÍA WAY GÓMEZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

GUATEMALA, MARZO DE 2022

HONORABLE JUNTA DIRECTIVA

DEL

CENTRO UNIVERSITARIO DE SANTA ROSA

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DIRECTOR:	Lic.	José Luis Aguirre Pumay
SECRETARIO:	Lic.	Elmer Amilcar Carrillo Chavez
REPRESENTANTE DE PROFESORES TITULARES:	Lic.	Alex Edgardo Lone Ayala
REPRESENTANTE DE PROFESORES TITULARES:	Lic.	Walter Armando Carvajal Días
REPRESENTANTE DE EGRESADOS:	Lic.	José Domingo Gónzalez Morales
REPRESENTANTE ESTUDIANTIL:	Br.	Héctor Edmundo Pablo Solís
REPRESENTANTE ESTUDIANTIL:	Br.	Samuel Antonio Hernández del Cid

AUTORIDADES DEL CENTRO UNIVERSITARIO

FASE PRIVADA

Presidente	Lic.	Efraín Barrientos Jiménez
Secretaria	Licda.	Shirley Corina Virginia Gónzalez Melgar
Vocal I	Lic.	Jacobo Benjamín Reyes Ruíz

FASE PUBLICA

Presidente	Lic.	Obdulio Rosales Davila
Secretaria	Lic.	José Luis Aguirre Pumay
Vocal I	Lic.	Oscar Ricardo Quinteros Silva

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y del contenido de la tesis" (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y sociales en el Centro Universitario de Santa Rosa –CUNSARO- de la Universidad de San Carlos de Guatemala.

PROVIDENCIA No. UAT-17-2019

- - - DAD DE ASESORÍA DE TESIS. CARRERA CIENCIAS JURÍDICAS Y SOCIALES. SECCIÓN CHIQUIMULILLA DEL CENTRO UNIVERSITARIO DE SANTA ROSA. Chiquimulilla, veinticinco de septiembre de dos mil diecinueve.----------

Estefani Maria Way Gómez propone al Licenciado Saulo Pérez García para revisar el informe denominado: **Estrategia nacional de seguridad cibernética y su implementación en el ordenamiento jurídico guatemalteco**; según expediente número UAT-076-2018.

Atentamente pase a Licenciado Saulo Pérez García, para que proceda a revisar el informe final de la estudiante Estefani Maria Way Gómez, denominado: **Estrategia nacional de seguridad cibernética y su implementación en el ordenamiento jurídico guatemalteco.** Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que mejoren la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, que dice: *"tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes su opinión respecto del contenido científico y técnico de la tesis, la metodología, técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueran necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que consideren pertinentes"*.

Lic. Carlos Eduardo Cruz Véliz
COORDINADOR UNIDAD DE ASESORÍA DE TESIS

CECV/csrp
cc. archivo

LIC. SAULO PEREZ GARCÍA
ABOGADO Y NOTARIO
3ª. Av. 1-34, zona 1, Chiquimulilla, Santa Rosa
Tel. 55975518 --- 57238404 – 7885-1295
EMAIL: licsauloperez@hotmail.com -- licsauloperez@yahoo.com

UNIVERSIDAD DE SAN CARLOS • CENTRO UNIVERSITARIO DE SANTA ROSA • COORDINACIÓN ACADÉMICA

Chiquimulilla, 29 de noviembre del año 2019

Dr. CARLOS EDUARDO CRUZ VELIZ
COORDINADOR DE LA UNIDAD DE ASESORÍA DE TESIS
CARRERA CIENCIAS JURÍDICAS Y SOCIALES, SECCIÓN CHIQUIMULILLA
CENTRO UNIVERSITARIO DE SANTA ROSA, USAC.

Respetable Doctor:

Me dirijo a usted con el objeto de informarle que de conformidad con el nombramiento de fecha veinticinco de septiembre del año dos mil diecinueve, fui designado por su despacho para proceder a la revisión de la tesis de la estudiante ESTEFANI MARÍA WAY GÓMEZ, intitula: **"ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y SU IMPLEMENTACIÓN EN EL ORDENAMIENTO JURIDICO GUATEMALTECO"**, para lo cual manifiesto lo siguiente:

1. He revisado el trabajo de tesis relacionado y considero que el mismo reúne los requisitos exigidos en el artículo 32 del normativo para la elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales del Centro Universitario de Santa Rosa.

2. **Metodología y técnica de investigación utilizada.** La metodología de investigación reúne las condiciones para la consecución d objetivos y ordenamientos de las actividades para una reproducción de análisis descriptivos y explicativo para este tipo de estudio. En relación a las técnicas de investigación se identifica la utilización de del análisis documental para el desarrollo de síntesis y deducciones para la posterior generación de conclusiones.

3. **Redacción:** Cumple con las Normas mínimas establecidas en el Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales.

4. **Bibliografía investigativa:** la revisión y análisis documental son de fuentes bibliografías adecuadas, diversas y actualizada para el objeto de estudio.

Por las consideraciones anotadas anteriormente emito **DICTAMEN FAVORABLE Y APRUEBO,** el trabajo de investigación de tesis de la Bachiller **ESTEFANI MARÍA WAY GÓMEZ,** en tal sentido es procedente su revisión respectiva, debido a que se cumple con las exigencias que determina el artículo 32 del NORMATIVO.

LIC. SAULO PEREZ GARCIA
ABOGADO Y NOTARIO

LIC. SAULO PEREZ GARCIA
ABOGADO Y NOTARIO

UNIDAD DE ASESORÍA DE TESIS
CUNSARO –SECCIÓN CHIQUIMULILLA

PROVIDENCIA No. UAT-010-2019

UNIDAD DE ASESORÍA DE TESIS, CARRERA CIENCIAS JURÍDICAS Y SOCIALES, SECCIÓN CHIQUIMULILLA DEL CENTRO UNIVERSITARIO DE SANTA ROSA. Dieciséis de julio del año dos mil diecinueve. ----------

Atentamente, pase al LICENCIADO, **JOSÉ RODERICO MÉNDEZ SOLÓRZANO**, para que proceda a asesorar el trabajo de la estudiante **ESTEFANI MARIA WAY GOMEZ**, intitulado: **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNETICA Y SU IMPLEMENTACIÓN EN EL ORDENAMIENTO JURIDICO GUATEMALTECO**.

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que mejoren la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo32 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, que dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes su opinión respecto del contenido científico y técnico de la tesis, la metodología, técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueran necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que consideren pertinentes".

Lic. Manuel Orlando Bolaños Gudiel
COORDINADOR UNIDAD DE ASESORÍA DE TESIS

MOBG/VB

LIC JOSÉ RODERICO MÉNDEZ SOLÓRZANO
ABOGADO Y NOTARIO
TELEFONO: 5318-6947

Chiquimulilla, Santa Rosa, 21 de agosto del 2019

Dr. CARLOS EDUARDO CRUZ VELIZ
COORDINADOR DE LA UNIDAD DE ASESORIA DE TESIS
CARRERA CIENCIAS JURIDICAS Y SOCIALES, SECCION CHIQUIMULILLA
CENTRO UNIVERSITARIO DE SANTA ROSA, USAC.

DR. CRUZ VELIZ.

De manera respetuosa me dirijo a usted, en cumplimiento de la providencia emanada de la Unidad de Asesoría de Tesis, del Centro, Universitario de Santa Rosa, en la que se me nombro Asesor del trabajo de tesis titulado "ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y SU IMPLEMENTACIÓN EN EL ORDENAMIENTO JURIDICO GUATEMALTECO." Elaborado por la Bachiller, ESTEFANI MARÍA WAY GÓMEZ, identificada con carne número: 201442738.

Al finalizar la elaboración de trabajo de tesis relacionado informo que hice las recomendaciones y sugerencias respecto al tema desarrollado y el mismo reúne los requisitos exigidos en el normativo para la elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales del Centro Universitario de Santa Rosa; dado que los métodos y técnicas de investigación aplicadas son congruentes y adecuados para este tipo de investigación.

Por lo que considero que el trabajo de tesis de la Bachiller ESTEFANI MARÍA WAY GÓMEZ, reúne los requisitos requeridos en el Normativo para la elaboración de trabajo de tesis, y en virtud de ello emito DICTAMEN FAVORABLE aprobado el trabajo de tesis asesorado.

NOTIFIQUESE.

F_____
LIC. JOSÉ RODERICO MÉNDEZ SOLÓRZANO
ABOGADO Y NOTARIO
COLEGIADO No. 7,177

Lic. José Roderico Méndez Solórzano
ABOGADO Y NOTARIO

Oficio No. UAT 03-2020
Ref. WERG/csrp

Chiquimulilla, 09 de junio de 2020

Ingeniero
Cristiam Armando Aguirre Chinchilla
Director del Centro Universitario de Santa Rosa y
Coordinador de exámenes generales de graduación
Universidad de San Carlos de Guatemala
Cuilapa, Santa Rosa

Distinguido Señor Director:

Muy atenta y respetuosamente me dirijo a usted para referirle el informe final de la alumna Estefani María Way Gómez, quien se identifica con carné no. 201442738, para que se ordene la impresión según lo establece el artículo 31 del normativo para la elaboración de tesis.

La estudiante Estefani María Way Gómez ha cumplido con todos los requisitos de forma, fondo y estilo requeridos por el normativo y el instructivo general para la elaboración de tesis.

El documento cuenta con 141 páginas, incluyendo las páginas previas. Al agradecer su atención a la presente, quedo a sus respetables órdenes.

Lic. Walter Edmundo Ramírez González
COORDINADOR UNIDAD DE ASESORÌA DE TESIS

/cc. archivo

USAC
CUNSARO
Universidad de San Carlos de Guatemala

- DIRECCION CENTRO UNIVERSITARIO –

DIRECCIÓN DEL CENTRO UNIVERSITARIO DE SANTA ROSA –CUNSARO- DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,

Cuilapa, veinticuatro de Agosto de dos mil veinte

Orden de Impresión 01/2020

Con vista en los dictámenes favorables que anteceden y de conformidad con los artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales en el Centro Universitario de Santa Rosa –CUNSARO- de la Universidad de San Carlos de Guatemala, se autoriza la impresión del trabajo de tesis de la estudiante **ESTEFANI MARÍA WAY GÓMEZ**, Carné No. **201442738**, titulado **"ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y SU IMPLEMENTACION EN EL ORDENAMIENTO JURIDICO GUATEMALTECO"**.

"ID Y ENSEÑAD A TODOS"

MA.Ing. Civil. Cristiam Armando Aguirre Chinchilla

Director

DECICATORIA

A DIOS: Por darme el privilegio de la vida, por estar y cumplir cada sueño y cada meta que me he propuesto, por darme sabiduría e inteligencia en todo momento, por permitirme cerrar esta etapa de mi vida con éxito.

A MIS PADRES: Lic. Jorge Armando Way Segura y Licda. María del Carmen Gómez Hernández, por educarme y enseñarme que todo en la vida se obtiene confiando en Dios y trabajando duro, por amarme incondicionalmente, por apoyarme y ayudarme hacer realidad cada proyecto que he alcanzado y los que aún me faltan por cumplir.

A MIS HERMANOS: María del Carmen Way Gómez, Jorge Armando Way Gómez, Luz María Way Gómez, por brindarme su apoyo incondicionalmente en todo momento y enseñarme el significado de amor.

A MIS SOBRINAS: Luisa María Hernández Way y María del Carmen Hernández Way, por llenar mis días de amor y felicidad, por enseñarme cosas nuevas cada día.

A MI FAMILIA: Por formar parte de mi vida, por estar en cada parte de mis procesos y sus apoyos incondicionales.

A MIS AMIGOS: Por esta en cada etapa de mi vida y por apoyarme en cada proyecto.

A PERSONAS ESPECIALES: Doctora Lidia Guadalupe Jiménez Crespo, por su apoyo incondicional.

A LOS LICENCIADOS: Lic. Walter Ramirez, Lic. Alex Lone, Lic. Saulo Pérez, Lic. Manuel Bolaños, Lic. Luis Pumay, Lic. Federico Méndez, Lic. Carlos Cruz, Lic. Víctor Pérez, Lic. Delbhert García, por su apoyo y consejos que me brindaron a lo largo delacarrera.

EN ESPECIAL A: La Universidad de San Carlos de Guatemala, al Centro Universitario de Santa Rosa, que gracias a ellas no solo me han permitido mi desarrollo profesional, sino también personal y gracias al Pueblo de Guatemala por contribuir con el desarrollo de profesionales de éxito.

ÍNDICE

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

RESUMEN

En la actualidad el Estado de Guatemala solo cuenta con una estrategia nacional de seguridad cibernética en la que consigna la necesidad de crear un marco normativo en materia de ciberdelito y ante la ausencia de este marco normativo, esta estrategia o política contra el ciberdelito es inoperante, toda vez, que no se puede poner en marcha. La metodología utilizada en la investigación consistió básicamente en las formas de razonamiento inductivo-deductivo y el método jurídico los que ayudaron a obtener resultados valiosos en el sentido de que en Guatemala en materia de ciberdelito no se cuenta con las herramientas tecnológicas necesarias para combatir este nuevo tipo de cirminalidad y que adolece de un marco normativo especializado que fundamente la persecución y el juzgamiento. Entre las principales conclusiones están que el ciberdelito es de carácter transnacional que lo convierte en una preocupación a nivel global y que ningún Estado puede ni debe estar aislado, sino al contrario es precisa la cooperación internacional.


UNIVERSIDAD DE SAN CARLOS
CENTRO UNIVERSITARIO DE SANTA ROSA
COORDINACIÓN ACADÉMICA

INTRODUCCIÓN

Guatemala en la actualidad no cuenta con un marco normativo penal sobre el ciberdelito lo que complica la persecución, juzgamiento y sanción de este delito. Hoy el ciberdelito está evolucionando a la par que se desarrolla la ciencia informática y el acceso masivo a internet que facilita el acceso a las diferentes plataformas y redes sociales existentes.

El problema planteado en la presente investigación consiste en la dificultad de implementar la Estrategia de Seguridad Cibertética porque no cuenta con el marco jurídico normativo que legitime su contenido. La justificación se sustenta en la imposibilidad de alcanzar la serie de objetivos y acciones que se proponen en el documento relacionado, porque para fortalecer la cooperación, colaboración y coordinación en materia de seguridad cibernética es imprescindible la existencia de una marco jurídico normativo que Guatemala por el momento no cuenta. La hipótesis del presente trabajo de tesis se enfocó, a que ninguna política nacional de seguridad cibernética puede ser efectivamente ejecutada o puesta en marcha si no existe el marco jurídico normativo correspondiente, tal y como ocurre actualmente en Guatemala.

Los objetivos de la investigación fueron: objetivo general, establecer, que una estrategia o política sobre seguridad cibernética como la que el Estado de Guatemala plantea no tiene viabilidad de ser puesta en marcha, porque no se ha implementado en el ordenamiento jurídico penal guatemalteco de la normativa específica que

tipifique el ciberdelito; como objetivos específicos, determinar, que la ausencia de normativa sobre el ciberdelito coloca al Estado de Guatemala en una posición de vulnerabilidad respecto a la persecución, enjuiciamiento y sanción del ciberdelito; establecer que el Estado de Guatemala por virtud del principio de legalidad no está legitimado para sancionar el ciberdelito; determinar que los llamados delitos informáticos tipificados en el código penal guatemalteco no pertenecen a la naturaleza jurídica de los llamados ciberdelitos; identificar que la regulación de los delitos cibernéticos constituye el sustrato legal para la creación de una política de seguridad cibernética.

La investigación se dividió en cinco capítulos distribuidos así: el capítulo uno desarrolla lo relacionado con el derecho penal, definición, fuentes, características, naturaleza, norma penal y ley penal y, derecho penal guatemalteco; el capítulo dos trata sobre la teoría del delito, definición, naturaleza jurídica del delito, teorías sobre el delito, los elementos y la punibilidad; el capítulo tres aborda el ciberdelito, definición, naturaleza, el bien jurídico tutelado, la internacionalización del ciberdelito, el ciberdelito y la ciberdelincuencia, y los elementos del ciberdelito; el capítulo cuatro desarrolla la seguridad cibernética en Guatemala, antecedentes, política pública de seguridad cibernética, los desafíos de la lucha contra el ciberdelito y la estrategia nacional de seguridad cibernética; el capítulo cinco contiene la propuesta, el problema de ejecutar la estrategia nacional de seguridad cibernética sin el marco legal que la legitime, la incorporación normativa del ciberdelito a la legislación penal guatemalteca, se analiza la iniciativa 5254, Ley Contra la Ciberdelincuencia y los

comentarios finales. Además se incluyen las conclusiones, recomendaciones y la bibliografía utilizada.

La teoría que sirvió de base doctrinaria para comprender el ciberdelito es la teoría finalista del delito, que en este caso se aplicó dogmáticamente al fenómeno de la internacionalidad de la ciberdelincuencia. Los métodos utilizados fueron: el método inductivo, el método deductivo, el método analítico y el método sintético. En las técnicas, se utilizó especialmente la bibliográfica y documental.

Finalmente, para que Guatemala efectivamente inicie formalmente la lucha contra el ciberdelito, es necesario que se adhiera y ratifique el Convenio Sobre la Ciberdelincuencia, adopte una legislación especial sobre el ciberdelito.

CAPÍTULO I

1. El derecho penal

1.1. Generalidades

El derecho en general es un todo unitario, el cual para su estudio se sustenta en una serie de conceptos jurídicos fundamentales, principios, teorías y normas jurídicas comunes a todas las áreas del derecho. En este sentido, el derecho se divide en diferentes áreas específicas que permiten obtener el conocimiento y la comprensión de este conocimiento particular de cada área del derecho.

Es así que el derecho se divide en: derecho penal, civil, administrativo, laboral, constitucional, etcétera. Cada una de estas áreas del derecho a su vez se dividen en una parte sustantiva y otra llamada adjetiva; esta última constituida por el conjunto de procedimientos que sirven para hacer valer los derechos y garantías sustantivas denominada derecho procesal.

Antiguamente el derecho no estaba dividido como en la actualidad en diferentes áreas, éstas pertenecían a una sola concepción del derecho. Pero poco a poco fueron adquiriendo cierta autonomía hasta lograr la calidad de ciencias independientes; este es el caso del derecho penal que en la actualidad nadie duda de su carácter como ciencia penal autónoma.

"El derecho penal, como parte del derecho en general, es utilizado para controlar, orientar y planear la vida en común. Mediante él, se determinan y definen ciertos comportamientos, los cuales no deben ser realizados".[1]

En este orden, el derecho penal como parte de las ciencias jurídico penales y su carácter sancionador se le concibe también como una ciencia poco pacífica, no obstante, paradójicamente uno de sus fines principales es precisamente incidir en la convivencia pacífica entre los ciudadanos y el Estado.

Efectivamente, toda referencia al derecho penal se asocia inmediatamente con la violencia o por lo menos con actos de violencia llamados delitos. Por tanto, el derecho penal no obstante su naturaleza coercitiva, lo que trata es solucionar, no pacíficamente, los conflictos que surgen con motivo de la comisión de un delito mediante la coerción penal.

En el derecho penal antiguo especialmente en Roma, aunque éste era parte del derecho civil o ius civile se definía la coerción como la "facultad para imponer penas de flagelación, confiscación o muerte en los casos de desobediencia a lo ordenado por el magistrado".[2] En la actualidad, esta noción coercitiva del derecho penal ha observado sustanciales cambios sobre todo, en el desarrollo de las ideas penales concomitantemente con el desarrollo de la teoría de los derechos humanos.

---

[1] Hurtado Pozo, José. **Manual de derecho penal**. Pág. 10
[2] Di Pietro, Alfredo y Ángel Enrique Lapieza Elli. **Manual de derecho romano**. Pág. 21.

Actualmente, esta noción coercitiva del derecho penal se concibe como el sometimiento forzoso del sujeto activo de un delito a una pena, que generalmente es de prisión, excepcionalmente la pena de muerte (en Guatemala, por sentencia de la Corte de Constitucionalidad, la aplicación de la pena de muerte está expulsada del ordenamiento jurídico, no obstante, estar vigente).

"El derecho penal, tanto en los casos que sanciona, como en la forma de sancionarlos, es pues, violento".[3] Es debido a esta naturaleza coercitiva que dice que el derecho penal es la forma en que el Estado ejerce control social. La comisión de un delito siempre necesariamente conlleva diversas formas de violencia; toda vez, que la violencia es un elemento general que acompaña la comisión del delito.

El robo, el homicidio, el asesinato, la violación todos los cuales de una u otra forma, para ser cometidos se necesita la utilización de violencia. Hablar del derecho penal no solamente se circunscribe al delito (aunque este es uno de los elementos más importantes de su campo de estudio), sino también a la consecuencia jurídica del mismo, es decir, la pena.

En cuanto a la determinación de las penas y a su aplicación, solamente el Estado está facultado para crearlas e imponerlas; no obstante, la imposición de una pena no es del libre arbitrio de los jueces o magistrados. Para que el Estado esté facultado de imponer una pena es necesario que éstas estén plenamente establecidas como

[3] Muñoz Conde, Francisco. **Derecho penal y control social**. Pág. 18.

consecuencia jurídica de un delito y éste debidamente tipificado en la parte especial del Código Penal.

La tipificación de un delito y su correspondiente pena tienen que estar previamente establecidos en una ley anterior a la perpetración del delito; la anterioridad del delito y la pena se amparan por por virtud del principio de legalidad. A la facultad del Estado de imponer una pena previamente establecida, se le denomina ius puniendi. La facultad punitiva del Estado no es absoluta, la misma por virtud de ciertas garantías sustantivas y procesales tiene límites que están establecidos en la propia ley: Código Penal y Procesal Penal, la Constitución Política de la República y diferentes Convenios y Tratados internacionales en materia penal.

"No se puede olvidar que las leyes, en un Estado de derecho, ejercen la función de imponer límites a la intervención punitiva estatal, protegiendo a los ciudadanos contra la arbitrariedad y el error penal".[4]

La Constitución Política de la República ocupa la cúspide del ordenamiento jurídico en la jerarquía normativa, en general y en materia penal, en particular. Establece algunos de estos límites a la facultad punitiva del Estado; en la doctrina jurídico-penal estas limitantes se les denomina: garantías o principios jurídico-penales y procesal-penales.

---

[4] Hauck, Joao R. **Tecnología, vigilancia y sistema penal: La superación de paradigmas y las nuevas perspectivas bajo el punto de vista tecnológico. En lecciones y ensayos**. Pág. 36.

De tal forma, uno de los principales límites (garantías) al ius puniendi del Estado es, como ya se afirmó, el principio de legalidad, el cual está consagrado en el Artículo 17 de la Constitución Política de la República, que establece: "no son punibles las acciones u omisiones que no estén calificadas como delito o falta y penadas por ley anterior a su perpetración".

En la doctrina y en la legislación se considera este principio como la columna vertebral de todo el sistema punitivo penal en un Estado democrático de derecho. Es por virtud de este principio que la facultad sancionadora (punitiva) del Estado está limitada a no imponer una pena, que no esté previamente regulada como consecuencia de un determinado delito.

En otras ocasiones, aunque la pena esté perfectamente limitada, por circunstancias procesales y sustantivas, la pena no opera en el caso concreto. "La consecuencia del delito es fundamentalmente la coerción penal, cuya manifestación se ha caracterizado como pena. No obstante, puede acontecer que al delito no le siga como consecuencia jurídica la coerción penal, porque el derecho determine que ella no debe operar en ese supuesto, pese a la existencia del delito. Se trata de un grupo de casos de excepción, en que la coerción penal carece de operatividad (sic)".[5]

Otro aspecto que resulta importante sobre el carácter sancionador del derecho penal es, en cuanto a la función que ejerce el Estado como una forma legitimada de

[5] Zaffaroni, Eugenio Raúl. **Tratado de derecho penal: Parte General**. Tomo V. Pág. 13.

defensa social. Esta forma de defensa social que utiliza el Estado para garantizar la convivencia pacífica, se da por medio de la descripción de las conductas en el tipo penal mediante la protección de bienes jurídicos que el derecho penal considera importantes de tutelar. A esta caracterización también se le conoce como prevención general y prevención especial.

"La legitimidad de la represión de la prevención general y especial, no en el sentido utilitario, sino como necesidad racional, recalcando que la idea fundamental del derecho penal está en la tutela jurídica".[6]

La característica del derecho penal, de proteger ciertos bienes jurídicos penalmente relevantes, tiene como fin lograr en alguna medida la convivencia pacífica, que a partir de la prevención general y especial también tiene el propósito de que los habitantes se motiven por la norma y no la transgredan. Pero si la norma es violada, se pone en movimiento el aparato sancionador del Estado a través del ius puniendi.

"La presencia evidente e impositiva de esta protección brindada por la ley penal a los bienes jurídicos, ha determinado que la mayor parte de los juristas reconozcan en ella la tarea primaria y fundamental del derecho penal".[7] En este sentido, uno de lo los fines del derecho penal es la protección de los bienes jurídicos y para esto hace uso de la facultad punitiva.

---

[6] Zaffaroni, Eugenio Raúl. **Trabado de derecho penal, parte general**. Tomo II. Pág. 138.
[7] Hurtado Pozo, José. **Ob. Cit**. Pág. 12.

El derecho penal constituye entre otros mecanismos que utiliza el Estado, una forma de control social y el ius puniendi la respuesta a la perturbación de orden social establecido, que se traducen en el facultad del Estado a castigar.[8] Lo que también confirma que el Estado es el único que tiene la facultad de definir los delitos y establecer las respectivas penas e imponerlas. La facultad del Estado de tipificar conductas delictivas y sus respectivas penas como ya se afirmó, tiene límites. El principio de legalidad es uno de estos límites, que en materia específica de las penas también constituyen límites a la facultad punitiva del Estado, los principios de intervención mínima, de subsidiariedad y proporcionalidad.

El principio de intervención mínima "se plantea la necesidad que el derecho penal sólo debe ser utilizado como recurso de última ratio, cuando otros medios resultan ineficaces; impone la necesidad de agotar previamente recursos no penales, cuyas consecuencias sean menos drásticas, pero que puedan resultar más eficaces que las penas para la protección de bienes jurídicos".[9]

1.2. Definiciones de derecho penal

El delito, las penas, el delincuente, las teorías, doctrinas y principios necesariamente forman parte de toda definición de derecho penal. A continuación, se transcribirán

---

[8] Medina Cuenca, Arne. **Los principios limitativos del ius puniendi y las alternativas a las penas privativas de libertad**. Pág. 88.

[9] Moreno Hernández, Moisés. **Principios rectores en el derecho penal mexicano**. http://biblio.juridicas.unam.mx/libros/1/117/26.pdf. Extraído el 17 de marzo de 2019.

algunas definiciones de las cuales se hará un breve análisis, con el fin de determinar sus elementos constitutivos.

Derecho penal es "el conjunto de leyes que traducen normas tuitivas de bienes jurídicos y que precisan su alcance, cuya violación se llama delito e importa una coerción jurídica particularmente grave, que procura evitar nuevas violaciones por parte del autor".[10] También, "es el conjunto de las reglas jurídicas establecidas por el Estado, que asocian el crimen, como hecho, a la pena, como legítima consecuencia".[11] "Es la rama del derecho público interno relativa a los delitos, a las penas y a las medidas de seguridad, que tiene por objeto inmediato la creación y conservación del orden social".[12]

Además, es el "conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado, estableciendo el concepto de delito como presupuesto de la acción estatal, así como la responsabilidad del sujeto activo, y asociado a la infracción de la norma una pena finalista o una medida aseguradora".[13]

Asimismo es, "parte del ordenamiento jurídico, formada por las normas jurídicas reguladoras del poder punitivo del Estado (ius puniendi) en las que, mayormente, a

---

[10] Zaffaroni, Eugenio Raúl. **Tratado de derecho penal, parte general**. Tomo I. Pág. 24.
[11] Castellanos, Fernando. **Lineamientos elementales de derecho penal**. http://cdigital.dgb.uanl.mx/te/1020124909/1020124909_02.pdf. Extraído el 17 de marzo de 2019.
[12] Moreno Hernández, Moisés. **Ob. Cit**.
[13] Mariaca, Margot. **Introducción al derecho penal**. Bolivia, 2010. Pág. 3.

fin de tutelar, bienes jurídicos, se definen delitos para los cuales se establecen penas y medidas de seguridad".[14]

Como se puede apreciar en las definiciones transcritas, todas comparten ciertos elementos comunes como el delito y las penas. El Estado es el único que tiene la facultad de tipificar conductas; el Estado no crea el delito solo tipifica conductas, regulándolas porque considera que lesionan bienes jurídicos relevantes que pretende proteger. A la regulación de estas conductas que lesionan bienes que el Estado considera relevante para su protección, se les llama delitos, que necesariamente tienen como consecuencia la respectiva pena.

1.3. Fuentes del derecho penal

Según el Diccionario de la Academia Española en su séptima acepción y que es la que aquí interesa, fuente significa: "principio, fundamento u origen de algo".[15] En este sentido y referido al derecho penal lo que se trata es determinar cuál es el origen, de dónde brota el derecho penal y más específicamente el delito.

La doctrina está de acuerdo que la principal fuente del derecho penal es la ley, esto significa que para la tipificación de una conducta relevante para el derecho penal,

[14] Orts Berenguer, Enrique y José L. González Cussac. **Manual de derecho penal, parte general**. Pág. 11.
[15] Real Academina Española de la Lengua. https://dle.rae.es/?id=IYZhVtl. Extraído el 28 de marzo de 2019.

solo se puede hacer mediante la ley (observando el principio de legalidad) en la cual se tipifiquen las figuras delictivas y se establezcan las respectivas penas.

Afirmar que la fuente principal del derecho penal es la ley, significa que esta fuente está configurada por toda la legislación penal, decir, "el conjunto de preceptos penales que conforman en su conjunto el ordenamiento jurídico penal" (sic).[16] En Guatemala la ley es la fuente del ordenamiento jurídico y por tanto del derecho penal. La Ley del Organismo Judicial en el Artículo 2, establece que "la ley es la fuente del ordenamiento jurídico".

El artículo citado también establece que la jurisprudencia complementará esta fuente formal del derecho penal. Es importante hacer un breve análisis sobre el contenido normativo de este artículo, toda vez, que como se afirma al principio de este apartado, en derecho penal el principio de legalidad forma parte integrante de las garantías sustantivas de esta rama normativa, por lo que afirmar que la jurisprudencia complementa una fuente formal del derecho en principio es válida respecto al resto del ordenamiento jurídico, pero en materia penal no se le puede adjudicar dicha validez, debido al principio de legalidad.

Es indudable que en el proceso legislativo de tipificar delitos y asignarles sus respectivas penas, el legislador también se vale de otras fuentes que al final, se plasmarán en la definición de un delito o de toda una ley penal. En efecto, cuando el

[16] Zaffaroni, Eugenio Raúl. **Ob. Cit.** Tomo I. Pág. 124.

Estado determina que un determinado bien es relevante para el derecho penal, lo hace partiendo de la base de su protección, Bacigalupo afirma "que el Estado solamente debe intervenir mientras haya una acción objetiva que represente un peligro para determinado bien jurídico, de tal manera, que la intervención del derecho penal comienza con el peligro real para un bien jurídico que se considera relevanta para su debida protección".[17]

Aunque el argumento anterior no sería del todo válido para el legislador, si este bien, no hubiera sido previamente lesionado; es decir, la conducta que lesiona un bien que no está protegido por el derecho penal no puede ser objeto de reproche, toda vez, que hasta ese momento no está tipificada como delito. En consecuencia, en materia de fuentes del derecho penal la principal fuente es la ley, aunque en la doctrina también se mencionan otras fuentes: materiales, formales (la ley) e históricas.

1.3.1. Fuentes formales

La ley penal se caracteriza por ser una fuente formal del derecho penal que ocupa en la jerarquía normativa el segundo escalón por debajo de las normas constitucionales, éstas últimas ocupan la cúspide del ordenamiento jurídico guatemalteco representada por la Constitución Política de la República.

[17] Bacigalupo, Enrique. **Manual de derecho penal: Parte General**. Pág. 4.

La normativa constitucional es, si se le puede caracterizar de esta forma, la primera limitante de la facultad sancionadora del Estado y al mismo tiempo, una estructura legitimadora de esta facultad. Esto quiere decir que una tercera categoría (acuerdos, reglamentos, etcétera), no puede ser fuente del derecho penal por virtud de la jerarquía normativa.

Ahora bien, algunos autores consideran como fuente formal del derecho penal a la jurisprudencia (en este sentido, la autora no comparte este criterio debido a la limitante del principio de legalidad). (Para ampliar consultar apartado 1.2. del capítulo I). En la actualidad "se consideran como fuentes formales del derecho penal, determinados tratados y convenios en materia penal. A estas fuentes la doctrina las denomina como fuentes formales mediatas del derecho penal".[18]

"La única fuente inmediata y directa del derecho penal es la ley propiamente, esto es aquella que se ha dictado conforme a las exigencias materiales y formales de la Constitución. De este modo, el principio de legalidad excluye no sólo la posibilidad de que fuentes del derecho generalmente admitidas en otros dominios del orden jurídico, como la costumbre, la ley del contrato o la jurisprudencia puedan crear delitos o penas; también quedan excluidos como fuente directa del derecho penal aquellas regulaciones de inferior jerarquía a la de la ley".[19]

---

[18] Politoff L., Sergio y Jean Pierre Matus A., María Cecilia Ramírez. **Lecciones de derecho penal chileno; Parte general**. Pág. 94.
[19] **Ibíd**. Pág. 101.

1.3.2. Fuentes materiales (mediatas)

El bien jurídico protegido por el derecho penal o, dicho de otra forma, el bien jurídico penalmente relevante para el derecho penal es aquel que se lesiona mediante una conducta típica. Pero, qué pasa cuando un determinado bien no está protegido (tutelado), es decir, que no está tipificado como delito en la norma penal; simplemente no hay delito que perseguir ni sancionar.

Zaffaroni afirma "que no puede haber delito en el ordenamiento jurídico penal, sin que dicha conducta afecte (lesione) un bien jurídico."[20] En este sentido, todo bien jurídico tutelado por el derecho penal en un momento sin duda alguna, no era considerado como relevante para su protección, por ejemplo: el ciberdelito (caso de Guatemala).

En la actualidad, este tipo de conducta (ciberdelito) que como consecuencia del avance y desarrollo de la ciencia informática, el acceso masivo a internet y el alcance de la red informática mundial (World Wide Web por sus siglas en inglés), se ha convertido en una preocupación de la comunidad internacional. Toda vez, que lesiona bienes jurídicos que anteriormente al desarrollo de estos aspectos, no tenía relevancia para el derecho penal.

[20] Zaffaroni, Eugenio Raúl. **Ob. Cit**. Tomo I. Pág. 36.

Hoy, este tipo de conducta que ha sido considerada como delito, su fundamento fáctico se puede encontrar en la fuente material como el supuesto de hecho que genera la norma jurídico-penal. Por lo que también se le puede considerar como una fuente no formal, pero mediata del derecho penal.

1.3.3. Fuentes históricas

La importancia de este tipo de fuentes radica en su valor como fuente de consulta para determinada institución o figura delictiva; el valor que ostentan estas fuentes se puede localizar en los círculos académicos, con relación al estudio sobre la transformación de las leyes penales y su desarrollo en el pasado.

En algunos casos el legislador se vale de estas fuentes para la creación de nuevas normas jurídicas. Este tipo de proceso legislativo es casi seguro que no se da en materia penal, pero es efectivo en otras áreas del derecho, por ejemplo: civil, administrativo, laboral, mercantil, etcétera.

1.4. Características del derecho penal

Entre las características principales de esta rama del derecho están: que es normativo, valorativo y finalista. La naturaleza normativa tiene su fuente en la ley penal; partiendo de esta característica normativa del derecho penal surge su

naturaleza valorativa, esta característica se pone de manifiesto en la dogmática porque las soluciones que elabora, son juicios valorativos del contenido de la descripción de los tipos penales; la característica finalista del derecho penal surge de la noción del fin en sí mismo de la conducta típica y antijurídica, cuya tarea es determinar los motivos personales de la conducta delictiva a fin de motivar (prevención) a la no comisión del delito.[21]

El derecho penal protege ciertos bienes jurídicos que considera indispensables para la coexistencia en paz dentro de la sociedad, los cuales no nacen con la creación de las normas penales, sino más exactamente de la vida cotidiana, es decir, de la interacción de las personas en la sociedad. De esta cuenta "las características del derecho penal: normativo, valorativo y finalista se complementan entre sí dando como resultado cierta armonía indisoluble que, lo que pretende es la protección de las garantías individuales, frente a la facultad punitiva del Estado."[22]

1.5. Naturaleza jurídica del derecho penal

El derecho penal puede ser visto desde dos vertientes: "una normativa y la otra como ciencia jurídica; en este último sentido, el derecho penal como ciencia jurídica su

[21] Fontan Balestra, Carlos. **Derecho penal: introducción y parte general**. Pág. 23.
[22] **Ibíd**. Pág. 24.

naturaleza está constituida por el estudio, la interpretación de sus normas (dogmática) y la identificación y elaboración de los principios que lo inspiran."[23]

Por otra parte, el derecho penal desde su vertiente normativa pertenece al derecho público, toda vez, que sus normas son creadas por el Estado, el cual es el único legitimado para aplicarlas. Éstas generan una particular e individual relación entre el Estado y los particulares con motivo de la comisión del delito.

"Ese carácter resulta de la función reguladora de las relaciones entre el Estado y los individuos sometidos a un orden jurídico. No existe relación de soberanía y de sumisión más característica que la del individuo sometido al Estado por la coacción de deber sufrir una pena".[24]

1.6. Norma penal y ley penal

Existe, por lo general, una cierta confusión cuando se utilizan los conceptos jurídicos de norma penal y ley penal, y para una mejor comprensión hay que remitirse al estudio de los conceptos jurídicos fundamentales, porque a primera vista estas dos categorías penales caracterizan un mismo objeto, pero en realidad no es así, son diferentes y entre ambas existen diferencias sustanciales.

---

[23] **Ibíd**. Pág. 14.
[24] **Ibíd**. Pág. 24.

En todo caso, la naturaleza sancionadora del derecho penal obliga a diferenciar entre estos dos conceptos penales. Debe tenerse presente que la ley penal no solo se refiere al Código Penal, sino también a todas aquellas disposiciones normativas penales especiales que regulan algún tipo específico de actividad delictiva (Ley contra la Delincuencia Organizada; Ley Contra el Femicidio y Otras Formas de Violencia Contra la Mujer; Ley Contra la Defraudación y Contrabando Aduanero, por mencionar algunas). Mientras que la norma penal es el dispositivo jurídico penal que contiene la descripción de la conducta y su consecuencia, a esta descripción o definición de la conducta y su consecuencia se le llama tipo penal.

1.6.1. Definición

En el Código Penal no se encuentra una definición del delito; al contrario, en las normas de la ley penal se definen los delitos (robo, homicidio, asesinato, etcétera) mediante el tipo penal. De tal forma, la ley penal es el continente y la norma, en que está definido el delito, es el contenido. "De entre todos los comportamientos antijurídicos, la ley penal selecciona a través de la tipicidad aquellos que considera más graves. A la hora de analizar si una conducta es penalmente antijurídica, en primer lugar, habrá que determinar si se enmarca dentro de alguno de los tipos penales de la parte especial del código o de otras leyes".[25]

[25] González, Cauhapé- Cazaux. **Apuntes de derecho penal guatemalteco: La teoría del delito**. Pág. 73.

"Las leyes son las reglas generales, abstractas y obligatorias emanadas de la autoridad pública autorizada al efecto, que rigen la conducta de las personas".[26] Las características de la ley penal son: Generales, abstractas, obligatorias, coercitivas, de derecho público, etcétera.

La norma penal pertenece a la categoría filosófica del deber ser que forma parte del derecho objetivo, es decir, forma parte del conjunto de normas jurídico-penales que definen los delitos. Está claro que estas normas también forman parte de lo que se conoce en doctrina como normas positivas.

La norma está estructurada por el hecho jurídico y la consecuencia de derecho que en el caso de la norma penal, dicha estructura la compone por la definición del delito y la determinación de la pena correspondiente. "De tal forma; la norma penal no solo contiene la definición del delito, sino por su propia estructura, también la consecuencia jurídica; es decir, la pena."[27]

La ley penal se puede definir como el conjunto legislativo en materia penal que regula el delito, las penas, las medidas de seguridad que por lo general se dividen en parte especial y parte general; entre este conjunto legislativo se pueden encuadrar el Código Penal y demás leyes penales especiales. Mientras que norma penal se

[26] Antinori, Eduardo. **Conceptos básicos del derecho**. Pág. 36.
[27] García Máynez, Eduardo. **Introducción al estudio del derecho**. Pág. 173.

puede definir como el dispositivo penal cuya estructura se caracteriza por la descripción de la conducta (tipo penal) y su consecuencia (la pena).

1.7. El derecho penal guatemalteco

En general, el derecho penal guatemalteco sigue la línea garantista (observancia de las garantías sustantivas y procesales) y la humanista (respeto a los derechos humanos); además, tiene su fundamento en la Constitución Política de la República, por lo que se puede afirmar que basa su interpretación según las reglas de la hermenéutica constitucional. Este método interpretativo se caracteriza por la interpretación de las normas ordinaria a partir del contenido de la norma constitucional. Un ejemplo de esta forma interpretativa (hermenéutica) lo constituye el principio de legalidad (Artículo 17), la presunción de inocencia (Artículo 14), derecho de defensa (Artículo 12) y, la irretroactividad de la ley penal (Artículo 15). Todos los artículos citados son de la Constitución Política de la República.

La observancia de todas estas garantías surgen de la existencia o, dicho de otra forma, de la conformación de un Estado democrático de derecho; esto significa que la aplicación de la ley penal se basa en el respeto a las garantías sustantivas, procesales y de derechos humanos que favorecen al imputado.

CAPÍTULO II

2. Teoría del delito

2.1. Generalidades

El estudio del delito, para una mejor comprensión, se realiza por medio de la dogmática jurídico penal, por lo que es importante insistir en que el derecho penal no crea los delitos; al contrario, la creación del delito es un aspecto puramente legislativo que solo el Estado está facultado de crear. En la creación legislativa, los delitos se describen mediante el tipo penal, caracterizando las conductas humanas y protegiendo determinados bienes jurídicos de cualquier posible lesión por medio de estas conductas.

En todo caso, es por medio de la dogmática jurídico penal que se hace el análisis estratificado del delito. Por virtud de la dogmática se analizan los tipos penales vigentes, consistente con el desglose de los elementos de los elementos del delito con lo cual, se llega a la explicación científica y analítica de todos los elementos que lo conforman.

La norma penal contiene el tipo penal y el conjunto de las normas penales es a lo que se le denomina ley penal, que está contenida en un cuerpo legal llamado Código Penal. Por lo general, la definición de los delitos se encuentra en la parte especial del

Código Penal, cada uno de los delitos definidos en la parte especial del Código Penal contiene elementos que individualizan la conducta y según el bien jurídico protegido así será la naturaleza del delito. Por ejemplo: en el homicidio, el bien jurídico protegido es la vida.

Pacheco afirma que la teoría del delito no se limita únicamente al estudio de la aplicación de la ley penal, sino que también analiza por separado los estratos analíticos del delito.[28] Estos estratos analíticos son los que configuran objetiva y subjetivamente el delito.

En la actualidad, existe unanimidad doctrinaria en lo que se refiere a los elementos que configuran el delito, cuya caracterización y estudio es ampliamente aceptada en la teoría del delito. Zaffaroni afirma, "la dogmática penal se pregunta cuándo hay delito, cuándo se deba aplicar una pena y cuál debe ser la medida de la pena. Procura responderlo construyendo, con la ayuda de la lógica la idea del delito y la pena conforme al derecho penal vigente".[29] La dogmática también se proyecta hacia la política penal, que juega un papel fundamental en la interpretación de los tipos penales y, asimismo, de los textos jurídico penales. Por medio de la dogmática jurídico penal se plantean de forma sistemática las soluciones más viables a las diferentes circunstancias que se puedan plantear en un caso concreto.

---

[28] Pacheco Mandujano, Luis Alberto. **Teoría del delito**. Pág. 7.
[29] **Ibíd**. Pág. 281.

"La dogmática penal tiene como función determinar a través de un sistema interpretativo lógico el alcance del injusto, del reproche y de la punibilidad".[30] Por medio de ésta se pone de manifiesto cualquier error en la norma penal, especialmente en materia del tipo; es decir, al momento de interpretar el texto legal.

Zaffaroni afirma "que la dogmática jurídico penal contribuye a la comprensión de los momentos principales del delito y ayuda a comprender el alcance teleológico de la norma":[31] Esto se caracteriza para determinar cuando hay delito; es decir, si la conducta observada por el sujeto se encuadra en alguno de los tipos penales, después de hacer el análisis dogmático estratificado de los elementos del delito. Además "posibilita la adecuación de la interpretación de la norma conforme a su sentido teleológico y adaptado de las variables impuestas por la dinámica social":[32] Esto se refiere a la adecuación de la conducta en la norma y según el fin último de la conducta, por esta razón se afirma, que en el sentido teleológico se debe adaptar las variables de la dinámica social.

2.2. Definición de delito

Zaffaroni define el delito de una forma sencilla: "conducta típica, antijurídica y culpable".[33] Esta definición contiene los elementos o estratos analíticos del delito

---

[30] Zaffaroni, Eugenio Raúl. **Ob. Cit**. Tomo I. Pág. 158.
[31] **Ibíd**. Pág. 159.
[32] **Loc. Cit**.
[33] Zaffaroni, Eugenio Raúl. **Tratado de derecho penal, parte general**. Tomo III. Pág. 208.

aceptados en la actualidad por la mayoría de tratadistas; se puede apreciar, entonces, que la sencilla definición de Zaffaroni está conformada únicamente por los elementos característicos y aceptados del delito. Esta es la definición que se adopta en el presente estudio.

Otra definición un poco más compleja de delito es "conducta humana individualizada mediante un dispositivo legal (tipo) que revela su prohibición (típica), que por no estar permitida por ningún precepto jurídico (causas de justificación), es contraria al orden jurídico (antijurídica) y que, por serle exigible al autor que actuase de otra manera en esa circunstancia, le es reprochable (culpable)".[34]

Con relación a esta definición en el presente estudio no se está de acuerdo, toda vez que si bien contiene los elementos generales de la definición aceptada, la misma se enreda en explicar innecesariamente cada uno de estos elementos. Para dar una mejor comprensión de los elementos del delito se utiliza la dogmática penal.

2.3. Naturaleza jurídica del delito

Para determinar la naturaleza jurídica del delito es necesario caracterizar su noción en cuanto al hecho punible, es decir, el delito mismo. "En la vida real el delito se

[34] Pacheco Mandujano, Luis Alberto. **Ob. Cit**. Pág. 5.

presenta siempre como un hecho particular (homicidio, robo, violación, etc.), al que la ley atribuye la pena o medida como consecuencia jurídica".[35]

Es innegable que el delito como parte integrante y objeto de estudio del derecho penal por medio de la teoría del delito, absorbe la naturaleza jurídica de éste, es decir, cae en la esfera del derecho público. Aunque en este sentido no hay que confundir la acción pública del delito con su naturaleza jurídica, si se toma en cuenta que hay delitos de acción privada.

2.4. Teorías que explican el delito

En la actualidad todavía existe cierto debate en la teoría del delito sobre si éste es producto de la causalidad o que está determinado por el fin que se persigue con la conducta típica. Es así que las dos principales teorías que tratan de explicar el delito se dividen en: teoría de la causalidad y la teoría finalista.

Ambas teorías se fundamentan en la conducta, la diferencia es que en la teoría de la causalidad el resultado de la conducta está determinado por la causalidad como causa adecuada para producir el resultado dañoso; mientras que, para la teoría finalista, la conducta es el resultado del ejercicio de la actividad finalista de la acción humana voluntaria y no causal.

---

[35] Politoff L., Sergio y Jean Pierre Matus A., María Cecilia Ramírez. **Ob. Cit.** Pág. 157.

2.4.1. Teoría de la causalidad

La teoría de la causalidad es producto de la escuela positivista que afirma: "la criminalidad varía y depende de una serie de causas que se interrelacionan en la sociedad, en este sentido, por lo que el delito es siempre el producto de determinadas causas".[36] Concibe el delito como un mero producto natural sobre la noción del ser que se basa en la responsabilidad moral del sujeto; es a partir de esta noción que se crea la teoría del delincuente nato de Cesare Lombroso, "quien es aquel que está ataviado por una serie de rasgos antropológicos y anomalías físicas los cuales lo conducen a ser un criminal".[37]

Esta teoría confirma, que debido a las diferentes relaciones que se establecen en la sociedad, se traducen en acciones que generan consecuencias, por ejemplo, la comisión de un delito, el efecto de éste será producido por la causa inicial, es decir, la acción causal que le da origen. También, afirma que toda condición del resultado se encuentra en relación material con ésta, es decir, a la causalidad. Se caracteriza esta teoría (causalidad adecuada) en que, no toda condición del resultado es causa en sentido jurídico, "sino sólo aquella que es adecuada para producir el resultado".[38]

---

[36] Fontan Balestra, Carlos. **Ob. Cit**. Pág. 56.
[37] Andrade Rendón, Rosa Elena. **Teoría y método de Cesar Lombroso en el hombre delincuente**. Pág. 22.
[38] Landaverdi, Moris. **La causalidad en el derecho**. https://enfoquejuridico.org/2015/11/10/la-causalidad-en-derecho-penal/. Extraído el 1 de abril de 2019.

El Código Penal guatemalteco en el Artículo 10 regula la relación de causalidad al establecer los hechos previstos en las figuras delictivas serán atribuidos al imputado, cuando fueren consecuencia de una acción u omisión normalmente idónea para producirlos, conforme a la naturaleza del respectivo delito y a las circunstancias concretas del caso o cuando la ley expresamente los establece como consecuencia de determinada conducta. De la interpretación del contenido normativo del artículo citado se desprende que el derecho penal guatemalteco, por lo menos a nivel formal, sigue la teoría de la causalidad adecuada.

2.4.2. Teoría finalista

Según la teoría finalista, la conducta humana en general está sometida a la voluntad ya que no hay conducta que sea producto de la causalidad. En efecto, para esta teoría la conducta típica esta condicionada por la voluntad de obtener un determinado resultado; "este resultado es producto del poder de voluntad del ser humano guiado por la capacidad de prever, en cierta medida, el resultado de su propia actividad.[39]

Para la teoría finalista, la acción de la actividad humana siempre persigue un fin determinado, por lo que en la teoría del delito, la conducta entendida como actividad humana siempre está dirigida a la obtención de un resultado producto de la voluntad.

---

[39] Peña Gonzáles. Oscar y Frank Almanza Altamirano. **Teoría del delito: Manual práctico para su aplicación en la teoría del caso**. Pág. 93.

"La voluntad implica siempre una finalidad".[40] Esta es la teoría que se adopta en la presente investigación.

2.5. Elementos del delito

El derecho penal como una ciencia jurídico-normativa no crea los delitos, por el contrario lo que hace es regular determinadas conductas opuestas al orden jurídico penal, porque violentan y atentan contra ciertos bienes jurídicos protegidos o tutelados por el derecho penal.

Del estudio y análisis de estas conductas relevantes para el derecho penal, surge la teoría del delito que trata desde una perspectiva científica muy especial, llamada dogmática jurídico-penal de desglosar cada uno de los elementos que conforman el delito, siendo el elemento fundamental de éste la conducta. El derecho penal en tanto regula conductas que pueden lesionar determinados bienes, lo que hace es proteger estos bienes jurídicos para que los mismos no sean lesionados por la conducta típica.

En este sentido, si la norma penal contiene la descripción de la conducta mediante el tipo, que determina el carácter descriptivo, en sí misma no prohíbe por ejemplo, matar (homicidio); al contrario, describe una conducta que en su momento deber motivar al sujeto mediante la prevención general a no matar. Por ejemplo: el Artículo

[40] Girón Palles, José Gustavo. **Teoría del delito**. Pág. 9.

123 del Código Penal tipifica (describe) el delito de homicidio, la norma no prohíbe matar, sino la norma pretende motivar a los potenciales homicidas a no cometer el delito de homicidio.

"La teoría del delito es el estudio de la aplicación de la ley penal, que establece un orden para plantear y resolver los problemas de su aplicación, mediante el método analítico (dogmática) de estudiar por separado cada uno de los estratos que conforman el delito".[41]

En un primer momento analítico y excluyendo la culpabilidad se puede determinar lo que en la doctrina se le llama, un injusto penal (conducta típica y antijurídica),[42] en este punto, la culpabilidad todavía tiene que ser determinada, es decir, la desvaloración de la conducta típica y antijurídica.

Con la determinación de la culpabilidad se completan todos los elementos y se puede afirmar la existencia del delito, es decir, la concurrencia de todos elementos: conducta, tipicidad, antijurídica y culpabilidad. En los apartados siguientes se hará el análisis de los elementos del delito, con el propósito de comprender la configuración y existencia dogmática de éste.

---

[41] Pacheco Mandujano, Luis Alberto. **Ob. Cit.** Pág. 7.
[42] Zaffaroni, Eugenio Raúl. **Ob. Cit.** Tomo III. Pág. 12.

2.5.1. La conducta

La conducta según la teoría del delito aceptada por unaminidad por los tratadistas, es el primer elemento o estrato analítico. Zaffaroni considera que este primer estrato analítico no constituye cualquier conducta, sino ésta entendida como una conducta humana que "se constituye en la base común de todas las figuras delictivas tipificadas en las normas penales de la parte especial del Código Penal".[43]

Sin conducta no hay delito y si ésta no está tipificada se ampara en el principio de legalidad; la conducta es una condición natural de toda persona, por lo que afirmar que las personas observan diversidad de conductas no es incorrecto, porque de todas las conductas humanas las únicas que interesan para el derecho penal son aquellas que describe (tipo) la norma penal. Ésto equivale a afirmar que para el derecho penal y especialmente para la teoría del delito, las condutas que interesan con aquellas que están tipificadas en la parte especial del Código Penal.

Para la teoría finalista del delito, la conducta es considerada tanto como acción u omisión. Puig afirma que la conducta, en materia de derecho penal y especialmente en la teoría del delito, "adquiere una significación importante, se sirve en la

[43] **Ibíd**. Tomo III. Pág. 44.

determinación para la existencia o no de un delito y penada por la norma prohibitiva".[44]

La conducta, que el derecho penal considera relevante, es aquella que lesiona un bien jurídico tutelado que el legislador ha previsto puede ser lesionado por el hecho delictivo tipificado en la parte especial del Código Penal. Es importante aclarar que para el derecho penal, observando la conducta desde la óptica realista lo que hace es diferenciar las variadas conductas, con el objeto de determinar y reconocer aquellas que lesionan ciertos bienes jurídicos protegidos, en el entendido que conducta es el presupuesto del delito siempre y cuando, "se den los demás elementos del mismo".[45]

De tal forma que cuando se analiza la conducta en la teoría del delito, es necesario diferenciar entre el derecho y la moral, que constituye entre ambos una sustancial diferencia axiológica, "que se basa en el utilitarismo y sus efectos jurídicos que revisten la conducta en la teoría del delito frente a la conducta moralmente aceptada".[46]

Con el argumento anterior lo que se trata de puntualizar es que la conducta como el primer elemento analítico del delito, no se puede abordar desde el plano puramente

---

[44] Mir Puig, Santiago. **Función de la pena y teoría del delito en el Estado democrático de derecho**. **Ob. Cit.** Pág. 45.
[45] **Ibíd**. Págs. 48-49.
[46] Serrano Piedecasas Fernández, José Ramón y Juan María Terradillos Basoco. **Manual de teoría jurídica del delito**. Pág. 37.

moral, toda vez que la conducta, en la teoría del delito está fuera de este campo (la moral). Si bien, alguna conducta puede ser moralmente reprochable en determinado círculo, para el derecho penal puede que no sea así o al contrario.

Lo anterior tiene mucha relevancia por cuanto que con la noticia de la comisión de un delito, el órgano jurisdiccional competente al inicio debe establecer la existencia de una conducta penalmente relevante y diferenciar de ésta, cualquier injerencia moralmente considerada. Si la conducta no es relevante para el derecho penal, desde ya se puede determinar que no existe delito que perseguir, por tanto, es innecesario continuar con la investigación criminal. "Si no existe acción (*conducta*), ya no se continúa con el análisis de la siguiente categoría, la tipicidad".[47]

En este mismo sentido, el Código Penal en los Artículos 24 y 25 establece algunos presupuestos por medio de los cuales se puede determinar la ausencia de conducta, entre los que se pueden mencionar; a) La legítima defensa; b) Agresión legítima; c) Falta de provocación suficiente por parte del defensor; d) Fuerza exterior, etcétera.

Otro aspecto relevante con respecto a la conducta es la intención porque si el sujeto tiene la intención, por ejemplo, de cometer un robo y éste al final se arrepiente, aunque pudiera parecer reprochable tal intención, si no se exterioriza mediante la conducta, no hay nada que reprochar. "Es importante señalar que si la conducta se

[47] Girón Pallares, José Gustavo. **Ob. Cit**. Pág. 10.

encuentra en la fase interna, por muy deplorable que sea, si no se ha exteriorizado, no hay acción (*u omisión*)".[48]

2.5.2. La tipicidad

La tipicidad, estudiada en la teoría del delito, supone el análisis dogmático del tipo penal, éste es considerado en la teoría del delito como la descripción de la conducta en la norma, mientras que la tipicidad es la que individualiza la conducta penalmente relevante. Para los efectos de la presente investigación es importante señalar que la tipicidad entendida así (dispositivo individualizador de la conducta) y el tipo que describe la conducta cuya naturaleza es descriptiva obliga, a diferenciar entre la tipicidad y el tipo penal, así estar en posición de comprender la relación estrecha que existe entre ambos.

En cuanto al contenido de la tipicidad y del tipo, la mayoría de los estudiosos del derecho penal y de la teoría del delito consideran que la tipicidad es el proceso lógico por el cual el juzgador encuadra la conducta a la descripción que hace tipo penal de esta conducta. Mientras que, el tipo sería la descripción de la conducta contenida en la norma penal, que luego, mediante el proceso lógico jurídico y dogmático de encuadrar la conducta al tipo se determina que ésta (la conducta) es típica.

---

[48] **Loc. Cit.**

En este orden, la tipicidad "es la adecuación de un hecho cometido, a la descripción que de ese hecho se hace en la ley (*penal*)".[49] La tipicidad por tanto, es el dispositivo por excelencia "genuinamente penal, cuya función es precisamente la individualización de las conductas delictivas que le otorga relevancia penal a la conducta".[50]

Nieves identifica la tipicidad con la subsunción y la describe "como la relación entre un hecho –conducta- y un tipo penal, que permite concebir la tipicidad del primero, es decir, la operación lógica jurídica de que la conducta o acción se subsume bajo el tipo penal, lo que llama conducta típica".[51] La tipicidad concebida como la adecuación de la conducta al tipo penal, será efectiva siempre y cuando no se presente en este estrato analítico del delito algún elemento negativo.

La conducta que no está definida en el Código Penal y que aparentemente lesionó un bien jurídico tutelado por el derecho penal, automáticamente genera una duda razonable en el juzgador, en el sentido de considerar que la conducta no se puede encuadrar en ningún tipo penal porque la misma no está tipificada en la ley.

Otra situación sería si la conducta no se encuadra (tipicidad) en ningún tipo penal, se dice que la conducta es atípica, es decir que no existe en la parte especial del

---

[49] Rojas Chacón, José Alberto y Cecilia Sánchez Romero. **Teoría del delito aspectos teóricos y prácticos**. Tomo I. Pág. 79.
[50] **Ibíd**. Pág. 170.
[51] Nieves, Ricardo. **Teoría del delito y práctica penal. Reflexiones dogmáticas y mirada crítica**. Págs. 47 y 50.

Código Penal, por tanto no hay delito que perseguir (por ejemplo el ciberdelito en la actualidad en Guatemala).

De los argumentos anteriores se puede determinar la relación estrecha entre la conducta atípica y el principio de legalidad nullum crimen nulla poena sine lege, regulado en el Artículo 17 de la Constitución Política de la República: no son punibles las acciones u omisiones que no estén calificadas como delito o falta y penadas por ley anterior a su perpetración.

2.5.3. La antijuridicidad

La antijuridicidad, como el tercer elemento o estrato analítico del delito es el juicio negativo (desvalor) que se hace de la conducta típica.[52] Por lo tanto, como estrato analítico del delito, la antijuridicidad se considera en la teoría del delito de acto, como la desvaloración de la conducta y no como desvalor del delincuente.

También, a la antijuridicidad se le denomina en la teoría del delito como injusto penal, que se caracteriza en la teoría de la contrariedad como un elemento de desvalor de la conducta típica; es decir, por medio de este elemento se determina que la conducta típica es contraria al derecho penal.

[52] **Ibíd**. Pág. 12.

Según el argumento anterior la conducta típica y antijurídica no se puede considerar como un delito en sentido estricto, toda vez que, con antijurídica la conducta típica solo se considera como un delito en sentido amplio contrario a derecho; esto es lo que se conoce en la teoría del delito como injusto penal, es decir, "como una conducta típica desvalorada".[53]

"El delito lato sensu sería la conducta típica o la conducta típica y antijurídica -que se llama injusto penal-, es decir, la conducta que no es delito en sentido estricto, sea porque le faltan la antijuridicidad y la culpabilidad o la culpabilidad solamente (sic)".[54] Ahora bien, para poder superar este estrato analítico y afirmar la existencia del injusto penal es necesario analizar, si en la antijuridicidad no concurre algún elemento negativo que imposibilite considerar la conducta típica como contraria a derecho.

Con este análisis se puede determinar que, si bien la conducta es típica al momento de concurrir algún elemento negativo de la antijuridicidad, no es posible continuar con la desvaloración de la conducta. En el Código Penal a estos elementos negativos se les denomina causas de justificación (Artículo 24 del Código Penal).

"La función del juicio de antijuridicidad se reduce a una constatación negativa de la misma, es decir, a la determinación de si concurre o no alguna causa de

---

[53] **Loc. Cit.**
[54] Zaffaroni, Eugenio Raúl. **Ob. Cit.** Tomo III. Pág. 561.

justificación".[55] Las causas de justificación en el Código Penal, que eliminan la antijuridicidad de la conducta, están reguladas en el Artículo 24. En este caso la conducta típica no se considera contraria al derecho penal, por tanto, no merecedora de una pena.

Entre estas están: a) Legítima defensa, b) estado de necesidad, y c) legítimo ejercicio de un derecho. "Las causas de justificación son condiciones que justifican el actuar de la persona en una conducta inicialmente prohibida, pero que al concurrir situaciones justificantes su actuar es lícito. Este acto justificado prácticamente es un permiso del orden jurídico para obrar como se hizo".[56]

De tal forma, si el juez determina que confluye alguna o algunas de las causas de justificación enumeradas en el Artículo 24 del Código Penal, no puede seguir hacia el juicio de culpabilidad, toda vez, la conducta típica no es antijurídica porque ésta (la conducta) está amparada en una causa de justificación.

2.5.4. La culpabilidad

Desde la noción puramente subjetiva y desde la teoría del delito se denomina capacidad de culpabilidad o la capacidad mental de comprender el carácter ilícito de la conducta y determinarse de acuerdo a esa comprensión, este aspecto subjetivo es

[55] **Ibíd**. Pág. 54.
[56] **Ibíd**. Pág. 59.

el que orienta el juicio de reproche de la conducta típica y antijurídica. Por supuesto que la reprochabilidad recae en la conducta y no en el autor de la conducta. Por medio de la culpabilidad se le reprocha la conducta desvalorada y se sanciona al autor de esa conducta.

La culpabilidad "es el conjunto de condiciones por la que se justifica la imposición de una pena al autor de un delito".[57] El juicio de reproche, que se hace de la conducta típica y antijurídica tiene ciertos presupuestos, entre los que se encuentran la verificación de sí el sujeto activo al momento de cometer el hecho, estaba en posibilidad de motivarse por la norma violada, es decir, "la exigibilidad de motivación que provoca la norma (prevención general)".[58]

"La capacidad de culpabilidad consiste en aquellos supuestos que se refieren a la madurez psíquica y a la capacidad del sujeto para motivarse (edad, salud mental etc.) La capacidad de motivación es la capacidad de motivarse por el cumplimiento del deber. Esta capacidad requiere a) la capacidad de comprender la desaprobación jurídico penal, b) la capacidad de dirigir el comportamiento de acuerdo con esa comprensión".[59]

Se hace necesario aclarar que el juicio de culpabilidad o de reproche no va dirigido hacia el autor de la conducta, al contrario, en un Estado democrático de derecho

---

[57] Muñoz Conde, Francisco. **Derecho penal y control social**. Pág. 52.
[58] Zaffaroni, Eugenio Raúl. **Tratado de derecho penal. Parte general**. Tomo IV. Pág. 10.
[59] Girón Pallares, José Gustavo. **Ob. Cit**. Pág. 75.

respetuoso de las garantías individuales, el juicio de culpabilidad va dirigido hacia la conducta, aunque por supuesto de comprobarse la existencia del delito, el autor de la conducta será sentenciado con una pena. El desvalor y el reproche vayan dirigidos hacia el autor y no a la conducta. El juicio de culpabilidad (que sería más o menos la etapa procesal del debate), se inicia cuando se ha determinado que la conducta es típica y antijurídica (contraria a derecho) y el imputado es el presunto autor.

El contenido del derecho penal y procesal penal guatemalteco se inclina por un sistema de culpabilidad y no de autor. Lo que quiere decir que la reprochabilidad o juicio de culpabilidad van dirigidos a reprochar la conducta y no al autor de la conducta. Por lo que se puede afirmar que solamente mediante un juicio de culpabilidad se puede efectivamente reprochar la conducta y responsabilizar al sujeto.

Como en todos los elementos del delito en la culpabilidad también pueden concurrir elementos negativos. El Código Penal en el Artículo 25 denomina a estos elementos causas de inculpabilidad, por medio de los cuales, aunque la conducta sea típica y antijuridica por virtud de estos elementos negativos, no se puede responsabilizar al sujeto. Entre las causas de inculpabilidad están: a) Miedo invencible, b) Fuerza exterior, c) Error; d) Obediencia debida y e) omisión justificada.

La capacidad de culpabilidad tal y como se afirmó antes constituye el aspecto mental del sujeto, y el grado de motivación que la norma penal produce en éste con el objeto

que no cometa el delito. Este aspecto psíquico es lo que se conoce como imputabilidad-inimputabilidad.

Las causas de inimputabilidad están reguladas en el Artículo 25 del Código Penal, a) Ser menor de edad y b) Quien en el momento de la acción u omisión, no posea, a causa de enfermedad mental, de desarrollo psíquico incompleto o retardado o de trastorno mental transitorio, la capacidad de comprender el carácter ilícito del hecho o de determinarse de acuerdo con esa comprensión, salvo que el trastorno mental transitorio, haya sido buscado de propósito por el agente.

2.6. La punibilidad

La pena, según la estructura de la norma es la consecuencia jurídica del supuesto de derecho, que en este caso sería el delito. La pena o la teoría de la punibilidad no se estudia en la teoría del delito, sino que la misma se analiza fuera de esta; según la teoría finalista del delito, la punibilidad está fuera del análisis estratificado del delito por cuanto es la consecuencia del mismo. En algunos casos, aunque el delito sea efectivamente probado, es imposible la aplicación de una pena.

De esta cuenta se considera que la punibilidad es un elemento accidental del delito; de acuerdo a esta noción, se puede afirmar que la coherencia por medio de la cual se explica por qué, aunque exista un delito como tal, la aplicación de la pena puede

ser ineficaz, si el presupuesto para la imposición de una pena es, la existencia material y legal de un delito.

La confluencia de todos y cada uno de los elementos estratificados del delito: conducta típica, antijurídica y culpable es en principio el presupuesto considerativo y viable para la imposición de una pena. Pero qué pasa cuando no obstante la existencia del delito, la pena es ineficaz; es decir, no es aconsejable su imposición.

El anterior argumento se puede caracterizar de la siguiente forma: ante la imposibilidad de imponer una pena al responsable del delito, existe la posibilidad que éste sea inimputable. Porque en el momento del juicio de culpabilidad o de reproche de la conducta, es posible que concurra algún elemento de inimputabilidad, lo que determinaría la ineficacia de la pena, pero no de una medida de seguridad.

Zaffaroni afirma que "en el caso de que se dé el supuesto sobre la existencia jurídica de un delito y la imposibilidad de no poderse aplicar la pena establecida, existe la posibilidad de determinar la inoperancia de la pena, pese por supuesto la existencia del delito".[60]

Esta situación, al mismo tiempo, constituye una excepción para la aplicación de la pena; no obstante, la existencia del delito. "La pena en este supuesto carece de efectividad, esta inefectividad de la pena se puede deber a dos razones: la primera

[60] Zaffaroni, Eugenio Raúl. **Ob. Cit**. Tomo IV. Pág. 11.

que correspondería al derecho penal –*razones personales*- y la segunda las que están fuera del derecho penal y que corresponden al derecho procesal penal".[61]

[61] **Ibíd**.

CAPÍTULO III

3. El ciberdelito como especie del delito

3.1. Generalidades

Las formas de criminalidad siempre han evolucionado al mismo tiempo que evoluciona o se desarrolla la sociedad, tal es el caso del vertiginoso desarrollo de la tecnología informática y junto a estos avances también ha surgido una nueva forma de crimen. A este tipo de crímenes se les denomina ciberdelito, el cual se especializa precisamente por la utilización de plataformas informáticas para la comisión de este delito.

La comisión del ciberdelito tiene una particularidad para realizarlo; ya que no se necesita que el sujeto activo esté físicamente presente en el lugar afectado por el delito, puesto que el mismo se comete a distancia y los instrumentos del crimen son básicamente un ordenador (computadora) y conexión a internet. Esto, por supuesto, ha generado una creciente preocupación a nivel mundial, especialmente sobre el tratamiento que se le debe dar a este tipo de delitos porque como ya se afirmó anteriormente, el lugar de la comisión del delito no es el mismo del lugar en que el bien jurídico es afectado, es decir, es un delito que se comete a distancia.

"Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales".[62]

La comisión de este delito puede afectar a una compañía, institución estatal u otro ubicada en determinado lugar y ser cometido desde otro. Según la caracterización tradicional en la teoría del delito sobre el lugar donde se cometió el hecho delictivo, el Código Penal guatemalteco en el Artículo 20 establece que "el delito se considera realizado: en el lugar donde se ejecutó la acción, en todo o en parte; en el lugar donde se produjo o debió producirse el resultado y en los delitos de omisión, en el lugar donde debió cumplirse la acción omitida".

En el caso anteriormente citado, no hay problema de ubicar el lugar de la comisión del delito, pero tratándose del ciberdelito, el determinar el lugar en donde se cometió el hecho es un problema complejo para la teoría del delito y para las legislaciones penales. Toda vez que la acción delictiva se realiza en un lugar o en un territorio, que por lo general son desconocidos y cuyos efectos se producen en otros lugares o países.

---

[62] Acurio del Pino, Santiago. **Delitos informáticos: Generalidades**. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. Extraído el 28 de marzo de 2019.

Por medio de la teoría del delito se le ha dado una solución al problema planteado, es decir, la ubicación o el lugar donde se cometió el hecho delictivo y tratándose del ciberdelito la ubicación de la comisión del delito o de donde surte sus efectos, se determina de acuerdo a lo regulado en el Artículo 22 de la Convención sobre el ciberdelito.

Los argumentos del párrafo anterior se sustentan en lo regulado en el Artículo 22 del Convención sobre el Ciberdelito: "1 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido: a) En su territorio; o b) A bordo de un buque que enarbole pabellón de dicha Parte; o c) A bordo de una aeronave matriculada según las leyes de dicha Parte; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo. 2 Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos. 3 Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición. 4 El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho

interno. 5 Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales".

La solución a la que se hace referencia es que el delito se comete en "todas las jurisdicciones en las que se haya realizado algún elemento del tipo; en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".[63]

El ciberdelito, en consecuencia, no se puede considerar para su tratamiento desde la esfera exclusivamente local, si se toma en cuenta la caracterización del mismo en el sentido de que la acción (delito) se realiza en un Estado diferente a aquel en que surte sus efectos, lo que ha determinado la necesidad de internacionalizar el tratamiento jurídico penal del ciberdelito.

Finalmente, la preocupación de la comunidad internacional se ha orientado a dirigir sus esfuerzos para que los Estados adopten políticas y legislaciones específicas en la prevención, combate, persecución y enjuiciamiento del ciberdelito y la ciberdelincuencia.

---

[63] Ortiz Pradillo, Juan Carlos. **Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos**. Pág. 8.

3.2. Definición de ciberdelito

El ciberdelito es "cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito (sic)".[64]

También, es la "actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito".[65] Es el "acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[66]

Si bien las definiciones transcritas proporcionan elementos valiosos para caracterizar el ciberdelito, dogmáticamente no parecen estar completas. De los elementos de cada una de ellas se pueden extraer aquellos que ayudan a individualizar el ciberdelito. Hay que tener presente que el análisis y estudio de este tipo de conducta es relativamente nuevo, lo que se puede atribuir a que su desarrollo dogmático en la teoría del delito no es muy abundante. Prueba de ello es que, la mayoría de estudios especializados sobre este delito se pueden encontrar dispersos en revistas, foros y

---

[64] **Loc. Cit.**
[65] Posada Maya, Ricardo. **El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual**. Pág. 80.
[66] Lima, María de la Luz. **Delitos electrónicos**. Pág. 100.

congresos nacionales e internacionales sobre informática, ciberdelito, ciberseguridad y en pocas tesis académicas.

Pero, entre los elementos más relevantes de las definiciones transcritas se pueden destacar: el uso de ordenadores (computadores), acceso a internet, diferentes plataformas de redes informáticas, todo lo cual, puede ser utilizado como medio o fin para la comisión del ciberdelito.

3.2.1. Diferencia entre ciberdelito y delito informático

A pesar del hecho de que en la teoría del delito, el análisis jurídico y dogmático del ciberdelito es relativamente nuevo, se ha podido apreciar que se tienden a confundir los términos ciberdelito y delito informático. Más exactamente porque son considerados como sinónimos, aunque no lo son.

"Las diferencias entre el concepto de delitos informáticos y cibercrimen, conceptos que normalmente son utilizados como sinónimos pero que a fines académicos y doctrinarios tienen diferencias que es aquí el momento adecuado para señalarlas".[67]

Una de las diferencias entre estos dos términos "radica en su organización. "El delito informático es aquel que se comete casi a diario, por ejemplo: acceso indebido a una

[67] Temperini, Marcelo. **Delitos informático y cibercrimen: alcances, conceptos y características. En cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet**. Pág. 56.

cuenta de correo electrónico, borrar información importante de una computadora que no le pertenece al quien borró la información, una amenaza de muerte utilizando una red social o similar".[68]

En cuanto al ciberdelito, se refiere a toda una serie de conductas delictivas que observan un grado de sofisticación y profesionalismo informático, "utilizando para ello técnicas delictivas altamente tecnológicas motivadas, especialmente por cuestiones puramente económicas, para divulgar a la opinión pública información sensible de entidades públicas, privadas o de personas particulares".[69]

3.3. Naturaleza jurídica del ciberdelito

Para determinar con precisión la naturaleza del ciberdelito es necesario tomar en cuenta las características de éste: "a) capacidad de automatización; b) Tecnología integrada en los programas informáticos; c) ejecución a distancia; y, la más importante, de donde se deriva la naturaleza jurídica de este delito, d) el carácter transnacional de la ciberdelincuencia que necesita frecuentemente de la cooperación y colaboración judicial internacional".[70]

---

[68] **Loc. Cit.**
[69] **Loc. Cit.**
[70] Unión Internacional de Telecomunicaciones. **Guía de ciberseguridad para los países en desarrollo**. Pág. 17.

Por tanto, la naturaleza jurídica de este delito es de carácter internacional, toda vez que trasciende las fronteras nacionales, ya que puede ser cometido en un país y producir sus efectos en otro. Por esta razón y porque la rapidez con la que se ejecutan estos delitos, se hace necesario poner en práctica el funcionamiento de sistemas informáticos, protocolos de seguridad y emitir leyes que legitimen estos sistemas y protocolos.

3.4. El bien jurídico protegido en el ciberdelito

El bien jurídico protegido por el tipo penal del ciberdelito no constituye algo nuevo porque los bienes lesionados por este delito generalmente ya están regulados en los los códigos penales nacionales, aunque la comisión y repoercusiones internacionales lo confieren ciertas características que lo hacen diferente.

"Se puede decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente (sic)".[71]

---

[71] Acurio del Pino, Santiago. **Delitos informáticos: Generalidades**. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. extrapido el 29 de marzo de 2019.

En este sentido, tampoco hay que descartar que por la dinámica en el desarrollo de las TIC's (Tecnologías de Información y Comunicación) y la propia dinámica del ciberdelito, sea perfectamente posible que surjan en el futuro bienes jurídicos que para el derecho penal tradicional no son actualmente relevantes, pero en virtud de esta modalidad delictiva y su propia dinámica será o ya es necesaria su protección.

De tal forma que atendiendo a la noción de ciberseguridad, uno de los aspectos importantes o, dicho de otra forma, uno de los pasos fundamentales es incorporar a la legislación nacional el tipo penal del ciberdelito y al mismo tiempo implementar una política de seguridad cibernética, legitimada precisamente por esta legislación, que en el caso de Guatemala se encuentra plasmada en la Estrategia Nacional de Seguridad Cibernética, misma que actualmente no cuenta con un marco jurídico que la legitime.

3.5. La internacionalización del ciberdelito

Derivado de la naturaleza jurídica del ciberdelito (Ver apartado 3.2. del capítulo III) es importante, aunque sea de forma breve, resaltar los alcances que la comisión de este delito tiene en el plano internacional. Uno de estos alcances es la importancia que la comunidad internacional le ha brindado a la colaboración entre estados tendiente a la prevención, persecución y sanción del ciberdelito.

"Ningún país puede controlar lo que un sujeto transmite o hace desde el territorio de otro mediante las modernas redes de comunicación y, sin embargo, dichas actividades sí pueden tener notables efectos dentro de sus fronteras".[72]

En todo caso, la llamada internacionalización del ciberdelito se puede caracterizar por la naturaleza misma de éste, por la necesidad que los Estados tienen de colaboración con otros estados y porque este delito puede ser perseguido tanto por el Estado en el que se comete y por el Estado en que se producen sus efectos.

De tal forma "la internacionalización del ciberdelito ha obligado a la actualización del derecho penal internacional en materia informática, que en la actualidad se está caracterizando por la noción de un derecho penal internacional informático".[73]

El Convenio Sobre la Ciberdelincuencia o Convenio de Budapest, en el preámbulo, afirma precisamente la necesidad de la cooperación internacional contra el ciberdelito y la ciberdelincuencia, desde la perspectiva de un derecho penal internacional en los siguientes términos: "estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal".

---

[72] Galán Muñoz, Alfonso. **Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática**. Pág. 91.
[73] **Loc. Cit.**

3.6. El ciberdelito frente a la ciberseguridad

Los instrumentos por excelencia en la comisión de este tipo de delito son básicamente: un ordenador (computadora) y conexión a internet, por lo que cuando se habla de seguridad informática o seguridad cibernética, de lo que se está haciendo referencia es de todas aquellas aplicaciones y dispositivos que en alguna medida contrarresten los ataques cibernéticos, conductas que consideran como ciberdelitos.

No solamente se refiere en sentido estricto a esto, la seguridad informática o ciberseguridad abarca aspectos políticos, económicos y legislativos. En este orden, la seguridad informática "es entendida como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computadoras. En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización".[74]

Por supuesto que, ante la ineficacia actual de la legislación penal sobre el ciberdelito en Guatemala, una solución es la implementación de este tipo de sistemas de seguridad informática; aunque a la par de la implementación de las medidas preventivas para evitar los ataques informáticos y el ciberdelito, es necesaria la creación de políticas públicas acompañadas de la legislación penal correspondiente,

---

[74] Sain, Gustavo. **La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal. En Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet**. Pág. 18.

para fortalecer la respuesta penal al cibercrimen y la que seguridad informática sea integral.

3.6.1. Definición de ciberseguridad

Ciberseguridad es "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".[75]
Otra definición es que "la ciberseguridad es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque. Esto incluye soluciones tecnológicas como el uso de programas antivirus o la actualización periódica de software; además, de buenas prácticas en el uso de las tecnologías de la información, como no abrir archivos de direcciones de correos que provienen de fuentes desconocidas (sic)".[76]

Con diferentes términos pero igual contenido, las definiciones transcritas refieren, en términos generales, que la ciberseguridad incluye acciones tendientes a la protección de los equipos informáticos, las redes, los datos que en estos se almacena y el tráfico por medio de internet de estos datos. Pero la ciberseguridad para que tenga

[75] Ministerio de Gobernación (Guatemala). **Estrategia nacional de seguridad cibernética**. Pág. 60.
[76] MacGregor B., Rafael Fernández (coordinador). **Perspectiva de ciberseguridad en México**. Pág. 21.

un alcance y la legitimidad en la persecución y sanción del ciberdelito, debe contar con el marco jurídico correspondiente (en el caso de Guatemala todavía no existe normativa sobre la materia).

3.6.2. Definición de ciberataque

La ciberseguridad generalmente comprende las acciones que toman los usuarios corporativos o individuales con el fin de proteger los dispositivos informáticos y la información que en ellos se almacena frente a los ciberataques; en un momento dado, estos (los ciberataques) pueden constituir la comisión de un delito, al que se le donimina ciberdelito. Esta caracterización se deriva dependiendo de cuál es el bien jurídico que se lesione con motivo del ciberdelito, porque una cosa es la protección individual o corporativa de los ciberataques y la otra, es la protección por parte del Estado del bien jurídico violentado por el ciberdelito. El ciberdelito abarca una serie de conductas que van desde ataques financieros y tecnológicos, hasta el robo de identidades e información sensible de empresas o gobiernos.

3.7. El ciberdelito y la denominación ciberdelincuencia

El Convenio Sobre la Ciberdelincuencia afirma en el preámbulo, que es urgente la cooperación entre los Estados frente a la ciberdelincuencia, toda vez que ésta atenta y pone en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas,

redes y datos informáticos, lo que hace necesaria la tipificación a nivel nacional de estas conductas para su efectiva persecución y sanción.

La denominación de ciberdelincuencia es una consecuencia lógica que se deriva precisamente del término ciberdelito. En este sentido se entiende por ciberdelincuencia a "las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas".[77]

Otra definición de ciberdelincuencia es: "el conjunto de aquellas acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito".[78]

Una tercera definición es: "actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva".[79]

De las tres definiciones transcritas se pueden establecer sus elementos: la ciberdelincuencia es una actividad o conducta delictiva; para cometer el hecho se vale de sistemas informáticos, redes, servidores con conexión a internet. Como se puede apreciar, tanto en la doctrina como en la legislación internacional (Convenio

[77] **Ibíd**. Pág. 18.
[78] Mateos Pascual, Pedro. **Ciberdelincuencia: Desarrollo y persecución tecnológica**. Pág. 18.
[79] Unión Internacional de Telecomunicaciones. **Ob. Cit. Guía de ciberseguridad**... Pág. 17.

de Budapest) el ciberdelito y la ciberdelincuencia tiene un tratamiento dogmático como sinónimos.

3.8. Elementos configurativos del ciberdelito

En la legislación penal guatemalteca no se contemplan los ciberdelitos, el Código Penal solamente describe algunas conductas denominadas delitos informáticos. Entre estas están: a) destrucción de registros informáticos (Artículo 274 A); b) alteración de programas (Artículo 274 B); c) reproducción de instrucciones o programas de computación (Artículo 274 C); d) registros prohibidos (274 D); e) manipulación de información (Artículo 274 E); f) uso de información (Artículo 274 F); y, g) programas destructivos (Artículo 274 G).

Todos los anteriores delitos caen en la categoría, como la denominación lo indica, en los llamados delitos informáticos, pero no en la categoría de los ciberdelitos. Toda vez, que los primeros (delitos informáticos), son aquellos que se cometen a diario, por ejemplo: acceso indebido a una cuenta de correo electrónico o borrar información importante de una computadora que no le pertenece a quien borró la información, etcétera, lo que suena similar a los delitos informáticos que tipifica el Código Penal de Guatemala y el ciberdelito se refiere a toda una serie de conductas delictivas que observan un grado de sofisticación y profesionalismo informático, utilizando para ello técnicas delictivas altamente tecnológicas motivadas especialmente por cuestiones puramente económicas.

En materia de ciberdelitos la configuración actual o dicho de otra forma, la definición de estas conductas se hace en plural, es decir, se habla de ciberdelitos toda vez que abarcan una gran variedad de conductas delictivas, entre las que se encuentran:

a) "Ataques contra sistemas y datos informáticos;
b) Usurpación de la identidad;
c) Distribución de imágenes de agresiones sexuales contra menores;
d) Estafas a través de Internet;
e) Intrusión en servicios financieros en línea;
f) Difusión de virus;
g) Botnets (redes de equipos infectados controlados por usuarios remotos);
h) Phishing (adquisición fraudulenta de información personal confidencial)".[80]

Por tanto, se deduce la afirmación de que el ciberdelito y el ciberataque son dos instituciones jurídicas distintas. El ciberdelito abarca una serie de conductas que van desde ataques financieros y tecnológicos hasta robo de identidades e información sensible de empresas y gobiernos. En este orden, se puede afirmar que el ciberdelito y el ciberataque son dos cosas distintas. En consecuencia, el ciberataque es "un intento no autorizado por la vía digital de acceder a un sistema de control, dispositivo

[80] Loredo González, Jesús Alberto y Aurelio Ramírez Granados. **Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo**. Pág. 45.

electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones".[81]

[81] MacGregor B., Rafael Fernández (coordinador). **Ob. Cit.** Pág. 16.


UNIVERSIDAD DE SAN CARLOS
CENTRO UNIVERSITARIO DE SANTA ROSA
COORDINACIÓN ACADÉMICA

CAPÍTULO IV

4. La seguridad cibernética en Guatemala

4.1. Generalidades

Para que exista como institución la Estrategia Nacional de Seguridad Cibernética de Guatemala, es imprescindible la creación de leyes que le proporcionen el sustento jurídico de legitimación en las cuales se regule todo lo relativo al diberdelito y a la seguridad cibernética, que garantice en primer lugar, la persecución del ciberdelito y en segundo lugar, la protección los datos informáticos y la información almacenada en dispositivos digitales.

Con el desarrollo de la informática y la transmisión multidireccional de datos a través de internet, surgieron los ciberataques, situación que provocó la necesidad de resguardar toda esta información, pero sin la existencia del debido soporte legislativo, que surgió después, como una forma de legitimidad jurídica en la tipificación de los delitos cibernéticos, la lucha contra los ciberataques y el ciberdelito.

La seguridad cibernética antecede a la legislación que tipifica los delitos cibernéticos, porque históricamente la seguridad cibernética nació con la transmisión de datos, el almacenamiento de éstos y la consiguiente vulnerabilidad de los sistemas informáticos.

En este sentido, la seguridad cibernética normalmente ha estado a cargo de empresas privadas que ofrecen este servicio, el cual va dirigido a la banca, la industria, las bolsas de valores y en general a todas aquellas actividades económicas y de servicios que utilicen sistemas informáticos y, que en un momento dado pueden ser objeto de ciberataques.

Frente a esta problemática, es decir los ciberataques, no es suficiente con los servicios de ciberseguridad que prestan ciertas compañías especializadas en la materia; a la par de esta estrategia privada en la protección de la información informática se hace necesaria la incorporación legislativa de leyes penales que sancionen los ciberataques, que una vez tipificados se convierten en ciberdelitos.

Está claro que la seguridad cibernética y la legislación que sancione el ciberdelito, son dos componentes clave en la lucha en contra el cibercrimen. En especial porque el ciberdelito por su propia naturaleza es transnacional, lo que lo caracteriza no solo como un problema nacional sino mundial, porque hoy el ciberdelito es una preocupación internacional.

4.2. Antecedentes de la Estrategia Nacional de Seguridad Cibernética

En el año 2018, el gobierno de la República de Guatemala lanzó un documento titulado: Estrategia Nacional de Seguridad Cibernética. Este documento, según afirma en la introducción, constituye un primer paso que tiene como objetivo

establecer directrices y objetivos en materia de seguridad cibernética. Los objetivos se centran únicamente en la seguridad cibernética y no en la necesidad de crear un marco jurídico normativo que combata los ciberataques. En ellos solamente se hace alusión a la promoción de reformas en materia de seguridad cibernética.

Asimismo, la Estrategia Nacional de Seguridad Cibernética reconoce que "no establece acciones específicas en el ámbito de la Seguridad Cibernética y Protección de Infraestructuras Críticas".[82] Lo que significa que la Estrategia solo se enfoca en la protección del ciberespacio; acciones que, desde hace más de tres década empresas privadas de seguridad cibernética han desarrollado.

La seguridad cibernética, vista desde la óptica del Estado, es relativamente reciente; puesto que no fue sino hasta la publicación del Plan Operativo Institucional 2016-2020, que por primera vez se tocó el tema de la ciberseguridad, mientras que por parte del sector privado la seguridad cibernética se ha estado desarrollando desde hace más de tres décadas.

4.2.1. Informe de seguridad cibernética: Observatorio de la Seguridad Cibernética en América Latina

Como producto del Informe sobre Seguridad Cibernética de 2016, el que se puede considerar el antecedente más cercano de la Estrategia Nacional de Seguridad

[82] Ministerio de Gobernación (Guatemala). **Ob. Cit. Estrategia nacional**... Pág. 15.

Cibernética guatemalteca, el gobierno se apresura y pública una serie de documentos en los que propone acciones a seguir en materia de seguridad cibernética, que a estas alturas (2020) ninguna ha podido ser efectivamente operativa.

La causa de la inoperancia de la Estrategia Nacional de Seguridad Cibernética es que no cuenta con el marco normativo legal para su implementación, toda vez que, no está legitimada por ninguna norma legal. En este sentido las directrices y objetivos plasmados en el informe no existen ni han nacido a la vida jurídica, lo que es lo mismo afirmar que no tienen legitimidad jurídica. Entre tanto, la seguridad cibernética por el momento sigue siendo por lo menos por parte del Estado de Guatemala una preocupación del sector privado.

"Aunque Guatemala no cuenta con una estrategia a nivel nacional para el desarrollo de la educación de seguridad cibernética, una universidad técnica y varias empresas privadas ofrecen títulos y certificaciones en seguridad de la información".[83] Como se puede apreciar, es el sector privado en más interesado en la protección de los ciberataques, por lo que exige una acción coordinada para la prevención, preparación, respuesta y recuperación frente a incidentes por parte de las autoridades gubernamentales, el sector privado y los ciudadanos.

[83] Observatorio de la Seguridad Cibernética en América Latina y el Caribe. **Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?** Pág. 76.

4.2.2. Plan Estratégico Institucional 2016-2020

El Plan Estratégico Institucional 2016-2020 hace una reseña de las obligaciones que el Estado de Guatemala tiene a nivel internacional en el combate del ciberdelito. Además, plantea la necesidad de hacer frente a los delitos informáticos y a los delitos en internet mediante la colaboración internacional que suena paradójico ya que el Estado de Guatemala no es parte del Convenio sobre la diberdelincuencia.

Dicho planteamiento se basa en el Convenio Sobre la Ciberdelincuencia o Convenio de Budapest, del cual Guatemala no es signataria. En este Convenio se obliga a los Estados Partes a que armonicen las leyes penales nacionales, mejorar las técnicas de investigación y promover la cooperación entre los diferentes países en el combate contra el ciberdelito.

Uno de los problemas que se presentan de inmediato sobre el Plan Estratégico Institucional 2016-2020, es que tampoco cuenta con un marco normativo legal que le de sustento y legitimidad jurídica. Asimismo, el Estado de Guatemala no ha hecho las reformas o implementado las leyes necesarias en materia de ciberdelito, según lo establece el Convencio de Budapest sobre la ciberdelincuencia.

Si bien, por parte del sector privado la ciberseguridad ha observado un cierto desarrollo, por parte del gobierno desafortunadamente ha estado relegado, ya que no se han tomado acciones concretas en este sentido y lo que es todavía más

preocupante no se ha legislado en la creación de leyes que persigan y sancionen el ciberdelito.

4.3. Política pública nacional contra el ciberdelito

La definición que el Estado de Guatemala propone para una política contra el ciberdelito es la que define la política de seguridad cibernética, según la cual, "es aquella que pretende desarrollar mecanismos efectivos encaminados a la protección del ciberespacio y la construcción de cultura de ciberseguridad en la sociedad".[84]

En cuanto a una política pública nacional contra el ciberdelito propiamente dicha, Guatemala en la actualidad no cuenta con ella. Con lo único que cuenta el Estado de Guatemala es con una propuesta de política pública contra el ciberdelito, esta propuesta solamente se basa en la perspectiva de creación de una cultura de ciberseguridad y en menor medida de leyes tendientes a la persecución, juzgamiento y sanción del ciberdelito. En la actualidad ni una ni otra propuesta se han concretizado.

Entre los lineamientos de este proyecto (que no se ha realizado) se propuso: a) adecuar los instrumentos legales del Sistema Nacional de Seguridad para incluir la seguridad cibernética con un enfoque de prevención y gestión de riesgos; b) crear, aprobar e implementar una ley contra la ciberdelincuencia, con referencia en

[84] Ministerio de Gobernación (Guatemala). **Ob. Cit. Estrategia nacional**... Pág. 15.

estándares internacionales aplicados a la realidad guatemalteca y; c) modernizar las instituciones del sector justicia y adecuar normas y estándares en los procesos judiciales y el manejo de la evidencia digital.[85]

El Estado de Guatemala no cuenta con una ley especial contra el ciberdelito. No obstante, desde el año 2017 un año antes de que el gobierno publicara la Estrategia Nacional de Seguridad Cibernética, se presentó al Congreso de la República una iniciativa de Ley Contra la Ciberdelincuencia, (Iniciativa de ley 5254). Para poder implementar el funcionamiento eficaz de una política pública contra el ciberdelito se requiere la creación de toda la estructura jurídica penal necesaria, con el objeto de dotar a estas políticas públicas de la legitimación de ejecución, la sustentación y, certeza y seguridad jurídica necesarias.

En este orden, según la autora de la presente investigación, los lineamientos básicos para estructurar una política pública contra el ciberdelito, deben tomar en cuenta: a) definir toda la estructura de la información; b) estructurar acciones concretas en materia de prevención y sanción del ciberdelito; c) difusión e información y; d) la debida cooperación y asistencia internacional. Todo lo cual, contribuirá a la institucionalización de la ciberseguridad y el combate al ciberdelito.

[85] **Ibíd**. Pág. 36.

4.4. Desafíos que presenta la lucha contra el ciberdelito

El término ciberdelito se puede considerar en un sentido plural ya que el mismo abarca una serie de tipos delictivos, todos con una misma naturaleza jurídica y de carácter internacional. En efecto, el ciberdelito comprende una variedad de infracciones penales, lo que supone un grado de complejidad al momento de su tipificación y clasificación.

Un aspecto que resulta muy importante y que presenta uno de los desafíos más grandes en el combate contra el ciberdelito, lo constituyen los alcances que el mismo tiene en las esferas económica, política y social, esferas en donde surte sus efectos la comisión de un ciberdelito.

"Debido a la incertidumbre acerca de cuál es la proporción de delitos que los afectados informan y al hecho de que no se ha encontrado una explicación a la reducción del número de ciberdelitos registrados, por el momento no existen pruebas suficientes para predecir la tendencia y la evolución en el futuro".[86]

Entre los países latinoamericanos que se consideran más vulnerables a los ciberataques esta Guatemala debido a la poca infraestructura informática y la carencia de una ley penal especial que tipifique los ciberdelitos, por ello está en la

[86] Unión Internacional de Telecomunicaciones. **El ciberdelito: Guía para los países en desarrollo**. Pág. 20.

lista de los países con mayor vulnerabilidad de estos ataques. No obstante, que cuenta con documentos sobre seguridad cibernética, ninguno está operativo; esto no representa la solución al problema y debido a la alta vulnerabilidad, falta de tipificación del ciberdelito, los ciberataques no pueden ser perseguibles.

Al contrario, en materia de ciberseguridad, la iniciativa privada ha tomado la delantera, algo de lo que hasta los gobiernos se han beneficiado porque al final, éstos resultan siendo clientes de las empresas de ciberseguridad. Asimismo, otro de los desafíos sobre el combate del ciberdelito lo constituye en sí mismo el hecho delictivo."Los delincuentes buscan secretos comerciales",[87] esta es una de las razones porqué es el sector privado el más interesado en la seguridad cibernética, aunque de esta preocupación no se puede sustraer el Estado.

En general, el uso masivo de internet y la utilización de las tecnologías de la información y la comunicación, es otro factor que presenta serios desafíos en la lucha contra el ciberdelito, si se toma en cuenta que éste por lo general no tiene rostro y probablemente el hecho se comenta desde un país, hacia objetivos ubicados en otros países.

"El reciente desarrollo de las TIC ha redundado no sólo en nuevos ciberdelitos y métodos delictivos, sino también en nuevas formas de investigar el delito

[87] **Ibíd**. Pág. 25.

cibernético".[88] Por esto, es importante que se tomen todas las medidas legislativas necesarias a fin de que el Estado (de Guatemala) se fortalezca en la lucha y sanción del ciberdelito.

Hoy, el Estado de Guatemala no cuenta con recursos jurídico-normativos, lo que implica que todo intento en la lucha contra el ciberdelito será estéril ya que no puede ser sancionado en el territorio guatemalteco. Si en la legislación penal guatemalteca no están tipificados los ciberdelitos, éstos no pueden ser perseguidos ni sancionados.

El Estado de Guatemala, no ha logrado beneficiarse integralmente de los avances de la legislación penal internacional sobre la ciberdelincuencia y al mismo tiempo de los avances logrados en el campo de las tecnologías de la información y comunicación, sobre todo fortalecer en gran medida las capacidades de las entidades encargadas de hacer cumplir la ley".[89]

Es por las anteriores razones, los desafíos que presenta la lucha contra el ciberdelito comienzan con la adhesión y ratificación del Convenio de Budapest, a lo que sigue la creación legislativa de leyes penales que tipifiquen los delitos cibernéticos y que sancionen este tipo de conductas; de lo contrario, Guatemala no podrá desarrollar las

[88] **Ibíd**. Pág. 69.
[89] **Loc. Cit**.

capacidades necesarias para combatir y sancionar estos delitos, ni tener la capacidad de cooperar internacionalmente en esta materia.

"Las entidades encargadas de hacer cumplir la ley pueden utilizar ya la potencia cada vez mayor de los sistemas informáticos y los complejos programas forenses para acelerar las investigaciones".[90] Lamentablemente Guatemala no cuenta con estas capacidades tanto en materia legislativa como de cooperación internacional.

4.5. La Estrategia Nacional de Seguridad Cibernética

La ciberseguridad incuestionablemente desempeña un papel importante en el desarrollo de la protección de datos, tanto en su fase de transferencia como de almacenamiento. En este sentido, las tecnologías de la información y comunicación, así como de los servicios de Internet son los campos en donde el cibercrimen opera.

Por lo tanto, lograr que el uso de internet (navegar por la web) sea confiablemente seguro, es el motor que ha impulsado el desarrollo de novedosos sistemas de seguridad cibernética. Estos nuevos sistemas de seguridad cibernética tienen y deben ser aprovechados para el establecimiento de políticas de seguridad cibernética impulsadas por el Estado siempre y cuando cuenten con el debido soporte legal.

[90] **Loc. Cit.**

Se afirma, por tanto, que las estrategias de ciberseguridad tienen que contar con el marco jurídico normativo imprescindible para una mejor puesta en marcha y, sobre todo, la institucionalización de la ciberseguridad del Estado. Esto significa, dotar a los diferentes usuarios (individuales o colectivos) de la seguridad y certeza jurídica del del tráfico informático y la prevención del ciberdelito.

En este sentido se afirma, "que solo en España un total del 95% de los ciberdelitos en 2014 quedaron impunes, es decir, el sujeto o sujetos activos de estos delitos jamás fueron encontrados".[91] El dato señalado, también pone de manifiesto la gran complejidad que tienen los países desarrollados en la persecución del ciberdelito, no se diga los desafíos que representa para los países Latinoamericanos.

Ahora bien, si se comparan los recursos económicos y legislativos entre España y Guatemala, advirtiendo que el primero es Parte del Convenio de Budapest y que cuenta con una legislación penal propia sobre el ciberdelito, se puede hacer una comparación empírica de los alcances y daños que el ciberdelito puede o está ocasionando en Guatemala (especialmente el grado de impunidad), considerando que en primer lugar: que no es Parte del Convenio de Budapest y, en segundo lugar: no cuenta con la legislación penal especial sobre ciberdelito.

[91] Fundación Telefónica. **Ciberseguridad, la protección de la información en un mundo digital**. Pág. 32.

Hablar de impunidad del ciberdelito en Guatemala se asocia inmediatamente al hecho de que en esta materia Guatemala está aislada y, al mismo tiempo que no cuenta con la legislación necesaria. De tal forma, que los niveles de impunidad devienen en que, en el país no existe materia que persequir respecto al ciberdelito. Por lo que se puede afirmar que la sola estrategia nacional de seguridad cibernética, no representa ningún avance ni fortalece la lucha contra el ciberdelito.

De tal forma, la lucha contra este delito no se puede integrar plenamente solo con la publicación de una estrategia nacional de seguridad cibernética, ni tampoco con realizar reformas al Código Penal, al contrario, la lucha contra este tipo de delitos requiere de algo más profundo, es decir, la creación de leyes especiales que tipifiquen y sancionen el ciberdelito en concordancia con las normas jurídicas internacionales sobre la materia.

En este sentido, la estrategia nacional de seguridad cibernética más que ser una propuesta seria de política pública contra el ciberdelito, es un documento cosmético que no resuelve el problema ni fortalece la seguridad cibernética. El hecho de que el Estado de Guatemala desafortunadamente no es parte del Convenio de Budapest, por sí mismo desvela la falta de seriedad y compromiso del Estado en la lucha y sanción del ciberdelito.

La Estrategia Nacional de Seguridad Cibernética entre las bases que propone para construir una política pública de seguridad cibernética están: a) la armonización de

los delitos cibernéticos; b) el fortalecimiento de los procesos de investigación cibercriminal, y c) la admisibilidad de la evidencia electrónica. Aunque los anteriores aspectos están en concordancia con los objetivos del Convenio de Budapest, estas propuestas por parte del Estado no tienen ningún sustento legal ni sentido inmediato.

En este orden, el preámbulo del Convenio de Budapest se afirma, que "convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada".

Asimismo, dicho instrumento internacional, en otra parte, afirma que pretende dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, aso cp,p facilitar la obtención de pruebas electrónicas de los delitos, es necesaria la plena colaboración internacional. Estos en general son parte de ejes que el Convenio de Budapest regula normativamente en la lucha contra el ciberdelito y que el Estado de Guatemala, por medio de la Estrategia Nacional de Seguridad Cibernética propone como bases para implementar la ciberseguridad. Comparando el Convenio de Budapest con la Estrateria, este último documento no es normativo sino solo una serie de buenas intenciones.

Es por las razones mencionadas en el párrafo anterior en la presente investigación y sustentado en los argumentos anteriores que se puede afirmar, que la propuesta del

Estado de Guatemala en materia de seguridad cibernética no está revestida de la seriedad ni el formalismo que se requieren para una efectiva incorporación de políticas públicas efectivas.

Aunque parezca repetitivo, la Estrategia Nacional de Seguridad Cibernética no posee la jerarquía jurídica ni normativa para efectivamente perseguir y sancionar el ciberdelito en Guatemala; es más, esta estrategia no cuenta con ningún sustento legal y aunado a esto Guatemala no es parte del Convenio de Budapest y no cuenta con un marco normativo legal propio que tipifique el ciberdelito, que es una de las principales obligaciones de los Estados que son Parte del Convenio.

En este sentido, en el Convenio de Budapest no se establece la creación de estrategias de seguridad cibernética (aunque estas son importantes, más no efectivas sin el debido sustento jurídico normativo), al contrario, el Convenio citado establece que los Estados Partes se comprometen a adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar y sancionar como delito, en el derecho interno, el ciberdelito en todas sus manifestaciones.


UNIVERSIDAD DE SAN CARLOS
CENTRO UNIVERSITARIO DE SANTA ROSA
COORDINACIÓN ACADÉMICA

CAPÍTULO V

5. Estrategia Nacional de Seguridad Cibernética y su implementación en el ordenamiento jurídico guatemalteco

5.1. Generalidades

El hecho de que el Estado de Guatemala no sea Parte del Convenio Sobre la Ciberdelincuencia (Convenio de Budapest) en principio no es obstáculo para que en la legislación penal Guatemala se tipifique ya sea por virtud de una reforma o bien, por la creación de una ley especial sobre el ciberdelito (este último caso es el más aconsejable).

Ser parte del Convenio de Budapest representa para el Estado de Guatemala formar parte del grupo de naciones que interna e internacionalmente están comprometidos en la lucha global contra el ciberdelito.

Un aspecto importante definitivamente para la implementación de una política contra el ciberdelito es ser Parte del Convenio de Budapest que para un Estado en desarrollo como el guatemalteco, es participar de la experiencia de los países industrializados y tener la oportunidad de adquirir las capacidades necesarias tanto en la persecución penal como en la investigación criminal de este delito.

No es lo mismo ser parte del Convenio, percibir los beneficios y las experiencias de otros países, especialmente aquellos con un mayor grado de desarrollo e industrialización, que no formar parte y no percibir el mayor grado de los beneficios y las experiencias de estos estados en materia del combate al ciberdelito.

El Estado de Guatemala mediante la Estrategia Nacional de Seguridad Cibernética reconoce las grandes desventajas de no ser parte de este Convenio. "En las mesas de trabajo para el desarrollo de esta Estrategia, se determinó la importancia de que el país se adhiera al Convenio de Budapest, para generar y fortalecer esos vínculos de coordinación y cooperación internacionales facilitados por un marco jurídico armonizado con los países adscritos a dicho Convenio".[92]

Asi mismo, el Estado de Guatemala también reconoce en la Estrategia Nacional de Seguridad cibernética, la importancia de crear un marco jurídico penal nacional (con el cual no cuenta actualmente) en que incluyan las directrices que el Convenio de Budapest establece, de aquí la necesidad que el Estado de Guatemala se adhiera a este Convenio.

El Estado de Guatemala puede a su propia instancia crear una estrategia nacional de seguridad cibernética, incluso proponer la creación de una ley contra el ciberdelito tal y como lo ha hecho hasta el momento. Sin embargo, esta unilateralidad no es

[92] Ministerio de Gobernación (Guatemala). **Ob. Cit. Estrategia Nacional**... Pág. 21.

producente, toda vez que el Estado de Guatemala no obtiene los beneficios sobre las experiencias en materia de cooperación internacional, que los Estados parte del Convenio han adquirido.

5.2. El problema de ejecutar la Estrategia Nacional de Seguridad Cibernética sin un marco jurídico penal

Toda política pública en general y en particular una política pública sobre el ciberdelito, necesariamente debe contar con el marco legal idóneo que la legitime. En Guatemala por virtud del principio de legalidad los ciberdelitos tal y como se tipifican en el Convenio de Budapest no pueden ser penados, es decir, nadie puede ser condenado por un ciberdelito porque éstos no están debidamente tipificado en el Código Penal o en una ley penal especial, (Artículos 17 de la Constitución Política de la República y 1 del Código Penal).

Paradógicamente esto es lo que reconoce el Estado de Guatemala en la Estrategia Nacional de Seguridad Cibernética cuando afirma: "que a pesar de que existen investigaciones y enjuiciamientos por delitos cibernéticos, estos han sido enfocados en el tema de derecho de propiedad intelectual y de pornografía infantil y no en lo relativo al ciberespacio en general".[93]

[93] **Ibíd**. Pág. 22.

Sin la debida legislación penal sobre ciberdelito, cualquier estrategia sobre seguridad cibernética o bien política pública sobre el ciberdelito no es funcional. La seguridad cibernética ha sido hasta el momento una preocupación nacional solo es a nivel privado, tomando acciones prevenir contra los ciberataques lo que no tiene nada que ver con la prevención penal, este tipo de prevención contra los ciberataques es de naturaleza privada que no conlleva ningún tipo de sanción penal.

Asi mismo, sin una una legislación integral sobre seguridad cibernética y sobre el ciberdelito, las diferentes empresas que han adoptado protocolos de seguridad cibernética, no están obligadas a cooperar con las autoridades sobre los ciberataques de que son víctimas y revelar sus propios protocolos. "Debido a que no existe una normativa que regule el apoyo de los proveedores de Internet, se enfatizó que una regulación apropiada es necesaria para intercambiar información con las instituciones de seguridad y justicia específicamente en las investigaciones, para determinar la fuente de un ataque cibernético".[94]

Esto plantea un panorama complejo porque advierte que sin un marco normativo legal tanto la cooperación de las empresas privadas dedicadas a la prestación de servicios de internet o de seguridad cibernéticas, no están obligadas a proporcionar información al Estado. También, la falta de una legislación penal sobre ciberdelito impide en todo caso, la sola tentativa de iniciar una investigación criminal con motivo de un ciberataque, toda vez que en la legislación penal no están tipificados este tipo

[94] **Loc. Cit.**

de delitos, porque las investigaciones no prosperan debido a que los actuales delitos son solo aquellos que se denominan informáticos y no ciberdelitos propiamente dichos.

El Estado de Guatemala, en materia de investigación, no tiene las capacidades suficientes tanto técnicas como de investigación (porque son altamente especializadas y sofisticadas), por ejemplo, no existe una noción clara de lo que es la prueba digital, la cadena de custodia digital, la recolección de indicios digitales y cómo se manipulan los dispositivos que pueden ser parte de la prueba. "Para la investigación de delitos cibernéticos, se destaca la falta de conocimiento de las autoridades sobre la aplicación de la ley acerca de una prueba digital, así como de la cadena de custodia digital, el traslado y la sustracción de la evidencia sobre el ISO 27037. De igual forma las salas de audiencia no están equipadas para recibir evidencia digital, y hacen falta instrumentos para la adecuada recolección, preservación, transporte y análisis de la evidencia digital (ej. bolsas de Faraday utilizadas para preservar dispositivos móviles como evidencia)".[95]

Es evidente que si no existe la tipificación de un delito, no puede existir un protocolo adecuado en cuanto a la custodia digital, prueba digital, tampoco se hace necesario el equipamiento de las salas de audiencia para recibir evidencia digital; es decir, el Estado no puede erogar recursos (humanos, económicos, etcétera), para perseguir un delito que no está tipificado, como es el caso de Guatemala.

[95] **Loc. Cit.**

5.3. Convenio Sobre la Ciberdelincuencia (Convenio de Budapest)

Tomando en cuenta que el ciberdelito constituye una forma especializada de una conducta criminal y sobre todo debido a la complejidad en cuanto al lugar de la ejecución del hecho y el lugar en donde este genera sus efectos, de lo que se deriva la connotación que se conoce como la internacionalización del ciberdelito y el ciberdelincuente; este último, en la mayoría de los casos es anónimo, no tiene rostro y esto es lo que coayuva en los altos índices de impunidadm, la respuesta estatal también tiene que ser especializada y con altos índices de tecnificación y sofisticación.

Los países que son Parte del Convenio de Budapest y que cuentan con la legislación penal sobre ciberdelincuencia, tienen la experiencia, la sofisticación y las capacidades para combatir el ciberdelito y fortalecer la ciberseguridad. En este orden: ¿Cuáles serían las proyecciones de los países como Guatemala que son son Parte del Convenio de Budapest y no cuentan con una legislación sobre la ciberdelincuencia? Las proyecciones en la lucha contra el ciberdelito en países como Guatemala son casí nulas.

No ser parte del Convenio de Budapest y no contar con la legislación adecuada, forman parte de los puntos de esta proyección que que marcan la complejidad de las respuestas; estas mismas disyuntivas se presentaron en la comunidad europea en cuanto a la persecución penal del ciberdelito y todavía más complejo, la aplicación

efectiva de la sanción penal del ciberdelito. Debido a esto, surge el primer instrumento internacional para perseguir y sancionar internacionalmente el ciberdelito, este instrumento internacional es el Convenio Sobre la Ciberdelincuencia.

Este, como ya se afirmó, es el primer instrumento de su tipo; es decir, constituye el primer instrumento internacional normativo y vinculante sobre la ciberdelincuencia. El Convenio fue suscrito en el año 2001 como una iniciativa del Consejo de Europa, mismo que no se suscribió exclusivamente para los países europeos, sino que la firma de adhesión está abierta para todos los Estados no europeos.

El preámbulo del Convencio afirma: "los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio...". Aunque el Convenio surgió en una región determinada, sus alcances han sido globales, lo que dio paso a la posibilidad a que Estados de otros continentes (como Guatemala) se puedan adhier al mismo. Lo que por supuesto le da cierto carácter mundial.

La posibilidad está abierta para cualquier Estado que esté interesado en formar parte del Convenio se pueda adherir, inevitablemente lleva a cuestionar sobre la creación en Guatemala de la estrategia nacional de seguridad cibernética y proponer una iniciativa de ley sobre ciberdelincuencia, sin ser parte del Convenio de Budapest.

La probabilidad de que el Estado de Guatemala individualmente tenga éxito en la lucha contra el ciberdelito se minimizan si no es parte de una comunidad global, cuyo

objetivo es la lucha internacional contra el ciberdelito mediante la cooperación internacional.

Guatemala en un momento dado tendrá obligadamente que formar parte de este Convenio, se ignoran los motivos por los que el Estado de Guatemala no se ha adherido a áste, pero lo cierto es que no se puede pretender prevenir, perseguir y sancionar un delito que por naturaleza es de carácter internacional, si no es a través de la cooperación internacional y esto solo se logra siendo parte del Convenio de Budapest.

5.3.1. Análisis jurídico de los alcances del Convenio de Budapest

Es en Europa por medio del Consejo de Seguridad Europea que se promueve la normativa jurídica internacional sobre la ciberdelincuencia con la que según se afirma en el preámbulo, se pretende establecer una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia.

Hay que comprender que al referirse a una política penal común, se hace en el sentido de que cada uno de los miembros del Convenio (países europeos y otros Estados signatarios no europeos), mantengan una estrecha relación de cooperación entre sí, en materia de combate y prevención del ciberdelito (ciberdelincuencia).

La forma que adquiere la estrecha cooperación, es que cada Estado Parte del Convenio adopte una legislación penal adecuada, lo que significa que contenga los elementos comunes de la tipificación de los delitos establecidos en el Convenio, para un efectivo combate a la ciberdelincuencia.

Es claro, que el propósito final de esta normativa internacional es la necesidad de garantizar (como lo afirma el preámbulo), el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos consagrados en diferentes instrumentos internacionales. El Convenio crea las bases por medio de las cuales se establecen los parámetros para que los Estados Partes puedan armonizar en sus propias legislaciones penales el ciberdelito.

"El Convenio de Budapest, por lo tanto, puede servir de lista de verificación para el desarrollo de leyes internas sustantivas y procesales relativas al delito cibernético y la evidencia electrónica. Tal parece que más de 130 Estados en el mundo lo han usado como directriz de una forma u otra. Sin embargo, el Convenio en su totalidad es un documento balanceado, juicioso y coherente y debe considerarse preferiblemente como un todo".[96]

Esta característica del Convenio de Budapest a parte de ser el primero de su clase, es lo que lo ha convertido en un éxito a nivel mundial. Toda vez, que "para los Estados que se convierten en Partes del Convenio, el tratado sirve como un marco

[96] Observatorio de la Seguridad Cibernética en América Latina y el Caribe. **Ob. Cit**. Pág. 22.

legal para la cooperación internacional".[97] En todo caso, no es absoluto, las bases no se agotan con el Convenio al contrario, en cada legislación penal se pueden incorporar, según sean las necesidades y el desarrollo tecnológico del Estado y los bienes jurídicos que pretenda proteger, aspectos propios de la jurisdicción penal.

En el Capítulo I del Convenio de Budapest se definen importantes términos como: sistema informático, datos informáticos, proveedor de servicios y datos sobre el tráfico (Artículo 1), también en el capítulo I del Convenio se establecen las directrices por medio de las cuales cada Estado parte, está obligado a incorporar a su propia legislación una serie de conductas tandientes a proteger la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

En el Capítulo II, se establecen todas aquellas medidas que los Estados Partes están obligados a adoptar, para tipificar los delitos cibernéticos.

Tutelar por lo menos:

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

a) El acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático (Artículo 2).

[97] **Loc. Cit.**

b) La interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos (Artículo 3).

c) Comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos (Artículo 4).

d) Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos (Artículo 5).

e) La comisión deliberada e ilegítima, producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos; una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático (Artículo 6).

Título 2. Delitos informáticos:

a) Introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con

independencia de que los datos sean o no directamente legibles e inteligibles (Artículo 7).

b) Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: Cualquier introducción, alteración, borrado o supresión de datos informáticos, cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona (Artículo 8).

En el título dos se establecen directrices sobre los delitos informáticos que protegen la integridad de los dispositivos informáticos de cualquier ataque cibernético, sirviendo esta directriz dirigida a cada Estado miembro con el objeto de que tipifique estas conductas en su propia legislación penal.

Título 3. Delitos relacionados con el contenido:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
b) La oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
c) La difusión o transmisión de pornografía infantil por medio de un sistema informático;
d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos (Artículo 9).

Se entiende que por virtud de las directrices establecidas en el título 3, cada estado parte tipifique en su propia legislación como ciberdelito todas las conductas relacionadas con la pornografía infantil; es decir, la utilización de personas menores de edad según la definición de niño que establece la Convención Sobre los Derechos del Niño en el Artículo 1, "para los efectos de la presente Convención, se entiende por niño todo ser humano menor de dieciocho años de edad".

En este mismo sentido, también el Convenio de Budapest, en concordancia con lo que establece la Convención Sobre los Derechos del Niños, establece que se entiende por minoría de edad toda persona menor de 18 años de edad (Artículo 9, numeral 3 del Convenio de Budapest). Se hace la salvedad que este parámetro en cuanto a los Estados Partes no puede ser superior, pero sí se puede establecer uno inferior, como mínimo de 16 años de edad. Lo que significa que en todas aquellas sociedades (naciones) en las que la mayoría de edad se alcanza a los 18 años de edad, en materia de pornografía infantil, las legislaciones de estos Estados se deben armonizar con lo que establece el Artículo 9 del Convenio de Budapest, respecto a la edad en la que se considera niño a una persona.

Título 4: Delitos Relacionados con infracciones de la propiedad intelectual y de los derechos afines:

a) Las infracciones de la propiedad intelectual y derechos afines, según se defina en la legislación de dicha Parte, siempre que estos hechos se cometan por medio de un sistema informático. Asimismo, se establece que la tipificación también deberá estar en armonía con los instrumentos internacionales sobre propiedad intelectual y derechos afines, si dicho Estado es parte de estos, lo que significa que la tipificación de estos ciberdelitos, se hará en concordancia con estos instrumentos internacionales sobre propiedad intelectual (Artículo 10 del Convenio).

También, en el Artículo 11 se establece la tentativa y la complicidad. Es de advertir que, por la complejidad de este tipo de delitos, si se toma en cuenta que el mismo se puede cometer desde un país distinto a aquel en que surte sus efectos, en materia de complicidad, se hace más complejo debido a que el cómplice puede estar en el país en donde el ciberdelito genera sus efectos, en el país del autor principal o bien en un tercer país.

Todas estas situaciónes son las que en un momento dado refuerzan la necesidad de la cooperación internacional entre los Estados Parte del Convenio de Budapest. Lo que significa que, al estar fuera del Convenio, se está también fuera de la totalidad de la cooperación entre los Estados Parte del Convenio (caso de Guatemala).

Además, en dicho artículo se establece que:

a) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos.
b) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de los delitos previstos.

El Convenio de Budapest también establece el principio de responsabilidad penal de las personas jurídicas. Al respecto el Artículo 12 regula que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias, para tipificar como delito en su derecho interno cualquier tentativa sobre la comisión del ciberdelito.

La comisión de un delito que sea cometido por cualquier persona física, tanto en calidad individual como miembro de una persona jurídica, que ejerza funciones directivas en la misma, la responsabilidad penal de las personas jurídicas como consecuencia de la comisión de un ciberdelito, se considera cometido por la persona individual.

Se interpreta que ser miembro de cualquier órgano significa formar parte de un poder de representación; una autorización para tomar decisiones en nombre de la persona jurídica y; una autorización para ejercer funciones de control en la persona jurídica.

La responsabilidad de la persona jurídica no se limita a la responsabilidad penal ésta puede ser del orden civil o administrativa, sin perjuicio de la responsabilidad penal de las personas o persona individual que haya cometido el hecho delictivo. El Convenio de Budapest también regula el principio general por medio del cual se establecen las sanciones y medidas que se deben adoptar en cada legislación penal interna de los Estados Parte.

El Artículo 13 del Convenio, establece que:

a) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad y que puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

Es importante resaltar que las sanciones penales que se adopten por cada Estado Parte se deben regir por el principio de proporcionalidad y el de legalidad. Esta es una garantía se establece en el Convenio de Budapest; sin embargo, las sanciones o medidas penales que se establezcan por cada Estado parte, deben ser efectivas y que promuevan la prevención general y especial. Entre estas sanciones también se pueden aplicar aquellas de carácter pecuniario especialmente contra las personas jurídicas que resulten responsables del ciberdelito.

El Convenio de Budapest regula los principios sobre el derecho procesal aplicable al ciberdelito que tiene que ser legislado por cada Estado Parte, siempre tomando en cuenta lo que al respecto regula este instrumento normativo internacional.

El Artículo 14 del Convencio establece que:

a) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.

Se entiende que en materia sustantiva y adjetiva cada Estado Parte se compromete a adoptar medidas legislativas que tiendan no solo a la reforma de los Códigos Penales, sino más exactamente a la creación de normas jurídicas sustantivas y procedimentales especiales en materia de ciberdelito.

Se establecen normas sobre la extradición (Artículo 24) debido al carácter internacional de este delito, las salvaguardas (Artículo 15) que cada Estado establezca para su derecho interno siempre y cuando garanticen la protección adecuada de los derechos humanos, las libertades individuales y la efectiva persecución, juzgamiento y sanción del ciberdelito.

Por último, se establece la facultad de cada Estado Parte a solicitar enmiendas al Convenio de Budapest. Estas enmiendas se refieren especialmente a cuestiones de

la legislación interna de cada Estado una vez adoptado el Convenio y ser Parte del Mismo, los Estados parte pueden solicitar al Secretario General del Consejo de Europa la enmienda propuesta, esto con el fin de armonizar la legislación nacional con el Convenio.

5.3.2. El principio de legalidad y el ciberdelito

En el Convenio de Budapest no se establece nada respecto al principio de legalidad por lo que el tratamiento de este principio se reserva a cada Estado Parte. En este sentido, se ha afirmado que el principio de legalidad se puede violar, en el supuesto de que en un Estado no esté tipificado el ciberdelito (caso de Guatemala) y éste sea en donde se ejecuta el hecho aunque surta sus efectos en otro Estado en el cual sí está tipificado el ciberdelito, bien puede iniciar la persecución penal.

Este es uno de los debates que más fuerza han tenido, sobre todo cuando se discute la cooperación internacional con aquellos Estados que no son miembros del convenio de Budapest y que al mismo tiempo no cuentan con una ley sobre ciberdelincuencia.

De tal forma, para poder armonizar el principio de legalidad con el resto de Estados Parte del Convenio de Budapest, es necesario ser miembro de esta normativa internacional, de lo contrario, la aplicación de un derecho nacional respecto a la comisión de un ciberdelito ejecutado en otro Estado, tiene que estar amparado por

una legislación penal sobre el ciberdelito en ambos Estados, a esto es a lo que se denomina como armonizar la legislación.

Si en uno de los Estados no está tipificado el ciberdelito, por virtud del principio de legalidad en este Estado no es punible, mientras que en el Estado donde sí está tipificado el ciberdelito si el sujeto activo no está en este territorio es casi imposible solicitar su extradición, de allí el alto índice de impunidad de estos delitos.

El Artículo 8 del Código Penal de Guatemala establece que la extradición sólo podrá intentarse u otorgarse por delitos comunes. Cuando se trate de extradición comprendida en tratados internacionales, sólo podrá otorgarse si existe reciprocidad", siempre y cuando la conducta sea delito en ambos Estados.

La Constitución Política de la República de Guatemala, establece en el Artículo 27, segundo párrafo que la extradición se rige por lo dispuesto en tratados internacionales. Mientras que en el Artículo 1 de la Ley Reguladora del Procedimiento de Extradición se regula "el procedimiento de extradición se regirá por los tratados o convenios de los cuales Guatemala sea parte; en lo no previsto en los mismos se regirá por la presente ley".

En el caso de que el delito esté tipificado en el Código Penal o en alguna ley penal especial de un Estado Parte, como sería el caso del ciberdelito, la falta de tipificación en otro Estado en que se ejecutó o bien surte sus efectos, es un problema que

dogmáticamente no puede ser solucionado aplicando la analogía; es decir, la adecuación de una conducta no tipificada en un Estado (ciberdelito), pero que sí está tipificada en otro.

El Artículo 7 del Código Penal de Guatemala establece: "por analogía, los jueces no podrán crear figuras delictivas ni aplicar sanciones". Es por esta razón que es importante que todos aquellos Estados que pretenden proponer o crear una política sobre el ciberdelito, sean parte del Convenio de Budapest de lo contrario están aislados de toda cooperación internacional sobre la materia.

Otro aspecto importante en el que hay que recalcar es que Guatemala no es parte del Convenio de Budapest, tampoco posee una legislación especial sobre el ciberdelito, por lo que cualquier intento de poner en marcha una policía sobre este delito sería fallida.

Lo que se trata de establecer es que si bien Guatemala en el año 2018 publicó la estrategia nacional de seguridad cibernética, esta en sí misma no posee la fuerza ni la legitimidad legal para ser operativa, porque Guatemala no es parte del Convenio de Budapest y tampoco posee una legislación especial sobre el ciberdelito.

En consecuencia, el Estado de Guatemala no puede penar a nadie por la comisión de un ciberdelito, ni se puede perseguir internacionalmente, toda vez que no está tipificado expresamente en la ley penal. Por lo que si alguien en el Estado de

Guatemala comete este delito y sus efectos se dan en otro Estado, en Guatemala no se puede perseguir ni condenar al sujeto. Tampoco se puede aplicar por analogía la legislación del Estado que sufre el ataque, aunque en este sí esté tipificado el ciberdelito. Otro factor que favorece la impunidad en Guatemala de este delito, es que no se puede intentar la extradición del sujeto al que se le imputa el ciberdelito si éste lo ha cometido desde otro Estado y surte sus efectos en Guatemala.

5.4. Análisis de la iniciativa 5254, Ley Contra la Ciberdelincuencia

En marzo de 2017 se presentó al Congreso de la República la iniciativa de ley 5254, que pretende se apruebe la Ley Contra la Ciberdelincuencia. En la exposición de motivos de esta iniciativa se afirma: junto al avance de las tecnologías de la información y comunicación han surgido actividades que se pueden considerar de ilícitas, por lo que es necesaria su tipificación en una ley especial.

Asimismo, se afirma en los motivos de esta iniciativa afirma que los actuales tipos penales contenidos en el Código Penal bajo la denominación de delitos informáticos, ya no responden a las nuevas modalidades de los ciberdelitos que, por su propia naturaleza se comenten utilizando sistemas o redes informáticas.

Muchos de estos delitos ya están reconocidos en la legislación internacional (Convenio de Budapest), lo que hace imprescindible (así lo reconoce esta iniciativa) que el Estado de Guatemala se adhiera a este Convenio. También se reconoce que

solo mediante la adhesión y la ratificación, Guatemala podrá (tal y como se ha afirmado en la presente investigación) lograr la cooperación internacional con el objetivo de contribuir en la lucha contra el ciberdelito.

Uno de los problemas más recurrentes al presentar iniciativas de esta naturaleza lo representa el tiempo, si se toma en cuenta el acelerado desarrollo de la tecnología informática y de internet, que hace de cualquier iniciativa sin aprobar obsoleta, inclusive de leyes sobre ciberdelito vigentes que con el tiempo es necesaria su reforma, para incluir nuevos tipos penales o actualizar los existentes.

El hecho de que Guatemala no sea parte del Convenio de Budapest hizo imperioso que en la exposición de motivos de la iniciativa 5254 analizada, se reconociera que no obstante han transcurrido más de quince años de la firma del Convenio de Budapest, hasta ahora se presenta una iniciativa coherente y actualizada (año 2017) con el texto sin ninguna reserva del Convenio.

El Artículo 1 de esta iniciativa establece el objeto de la ley, el cual es la tipificación de las figuras delictivas y la adecuación de las normas penales existentes para hacer frente a la ciberdelincuencia, se establecen las reglas que regirán el proceso en esta materia, se regulan los medios de prueba digital y pruebas electrónicas, se contempla la creación de los órganos jurisdiccionales competentes y de investigación cibercriminal y lo más significatifo, se establece la cooperación internacional.

Con respecto a la cooperación internacional, Guatemala al no ser parte del Convenio de Budapest, no goza de todos los beneficios de esta cooperación. Lo que no quiere decir, en aras de combatir la ciberdelincuencia que otros Estados no cooperen según sus propios intereses en la persecución y sanción del ciberdelito, pero esto es la excepción a la regla.

No se puede pretender que un Estado que no es parte del Convenio de Budapest pueda participar y beneficiarse plenamente de esta cooperación, sino en la medida que satisface los intereses de los Estados que sí son parte del Convenio. Esta es una realidad ineludible, porque si en algún momento se aprueba esta iniciativa la cooperación internacional se hará en función de los intereses de los Estados Parte del Convenio, entre los cuales se beneficiaria directamente Guatemala.

En el Artículo 2 se establecen los bienes jurídicos tutelados: los datos personales y la intimidad informática; la indemnidad sexual de los menores de edad, la confidencialidad, la integridad y la disponibilidad de la información y datos contenidos en sistemas informáticos o sistemas que utilicen tecnologías de información y comunicación o transmitidos por medio de éstas, los bienes, activos y pasivos patrimoniales representados en las transacciones u operaciones comerciales o financieras que se realicen por medios informáticos.

Los delitos que se tipifican en esta iniciativa son básicamente los mismos que se establecen en el Convenio de Budapest, aunque en algunos la denominación cambia:

a) Acceso ilícito (Artículo 8);
b) Interceptación ilícita (Artículo 9);
c) Ataque a la integridad de los datos (Artículo 10);
d) Ataque a la integridad del sistema (Artículo 11);
e) Falsificación informática (Artículo 12);
f) Apropiación de identidad ajena (Artículo 13);
g) Abuso de dispositivos (Artículo 14);
h) Fraude informático (Artículo 15);
i) Pornografía infantil (Artículo 17);
j) Acoso por medios cibernéticos (Artículo 18);
k) Delito contra la integridad sexual de una menor de edad o contacto a menor de edad con fines sexuales a través de las Tics (Artículo 19). Todos de la incitativa citada.

En el Artículo 31 se regula el principio de la cooperación internacional. De la redacción de este artículo se deduce, que siendo Guatemala un Estado que no se ha adherido al Convenio de Budapest la misma resulta incongruente, toda vez en el artículo analizado se establece que la cooperación internacional está sujeta a lo que regulan tratados y convenios internacionales ratificados por Guatemala.

Resulta incongruente la redacción del artículo analizado porque en materia de ciberdelito el único Convenio existente es el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, que es el instrumento internacional que establece la cooperación en materia de ciberdelito. Por lo que Guatemala al no ser parte de este Convenio, no goza como ya se afirmó de los beneficios integrales de estará cooperación, sino solo en la medida de los intereses de los Estados Parte.

Ahora bien, en cuanto a las penas que se establecen, éstas varían de entre un (1) año hasta los ocho (8) años de prisión y multas que van desde doscientos salarios mínimos hasta setecientos salarios mínimos de las actividades no agrícolas. Aunque, cuanto más se tarde el Congreso de la República en aprobar esta iniciativa o cualquier otra sobre el ciberdelito, más complejo será poder adaptarlas a los inevitables cambios en el uso y desarrollo de las tecnologías de la información y comunicación, así como al desarrollo de las aplicaciones que se utilizan por medio de internet.

5.5. La hipótesis y su comprobación

El Estado de Guatemala no es ajeno a los ataques cibernéticos, como ya se dejó plenamente establecido, tomando en cuenta que la estructura informática de protección de datos e información sensible no ha alcanzado el grado de desarrollo, especialmente en las instituciones públicas, no así en las instituciones privadas que

se han dado cuenta del peligro de tener expuesta su información y demás dados en sus servidores.

El Convenio de Budapest del que se hace constante referencia, especialmente a partir del capítulo III de esta investigación y atendiendo al hecho de que Guatemala no es parte del mismo, resulta contraproducente la sola creación de la Estrategia Nacional de Seguridad Cibernetica sin el marco normativo que le de vida jurídica. Otro hecho probado plenamente en la presente investigación es que Guatemala en la actualidad, no está preparada legislativa ni técnicamente para la persecución, juzgamiento y sanción del castigo del ciberdelito, es decir, no existen tipificadas las diferentes conductas por las cuales se comete un ciberdelito.

Por consiguiente, la hipótesis planteada en la presente investigación se formuló de la siguiente manera. "Ninguna política nacional de seguridad cibernética puede ser efectivamente ejecutada o puesta en marcha si no existe el marco jurídico normativo correspondiente, tal y como ocurre actualmente en Guatemala, por lo que solo con la incorporación normativa del ciberdelito al ordenamiento penal se puede legitimar cualquier política de seguridad cibernética".

En este orden de ideas a lo largo de todos capítulos desarrollados en la presente investigación y los argumentos propuestos, se pude establecer plenamente la comprobación de la hipótesis en los términos que se formuló: primero: porque se establece que por sí sola ninguna política o estragegia nacional de seguridad

cibernética puede ser efectivamente ejecutada o puesta en marcha si no existe el marco jurídico normativo correspondiente; segundo: que la forma de legitimar cualquier política o estrategia de seguridad cibernética necesariamente tiene que contar previamente con un normativo especial que regule todo lo relativo al ciberdelito, asimismo se puede probar que actualmente Guatemala no cuenta con este marco normativo.

Finalmemte, se puede establecer que el Estado de Guatemala para legitimar la persecución penal de los ciberdelitos, es necesario e imperativo que exista un marco jurídico penal que tipifique y sanciones estas conductas que en la actualidad por virtud del principio de legalidad no son punibles. Esta situación de legalidad reduce la capacidad del Estado de Guatemala de estar a la altura frente al combate internacional de los ciberdelitos, de lo que se deduce que con estas condiciones de nada sirve contar con una Estrategía de Seguridad Cibernética, porque al final solo es decorativa.

5.6. Propuesta de incorporación normativa del ciberdelito a la legislación penal guatemalteca

Como ya se dejó plenamente establecido mediante la comprobación de la hipótesis, Guatemala no es parte del Convenio de Budapest, lo que por supuesto imposibilita al Estado a beneficiarse de la cooperación internacional directa, aunque esta situación en principio no impide incorporar a la legislación penal las directrices del Convenio, lo

que no significa ser parte. Por lo que es necesaria la incorporación del Estado de Guatemala a la adhesión del Convenio de Budapest.

El propósito de ser parte de este Convenio es precisamente unificar esfuerzos, por medio de la cooperación internacional, entre los Estados Parte en la lucha contra la ciberdelincuencia. Uno de los principios básicos del Convenio es precisamente intensificar la cooperación entre los Estados Parte en la lucha contra el ciberdelito.

Esta situación, es decir, que Guatemala no sea parte del Convenio de Budapest fortalece el argumento aquí planteado, en el sentido de que si bien en el año 2018 se publicó la estrategia nacional de seguridad cibernética, esta publicación se hizo sin un respaldo normativo adecuado (tipificación del ciberdelito).

Esto se suma al hecho de que Guatemala no es parte del Convenio limita al Estado a participar de dicha cooperación en el combate de la ciberdelincuencia, de tal forma, que uno de los primeros pasos y el más importante para la efectiva cooperación en materia de armonizar a la legislación penal el ciberdelito guatemalteco y que Guatemala se adhiera al Convenio de Budapest.

Junto a la adhesión de Guatemala al Convenio de Budapest y la armonización de la legislación penal, se tiene que crear un marco jurídico que regule todo lo relativo a la seguridad cibernética, a los comités de seguridad cibernética, a los actores, acciones, instituciones, alineaciones a los planes estratégicos institucionales, la

forma en qué se incluirá la estrategia de seguridad cirbernética a los planes operativos anuales del sector público y los convenio de monitoreo que se establezcan con la iniciativa privada.

Todos estos ejes están descritos en la estrategia de seguridad ciernetica, pero mientra no exista el marco jurídico normativo que aquí se propone solo quedarán en buenas intenciones. Fue contraproducente la publicación de la estrategia, porque en primer lugar ésta se público sin que Guatemala sea parte del Convenio, sin tener un marco normativo armonizado al Convenio y sin contar con el sustento legal que regule todos los ejes descritos en el párrafo anterior. Lo que se puede considerar como una suerte de desatino político, porque da la impresión que el Estado de Guatemala escogió el camino errado respecto al ciberdelito, porque la forma idónea y lógica de emprender el combate contra el ciberdelito, es en este orden: a) adherirse al Convenio Sobre la Ciberdelincuencia; b) armonizar la legislación penal sobre el ciberdelito al convenio, y c) crear una política pública contra el ciberdelito,.

Desafortunadamente para Guatemala, el primer paso que ha dado es incongruente porque según la estratificación anterior, el útlimo paso, que en poco o en nada ayuda a combatir la cibercriminalidad, fue comenzar con la publicación de la estrategia de seguridad cibernética, lo que solo crea más dudas que respuestas. Aunque un Estado que no es miembro puede unilateralmente incorporar a su propia legislación penal las directrices del Convenio de Budapest, esta unilateralidad no garantiza la

plena cooperación de los otros Estados Partes del convenio en todo lo referente al ciberdelito y la ciberdelincuencia.

5.7. Comentarios finales

El desarrollo de la informática en todos sus aspectos también ha favorecido a grupos criminales o individuos en lo particular a tener acceso a estas herramientas, con el fin de cometer actos delictivos utilizando para el efecto ordenadores, dispositivos electrónicos y sobre todo el acceso a internet.

Los Estados, hoy más que nunca necesitan de las herramientas digitales y jurídicas a fin de desarrollar procedimientos forenses digitales armonizados con el fin de estandarizar las leyes penales nacionales con la legislación internacional (Convenio de Budapest). Porque en la actualidad todas las actividades económicas, industriales y de servicios están globalizadas de forma digital, los Estados no pueden permanecer al margen de la lucha contra la ciberdelincuencia por lo que la mejor estrategia para Guatemala es la adhesión y ratificación del Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

Con la adhesión y la ratificación del Convenio Sobre la Ciberdelincuencia se logrará dar un primer paso en esta lucha, toda vez que el ciberdelito trasciende las fronteras nacionales, lo cual hace necesario que las legislaciones penales internas tipifiquen el ciberdelito de acuerdo a la clasificación que hace el Convenio. Esto proporcionará las

herramientas necesarias para el combate, persecución y enjuiciamiento de la ciberdelincuencia y al mismo tiempo implica una estrecha cooperación con el resto de Estados Parte del Convenio.

Guatemala, no siendo Parte del Convenio Sobre la Ciberdelincuencia, está rezagada respecto a los Estados que sí son parte del mismo. Esto limita la cooperación y al mismo tiempo facilita que grupos criminales o individuos en particular, ejecuten en el territorio guatemalteco un ciberdelito, sabiendo que éste no está tipificado y por tanto no es punible.

Esta situación necesariamente incrementa la percepción internacional en el sentido de que el Estado de Guatemala no hace los esfuerzos necesarios para adherirse y ratificar el Convenio Sobre la Ciberdelincuencia y aprobar una legislación penal sobre el ciberdelito. Dos elementos con los que Guatemala no cuenta en la actualidad, que afectan la seguridad jurídica sobre la adopción de todas aquellas medidas legislativas que tiendan la perseguir, juzgar y sancionar el ciberdelito. Asimismo, no garantiza el debido equilibrio de la acción penal y el respeto a los derechos humanos, tomando en cuenta que muchos de los cibercrímenes abiertamente se cometen violentando derechos fundamentales especialmente de la niñez y la adolescencia.

En este contexto, la publicación de la Estrategia Nacional de Seguridad Cibernética por sí sola no contribuye en nada al problema del cibercrimen, ni soluciona las deficiencias sobre seguridad cibernética, tal y como quedó establecido mediante la

comprobación de la hipótesis. Puesto que en esta materia (ciberseguridad), es el sector privado el ha tomado sus propias medidas a fin de garantizar la seguridad de todos aquellos datos y transacciones que utiliza redes informáticas e internet.

El Estado de Guatemala no ha aportado nada para combatir el ciberdelito no obstante existir una iniciativa de ley que pretende aprobar la lucha frontal contra ciberdelincuencia, que a propósito está engavetada en el Congreso de la República desde marzo del año 2017. De esta cuenta en la actualidad Guatemala no posee una ley penal que tipifique los ciberdelitos, lo que hace imposible perseguir, juzgar y sancionar estas conductas y al mismo tiempo contribuye a la impunidad de los ejecutores de estos delitos.

CONCLUSIONES

1) El ciberdelito por tener carácter transnacional, lo convierte en una preocupación a nivel global en que ningún Estado puede ni debe estar aislado, sino que al contrario es precisa la cooperación internacional. En Guatemala, solo se cuenta con la ley penal que no tipifica estos delitos, por lo que según el principio de legalidad, no puede haber persecución penal.

2) El Convenio Sobre la Ciberdelincuencia o Convenio de Budapest es el instrumento normativo internacional, cuyo fin es la armonización de las diferentes leyes penales de los Estados Parte, en el combate de la ciberdelincuencia.

3) Guatemala no es parte del Convenio Sobre la Ciberdelincuencia, lo que ha ocasionado el aislamiento frente a la comunidad internacional, especialmente frente a los Estados Parte de éste y sobre la cooperación en todo lo relativo al ciberdelito.

4) Guatemala, no cuenta con una ley especial sobre la ciberdelincuencia lo que significa que la comisión en territorio guatemalteco de un ciberdelito es impune, por virtud del principio de legalidad, porque no puede ser penado.

5) La inexistencia de una normativa especial sobre la ciberdelincuencia en Guatemala, coloca al Estado en una posición compleja frente a los Estados Parte del Convenio Sobre la Ciberdelincuencia y en un alto nivel de vulnerabilidad.

6) Guatemala desde el año 2018 cuenta con una política pública denominada Estrategia nacional de Seguridad Cibernética, que no está amparada con la debida legitimidad jurídica necesaria para ser puesta en marcha, lo que la hace totalmente inoperante.

7) De todo lo desarrollado en la presente investigación, de los argumentos propuestos se puedo confirmar plenamente la hipótesis planteada en el sentido de que no basta con la existencia de la Estrategia Nacional de Seguridad Cibernética para legitimar la persecución penal del ciberdelito sino no va acompañada del marco legal correspondiente, si esta no va acompañada del marco legal correspondiente que legitime.

RECOMENDACIONES

1) El Estado de Guatemala para no estar retirado en la lucha internacional contra el ciberdelito, es necesario que forme parte de la comunidad internacional en materia de combate al ciberdelito.

2) El Estado al no ser parte del Convenio sobre el Ciberdelito es importante y necesario actualize la normativa sobre penal en el sentido de que la lucha contra el ciberdelito se fortalezca, con lo cual también se enviará un mesaje positivo a la comunidad internacional por la disposición del Estado a conbatir el ciberdelito.

3) Que el Estado de Guatemala ante la posibilidad establecida en el Artículo 37 numeral 1, debe solicitar su adhesión al Convenio sobre la Ciberdelincuencia o Convenio de Budapest, por de esta forma podrá opatar a los beneficios de la cooperación internacional.

4) Si bien, un primer paso es reformar la legislación penal para incluir el ciberdelito, el Estado de Guatemala tiene que crear una ley especial sobre el ciberdelito, disponiendo para ello la incorporación de las figuras delictiva y su definición del Convenio sobre el Ciberdelito.

5) El Estado de Guatemala tiene que mejorar sus capacidades informáticas de protección de datos con el objeto de suplir en alguna medida la falta de una

legislación que persigua el ciberdilito, lo que mejorará la posición compleja del Estado frente a los a los Estados Parte del Convenio Sobre la Ciberdelincuencia y en un alto nivel de vulnerabilidad.

6) El Estado de Guatemala, para poder llevar a cabo y que sea operativa la Estrategia nacional de Seguridad Cibernética, tiene que crear el marco jurídico normativo y las instituciones especializadas para poner en marcha dicha polílica, porque ésta por sí sola es totalmente inoperante.

7) El Estado de Guatemala, a través del Congreso de la República de Guatemala, debe regular en el Código Penal, los delitos informáticos que se realicen por medio de internet, para limitar las acciones cometidas por los delincuentes informáticos en la sociedad.

BIBLIOGRAFÍA

ANDRADE RENDÓN, Rosa Elena. **Teoría y método de Cesar Lombroso en el hombre delincuente**. Tesis de Grado Maestría, Instituto Tecnológico Nacional, Secretaría de Investigación y Posgrado. Ciudad de México: (s.e.), 2016.

ANTINORI, Eduardo. **Conceptos básicos del derecho**. 1ra. ed. Mendoza: Universidad del Aconcagua, 2006.

BACIGALUPO, Enrique. **Manual de derecho penal: Parte General**. 3ra. reimpresión. Santa Fe de Bogotá, Colombia: Ed. Temis, S. A, 1996.

DI PIETRO, Alfredo y Ángel Enrique Lapieza Elli. **Manual de derecho romano**. 4ta. ed. Argentina: Ed. Buenos Aires, 1982.

FONTAN BALESTRA, Carlos. **Derecho penal: introducción y parte general**. Buenos Aires, Argentina: Ed. Abeledo-Perrot, 1998.

FUNDACIÓN TELEFÓNICA. **Ciberseguridad, la protección de la información en un mundo digital**. 1ra. ed. España: Ed. Ariel, 2016.

GALÁN MUÑOZ, Alfonso. **Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática**. Revista de Derecho Penal y Procesal, No. 15, España, 2006.

GARCÍA MÁYNEZ, Eduardo. **Introducción al estudio del derecho**. 53ra. ed. México: Ed. Porrua, 2002.

GIRÓN PALLARES, José Gustavo. **Teoría del delito**. 2da. ed. Guatemala: Ministerio Público, 2013.

GONZÁLEZ, Cauhapé-Cazaux. **Apuntes de derecho penal guatemalteco: La teoría del delito**. 2da. ed. Guatemala: Fundación Mirna Mack, 2003.

HAUCK, Joao R. **Tecnología, vigilancia y sistema penal: La superación de paradigmas y las nuevas perspectivas bajo el punto de vista tecnológico.** Revista Lecciones y Ensayos No. 86, Buenos Aires, 2009.

HURTADO POZO, José. **Manual de derecho penal**. 2da. ed. Lima: Ed. Eddili, 1987.

LIMA, María de la Luz. **Delitos electrónicos**. Revista Criminalia, Academia Mexicana de Ciencias Penales. Porrúa, No. 1-6. Año L, enero-junio, México: 1984.

LOREDO GONZÁLEZ, Jesús Alberto y Aurelio Ramírez Granados. **Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo**. Facultad de Ciencias Físico Matemáticas, Universidad de Nuevo León. México: 2013.

MACGREGOR B., Rafael Fernández (coordinador). **Perspectiva de ciberseguridad en México**. México: Ed. McKinsey & Company, 2018.

MARIACA, Margot. **Introducción al derecho penal**. Facultad de Ciencias Jurídicas y Políticas, Universidad San Francisco Xavier. Bolivia, 2010.

MATEOS PASCUAL, Pedro. **Ciberdelincuencia: Desarrollo y persecución tecnológica**. Escuela Universitaria de Ingeniería Técnica y Telecomunicación, Universidad Politécnica de Madrid. España, 2014.

MEDINA CUENCA, Arne. **Los principios limitativos del ius puniendi y las alternativas a las penas privativas de libertad**. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., núm. 19, págs. 87-116, 2007.

MINISTERIO DE GOBERNACIÓN (Guatemala). **Estrategia nacional de seguridad cibernética**. Guatemala: Ministerio de Gobernación, 2018.

MINISTERIO DE GOBERNACIÓN (Guatemala). **Plan operativo institucional 2016-2020**. Guatemala: Ministerio de Gobernación, 2016.

MIR PUIG, Santiago. **Función de la pena y teoría del delito en el Estado democrático de derecho**. 2da. ed. Barcelona: Ed. Bosch, Casa Editorial, S. A., 1982.

MUÑOZ CONDE, Francisco. **Derecho penal y control social**. España: Ed. Gráficas del Exportador, 1985.

NIEVES, Ricardo. **Teoría del delito y práctica penal. Reflexiones dogmáticas y mirada crítica**. República Dominicana: Ed. Centenario, S. A., 2010.

OBSERVATORIO DE LA SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE. **Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?** Nueva York: Organización de los Estados Americanos, 2016.

ORTIZ PRADILLO, Juan Carlos. **Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos**. España: Universidad de Castilla la Mancha, 2016.

ORTS BERENGUER, Enrique y José L. González Cussac. **Manual de derecho penal, parte general**. Nicaragua: USAID, 2014.

PACHECO MANDUJANO, Luis Alberto. **Teoría del delito**. Perú: Ed. Iquitos, 2013.

PEÑA GONZÁLES, Oscar y Frank Almanza Altamirano. **Teoría del delito: Manual práctico para su aplicación en la teoría del caso**. Perú: Ed. Nomos & Thesis E.I.R.L., 2010.

POLITOFF L., Sergio y Jean Pierre Matus A., María Cecilia Ramírez. **Lecciones de derecho penal chileno; Parte general**. Santiago de Chile: Ed. Jurídica de Chile, 2003,

POSADA MAYA, Ricardo. **El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual**. Revista Nuevo Foro Penal Vol. 13, No. 88, enero-junio 2017, pp. 72-112. Universidad EAFIT, Medellín, Bogotá: 2017.

ROJAS CHACÓN, José Alberto y Cecilia Sánchez Romero. **Teoría del delito aspectos teóricos y prácticos**. Tomo I. Costa Rica: Unidad de Capacitación y Supervisión, Ministerio Público de Costa Rica, (s.f.).

SAIN, Gustavo. **La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal. En Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet**. Buenos Aires: Ed. Erreius, 2018.

SERRANO PIEDECASAS FERNÁNDEZ, José Ramón y Juan María Terradillos Basoco. **Manual de teoría jurídica del delito**. 1ra. ed. El Salvador: Consejo Nacional de la Judicatura, Escuela de Capacitación Judicial, 2003.

TEMPERINI, Marcelo. **Delitos informático y cibercrimen: alcances, conceptos y características. En cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet**. Buenos Aires: Ed. Erreius, 2018.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. **El ciberdelito: Guía para los países en desarrollo**. Ginebra, Suiza: División de Aplicaciones TIC y Ciberseguridad Departamento de Políticas y Estrategias Sector de Desarrollo de las Telecomunicaciones de la UIT, 2009.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. **Guía de ciberseguridad para los países en desarrollo**. Ginebra, Suiza: (s.e.), 2007.

ZAFFARONI, Eugenio Raúl. **Trabado de derecho penal, parte general**. Tomo I. Buenos Aires: Ed. Ediar, 1998.

ZAFFARONI, Eugenio Raúl. **Tratado de derecho penal, parte general**. Tomo II. Buenos Aires: Ed. Ediar, 1998.

ZAFFARONI, Eugenio Raúl. **Tratado de derecho penal, parte general**. Tomo III. Buenos Aires: Ed. Ediar, 1998.

ZAFFARONI, Eugenio Raúl. **Tratado de derecho penal. Parte general**. Tomo IV. Buenos Aires: Ed. Ediar, 1998.

ZAFFARONI, Eugenio Raúl. **Tratado de derecho penal: Parte General**. Tomo V. Buenos Aires: Ed. Ediar, 1998.

E-grafías:

ACURIO DEL PINO, Santiago. **Delitos informáticos: generalidades**. https://www.oas.org/juridico/spanish/ cyb ecu delitos inform.pdf . Extraido el 28 de marzo de 2019.

CASTELLANOS, Fernando. **Lineamientos elementales de derecho penal**. http://cdigital.dgb.uanl.mx/te/1020124909/1020124909_02.pdf Extrapido el 17 de marzo de 2019.

DÍAZ GÓMEZ, Andrés. **El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. Especial consideración a España y Argentina**. http://www.cienciared.com.ar/ra/usr/3/1115/hologramatica_n14_v4pp27_86.pdf Extrapido el 12 de abril de 2019.

LANDAVERDI, Moris. **La causalidad en el derecho**. https://enfoquejuridico.org/2015/11/10/la-causalidad-en-derecho-penal/ . Extraído el 1 de abril de 2019.

MORENO HERNÁNDEZ, Moisés. **Principios rectores en el derecho penal mexicano**. http://biblio.juridicas.unam.mx/libros/1/117/26.pdf. Extraido el 17 de octubre de 2016.

REAL ACADEMINA ESPAÑOLA DE LA LENGUA. https://dle.rae.es/?id=IYZhVtl. Extraído el 28 de marzo de 2019.

Legislación:

Asamblea Nacional Constituyente. **Constitución Política de la República de Guatemala**. 1985. Guatemala.

Consejo de Europa. **Convenio Sobre la Ciberdelincuencia**. 2001.

Asamblea General de las Naciones. **Convención Sobre los Derechos del Niño**. 1989.

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

Congreso de la República de Guatemala, **Ley Reguladora del Procedimiento de Extradición**, Decreto número 28-2008. Guatemala. 2008.

Iniciativa de ley, 2017, **Ley Contra la Ciberdelincuencia**, 2017.