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

ENFOQUE JURÍDICO DEL INCUMPLIMIENTO DEL ESTADO AL NO ADOPTAR EL CONVENIO DE BUDAPEST QUE ESTABLECE LOS DELITOS SOBRE CIBERDELINCUENCIA EN EL DERECHO PENAL

SHARON LORENA FRANCO DE LEÓN

GUATEMALA, NOVIEMBRE 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ENFOQUE JURÍDICO DEL INCUMPLIMIENTO DEL ESTADO AL NO ADOPTAR EL CONVENIO DE BUDAPEST QUE ESTABLECE LOS DELITOS SOBRE CIBERDELINCUENCIA EN EL DERECHO PENAL

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

SHARON LORENA FRANCO DE LEÓN

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, noviembre 2024

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

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

TRIBUNAL QUE PRÁCTICÓ
EL EXÁMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Licda. Gregoria Sánchez
Vocal:	Licda. Candi Claudy Vaneza Gramajo Izeppi
Secretario:	Lic. Josué Adán Figueroa

Segunda Fase:

Presidente:	Licda. Jennifer Isabel Soliz Revolorio
Vocal:	Lic. Miguel Estuardo Pascual Bonachea
Secretario:	Lic. Domingo Alfredo Ajcu Toc

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
N-006
GUATEMALA, C. A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 21 de noviembre de 2022

Atentamente pase al (a) Profesional, **DIXON DIAZ MENDOZA,** para que proceda a asesorar el trabajo de tesis del (a) estudiante **SHARON LORENA FRANCO DE LEÓN,** con carné 201502260 intitulado: **ENFOQUE JURÍDICO DEL INCUMPLIMIENTO DEL ESTADO AL NO ADOPTAR EL CONVENIO DE BUDAPEST QUE ESTABLECE LOS DELITOS SOBRE CIBERDELINCUENCIA EN EL DERECHO PENAL.**

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

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

Adjunto encontrará el plan de tesis respectivo.

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

CARLOS EBERTITO HERRERA RECINOS
Jefe (a) de la Unidad de Asesoría de Tesis

SAQO

Fecha de recepción 24 / 11 / 2022. (f) _____
Asesor(a)
(Firma y sello)

LIC. DIXON DIAZ MENDOZA
ABOGADO Y NOTARIO

Bufete Jurídico
Lic. Dixon Díaz Mendoza

Guatemala, 28 de febrero de 2023

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

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

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
15 ENE 2024
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Respetable Jefe de la Unidad de Tesis:

En cumplimiento a la resolución de fecha veintiuno de noviembre del año dos mil veintidós, en la que se me designó como asesor de la bachiller **Sharon Lorena Franco De León** con carné **201502260** quien realizó el trabajo de Tesis intitulado como: **"ENFOQUE JURÍDICO DEL INCUMPLIMIENTO DEL ESTADO AL NO ADOPTAR EL CONVENIO DE BUDAPEST QUE ESTABLECE LOS DELITOS SOBRE CIBERDELINCUENCIA EN EL DERECHO PENAL".** Por lo que resulta procedente dictaminar respecto a la asesoría del trabajo académico de investigación de conformidad con las siguientes justificaciones:

a. Del análisis efectuado al contenido, objeto de desarrollo, aportaciones y teorías sustentadas por la autora, se advierte que se calificó de sustento importante al momento de la asesoría efectuada, toda vez que el contenido científico que estriba de la presente tesis es referente a la falta de regulación y a la inobservancia del Estado de Guatemala de incorporar al ordenamiento jurídico legal vigente los delitos contenidos en el Convenio sobre la Ciberdelincuencia, los efectos jurídicos y las posibles soluciones al problema objeto de estudio, siendo un tema importante dentro del área del derecho penal y derecho internacional público al generar un análisis jurídico con aportes novedosos que buscan la regulación, aplicación, interpretación e integración de los delitos que se cometen en el ámbito del ciberespacio, enfocando en todo momento de forma técnica para obtener un resultado.

b. Al darle lectura al trabajo de tesis se percibe que la metodología de investigación aplicada por la autora fue basada en el método deductivo e inductivo, al estudiar las instituciones jurídicas relacionadas al tema partiendo de lo general a lo particular, permitiendo producción de conocimiento y obtención de criterio válidos. Se utilizó asimismo, el método analítico y sintético, utilizando la técnica de la investigación documental recopilando diversa información del tema, antecedentes y fundamento así como la

• 7a. Avenida 3-33, Zona 9 Oficina 502 Edificio Torre Empresarial 5to. Nivel • Teléfonos: 2362-1618, 2362-1619, 2362-1621 y 2362-1628
• Fax: 2362-1631 • Celular: 5204-8821 Correo Electrónico: didiazmendoza@hotmail.com

técnica bibliográfica para la recolección de datos de una forma adecuada y conforme el plan de investigación obteniendo la información que enriqueció el contenido.

c. La redacción utilizada por la autora en el desarrollo de la tesis ha sido apropiada en virtud que siempre se observó en un mismo sentido guardando la correlación en cada capítulo, empleando lenguaje eminentemente técnico y jurídico aportando la estudiante ideas y opiniones que fortalecieron el contenido de la investigación.

d. Con la investigación realizada existe contribución al derecho penal, pues el objetivo a investigar es la inobservancia del estado en integrar los delitos que están contenidos en el Convenio estudiado tomando en consideración los avances de la sociedad guatemalteca así como de las tecnologías de la información.

e. Como producto final de la investigación la estudiante elaboró la conclusión discursiva identificando cuales son los problemas concretos y consecuencias de la falta de aplicación, integración e interpretación de los delitos que se realizan en el mundo del ciberespacio, siendo transnacionales y traspasando sus consecuencias jurídicas al mundo real.

En atención a cada uno de las literales expuestas, y que no poseo con la estudiante parentesco alguno dentro de los grados de ley, a mi consideración el trabajo de investigación de la bachiller **SHARON LORENA FRANCO DE LEÓN,** llena los requisitos establecidos en el Normativo para la Elaboración de Tesis de la Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Público, cumpliendo satisfactoriamente con los requisitos contenidos en el artículo treinta y uno (31) de dicho normativo, a la investigación se formularon algunas recomendaciones por lo que habiendo observado en cada una de las revisiones las correcciones emitidas por mi persona, confiero **DICTAMEN FAVORABLE DEL PRESENTE TRABAJO DE TESIS.**

Sin otro particular, me suscribo de usted atentamente

Lic. Dixon Díaz Mendoza

Abogado y Notario

Colegiado 5084

LIC. DIXON DIAZ MENDOZA
ABOGADO Y NOTARIO

• 7a. Avenida 3-33, Zona 9 Oficina 502 Edificio Torre Empresarial 5to. Nivel • Teléfonos: 2362-1618, 2362-1619, 2362-1621 y 2362-1628
• Fax: 2362-1631 • Celular: 5204-8821 Correo Electrónico: didiazmendoza@hotmail.com

D.ORD. 714-2024

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

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **SHARON LORENA FRANCO DE LEÓN,** titulado **ENFOQUE JURÍDICO DEL INCUMPLIMIENTO DEL ESTADO AL NO ADOPTAR EL CONVENIO DE BUDAPEST QUE ESTABLECE LOS DELITOS SOBRE CIBERDELINCUENCIA EN EL DERECHO PENAL.** Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

HMAC/JIMR

DEDICATORIA

DIOS: Por llenarme de fortaleza y perseverancia para concluir cada una de mis metas.

A MIS PADRES: Por todo el amor y apoyo brindado a lo largo de mi vida y en cada una de las etapas de mis estudios y llevarme de la mano para encontrar mi camino profesional.

A MI FAMILIA: Gracias por su amor y por enseñarme a nunca rendirme ante los obstáculos de la vida.

A MIS AMIGOS: Por brindarme siempre apoyo y cariño incondicional en cada una de mis etapas, pero sobre todo por todas esas tardes compartidas en la cafetería, por las veces que estudiábamos antes de examen compartiendo materiales, por las clases de pres, preu, por los logros compartidos, gracias por siempre estar presentes.

A: La Tricentenaria Universidad de San Carlos de Guatemala, gloriosa casa de estudios que ha colmado mi espíritu de sabiduría.

A: La Facultad de Ciencias Jurídicas y Sociales, porque en sus aulas encontré la amistad y aprendizaje para culminar esta meta,

PRESENTACIÓN

La investigación es de tipo cualitativa, el estudio pertenece a la rama cognitiva del derecho penal guatemalteco y también del derecho internacional público, el sujeto de la presente investigación es el Convenio sobre la Ciberdelincuencia y su carácter de norma vinculante ante las naciones signatarias que por medio de la cooperación internacional buscan unificar delitos y sanciones para proteger a los ciudadanos de los flagelos que se dan en el mundo digital siendo la presente un análisis de derecho comparado.

La naturaleza jurídica o su rama cognoscitiva de la ciencia del derecho a la que pertenece no puede encuadrarse únicamente al derecho penal pues se hace una integración normativa ya que se estudió el derecho internacional público y el derecho penal guatemalteco. El contenido de sus argumentaciones y conclusión discursiva pertenecen al ámbito del derecho penal guatemalteco. El ámbito espacial abarcado es el territorio de la República de Guatemala siendo la población guatemalteca el público a interesar y su temporalidad se encuadra dentro del período comprendido de noviembre 2001 a la fecha.

La tesis ofrece como aporte académico el estudio de la normativa tanto nacional como internacional que protege los derechos de los ciudadanos de una población ante los flagelos que se cometen en el mundo digital, un delito de tipo transnacional pues con la facilidad de acceso al internet cualquier persona en cualquier parte del mundo puede realizar actos ilícitos por medio del anonimato de forma instantánea realizándose en el ciberespacio pero sus consecuencias se materializan en el mundo real.

Siendo que el convenio objeto de estudio es de carácter vinculante ante la comunidad internacional en materia penal que busca por medio de la cooperación internacional unificar u homogeneizar los tipos delictivos más frecuentes que se suscitan en el ciberespacio así como los mecanismos a implementar para sancionarlos son motivos por los que se ha convertido en una norma de carácter internacional importante de estudiar.

HIPÓTESIS

El Estado de Guatemala a pesar de encontrarse sufriendo flagelos a través del uso de las tecnologías de la información y de formar parte de los países observadores del Convenio sobre la Ciberdelincuencia no ha adoptado o legislado para crear algún tipo penal o mecanismo para sancionar los hechos delictivos que se realicen en la esfera del mundo digital dejando a la población guatemalteca sin una tutela judicial efectiva, acceso a la justicia y restitución a sus derechos en el supuesto de ser vulnerados, lo que genera en los ciudadanos guatemaltecos un estado de indefensión por el vacío legal existente.

COMPROBACIÓN DE HIPÓTESIS

La hipótesis de la presente investigación utilizó el método analítico y deductivo toda vez que permitió conocer los principios, características y garantías propias al derecho penal moderno, así como los principios que se deben atender en el Derecho Internacional Público, tomando en consideración también los principios jurídicos fundamentales del derecho para poder de este modo realizar el análisis correspondiente.

A este efecto se utilizó la técnica de investigación documental, puesto que se recopiló y seleccionó la información a través de la lectura de documentos, libros, revistas, periódicos, notas de sitios electrónicos, investigaciones practicadas por universidades de otros países de América Latina y demás países signatarios del Convenio objeto de estudio. Asimismo, el método del marco lógico permitió encontrar el objetivo de la presente investigación siendo la premisa principal que Guatemala ha incumplido o inobservado adoptar dentro de su cuerpo legal los delitos y sanciones contenidas en el Convenio sobre la Ciberdelincuencia.

La hipótesis ha sido comprobada con base en las investigaciones realizadas a los avances que Guatemala ha tenido en el tema de seguridad en el ciberespacio para proteger los derechos de los habitantes del país en cuánto a los flagelos sufridos en el ciberespacio para lo que se empleó la técnica de investigación documental y se pudo establecer que efectivamente a la fecha el estado de Guatemala no ha incorporado legislación alguna a su ordenamiento jurídico que regule los delitos y sanciones contenidas en el Convenio objeto de estudio, lo que deja en estado de indefensión a los ciudadanos de guatemaltecos al momento de sufrir vulneraciones de este tipo.

ÍNDICE

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

INTRODUCCIÓN

La investigación realizada versa sobre la necesidad que el Estado de Guatemala en cumplimiento al mandato constitucional contenido en el Artículo 1 de la Constitución Política de la República de Guatemala cumpla con velar por la protección de los derechos inherentes a cada ciudadano guatemalteco, incorporando a la legislación nacional los delitos y las sanciones contenidas en el Convenio sobre la Ciberdelincuencia, firmado en Budapest Hungría en el año 2001, en virtud que al existir el vacío legal o la ausencia de una norma que restituya los derechos conculcados a los ciudadanos en el ciberespacio se les deja en un estado de indefensión ante estos flagelos.

Tiene como enfoque jurídico el incumplimiento del Estado de Guatemala al legislar sobre la integración de los ciberdelitos dejando a sus habitantes a la deriva en cuanto a la restitución de los derechos vulnerados siendo esto una responsabilidad del Estado, y en virtud de lo investigado se arriba a la conclusión que los objetivos propuestos han sido alcanzados pues se estudió el derecho penal guatemalteco y el derecho internacional público, y en específico el Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

De lo anterior se puede colegir que la hipótesis planteada fue comprobada, pues resulta evidente señalar que las sociedades han evolucionado, por lo que como usuarios de las tecnologías de la información se necesitan nuevas herramientas para comprender adecuadamente esta era y para que los derechos de cada uno de los ciudadanos se encuentren debidamente protegidos, situación en la que actualmente nos encontramos con un vacío legal por el incumplimiento del Estado al integrar los delitos del citado convenio.

De tal forma que el primer capítulo versa sobre qué es el derecho penal y sus aspectos generales pero a la vez importantes para entender cómo funciona esta ciencia del derecho, en el segundo se aborda lo relativo al delito, tema que dará la pauta para

introducir el delito cibernético, el tercero versa sobre la ciberdelincuencia en otros países dónde se realiza un análisis de derecho comparado, el cuarto introduce al tema objeto de estudio y el quinto desarrolla específicamente el objeto de estudio.

Las tecnologías de la información han protagonizado transformaciones sin precedentes, internet no es solo una herramienta, con el desarrollo de mayor tecnología y conocimientos también se abre la brecha para el uso perverso infligiendo daños de diversa índole, constituirá pues este trabajo un aporte a la medida que su lectura propicie la reflexión sobre el problema, pues solo cuestionando la realidad se contribuye a buscar mejores respuestas o soluciones a la problemática objeto de estudio.

Desde el punto de vista jurídico se establece que es una problemática que llevado a que las grandes naciones de la comunidad internacional a reunirse para discutir sobre el problema y plantear posibles soluciones, lo que conllevó a la promulgación del Convenio sobre la Ciberdelincuencia, en Budapest Hungría, buscando unificar delitos y sanciones en la comunidad internacional para facilitar la persecución y castigo del ilícito cometido. En la presente investigación, se utilizó la técnica de la investigación documental en conjunto con el método analítico deductivo, aplicando el razonamiento iniciando por los conocimientos generales hasta llegar a lo particular.

Por la investigación realizada, se arriba a la conclusión que se alcanzó el objetivo general del presente trabajo al determinarse mediante el derecho comparado y siendo una investigación de tipo cualitativa, determinando su tiempo desde 2001 que se dio la creación del Convenio sobre la Ciberdelincuencia siendo hasta el momento la norma internacional más completa con un marco jurídico integral y coherente en contra del ciberdelito y la evidencia electrónica que, el Estado de Guatemala ha estado inobservante al Convenio, sin crear un cuerpo legal que adopte o tipifique los flagelos cibernéticos, sanciones y los mecanismos a seguir para la restitución de los derechos conculcados dejando a los guatemaltecos sin una tutela judicial efectiva.

CAPÍTULO I

1. Derecho Penal

Derecho Penal es una ciencia del derecho perteneciente al área del derecho público toda vez que el Estado interviene activamente en la solución de conflictos buscando preservar el orden y la paz pública en una sociedad, así como rehabilitar a las personas que han infringido las normas del andamiaje jurídico propio a ese Estado.

A lo largo de la historia, el derecho penal ha evolucionado en respuesta a los desafíos cambiantes de la sociedad y ha sido moldeado por una variedad de influencias culturales, políticas y también filosóficas, teniendo raíces profundas que se remontan a las antiguas civilizaciones lo que sin duda alguna debe ser estudiado para poder llegar a una definición sobre que es el derecho penal, su naturaleza, características y estructura.

1.1. Definición de Derecho Penal

Los orígenes del derecho penal se remontan a los tiempos primitivos y su concepto ha ido evolucionando a través de la historia, pasando por marcadas etapas como lo fue en el Derecho Romano, la Edad Media, la evolución del derecho penal como una ciencia hasta llegar a la evolución de las escuelas distintivas del derecho penal, todo esto permitió tener la conceptualización actual.

En la actualidad gracias a la historia y la evolución de las diferentes etapas que atravesó la ciencia del derecho y las sociedades del mundo, se puede definir el derecho penal desde distintas perspectivas, siendo las principales las siguientes:

a. Desde el punto de vista subjetivo o *Ius Puniendi:* Es la facultad de castigar que tiene el Estado como único ente soberano, es el derecho del Estado a determinar los

delitos, señalar, imponer y ejecutar las penas correspondientes o las medidas de seguridad en su caso, la potestad de penar no es un simple derecho, sino un atributo de la soberanía estatal, ya que es al Estado con exclusividad a quien corresponde esta tarea, ninguna persona individual o jurídica, puede arrogarse dicha actividad que viene a ser un monopolio de la soberanía de los Estados.

b. Desde el punto de vista o *Ius Poenale*: Es el conjunto de normas jurídico-penales que regulan la actividad punitiva del Estado, que determinan en abstracto los delitos, las penas y las medidas de seguridad, actuando a su vez como un dispositivo legal que limita la facultad de castigar del Estado a través del principio de legalidad, de defensa o de reversa que contiene el Código Penal de Guatemala en su Artículo uno y que se complementa con el Artículo siete del mismo código.

El Diccionario Panhispánico del Español de la Real Academia Española define el derecho penal como: "Rama del Derecho que estudia las normas penales, las conductas que las infringen y la imposición de penas o sanciones aplicables a los autores de delitos y faltas"[1].

Muchos conceptos o definiciones se dan en doctrina sobre lo que constituye el derecho penal, el autor argentino Eugenio Raúl Zaffaroni por su parte lo describe indicando que se puede afirmar que el derecho penal es la rama del saber jurídico que, mediante la interpretación de las leyes penales propone a los jueces un sistema orientador de las decisiones que contiene y reduce el poder punitivo para impulsar el progreso del estado constitucional de derecho.

Se puede concluir que el derecho penal es una de las ramas del derecho público el cual establece y regula las penas de delitos y/o crímenes con el propósito de mantener a la sociedad protegida. El derecho penal se compone de una serie de normas jurídicas

[1] https://dpej.rae.es Diccionario Panhispánico del Español Jurídico. **Derecho Penal.** (Consultado: 2 de julio de 2023).

mediante las que el Estado puede definir las conductas u omisiones que se consideran delitos.

1.2. Naturaleza jurídica del Derecho Penal

Naturaleza jurídica se refiere a las características, la connotación o los elementos esenciales y de existencia de determinada área del derecho o institución jurídica. Se define la Naturaleza como "la esencia de un ser, es un conjunto de todo lo existente"[2].

El carácter o naturaleza jurídica del derecho penal se debe de entender en un principio que "tiene una función de protección, esta implica que el derecho penal conlleva la tutela de bienes jurídicos ante posibles o eventuales afectaciones susceptibles de conmover el sentimiento de seguridad jurídica de los habitantes de la Nación"[3].

Uno de los conceptos a tener en cuenta como objeto de estudio para entender la naturaleza jurídica del derecho penal es el de derecho público, concepto que en su acepción el Diccionario Panhispánico del Español Jurídico lo define de la siguiente manera: "Parte del ordenamiento que regula la organización y funcionamiento de las instituciones y órganos políticos y administrativos, así como las relaciones entre el poder público y los ciudadanos. Forman parte del derecho público disciplinas como el derecho constitucional, el derecho administrativo, el derecho procesal, el derecho penal o derecho financiero"[4].

Lo anterior expuesto permite colegir que el carácter o naturaleza jurídica del derecho penal es eminentemente público toda vez que el Estado interviene activamente en la

---

[2] Cabanellas, Guillermo. **Diccionario Enciclopédico de Derecho Usual.** Pág. 516.
[3] Zaffaroni, Eugenio Raúl. **Tratado de derecho penal. Parte General.** Pág. 24.
[4] https://dpej.rae.es/lema/derecho-público Diccionario Panhispánico del Español Jurídico. **Derecho Público** (Consultado:15 de julio de 2023).

solución de conflictos buscando preservar el orden y la paz pública, y como derecho público reconoce implícitamente la facultad que tiene el Estado de incriminar a los individuos por las posibles conductas de transgresión o afectación que pudieran dirigir contra los bienes jurídicos tutelados por el Estado.

El Estado de derecho supone el reconocimiento que todos los ciudadanos de una nación son iguales ante la ley siendo esto uno de los derechos inherentes a su persona, asimismo que es obligación o deber del Estado garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona, ello se encuentra materializado en la norma suprema del ordenamiento jurídico guatemalteco siendo la Constitución Política de la República de Guatemala.

"El derecho penal debe ser concebido como un límite al poder punitivo y no como una herramienta habilitante al poder punitivo del Estado"[5]. Otros tratadistas han indicado que la naturaleza jurídica del derecho penal constituye o se incluye dentro del ámbito del derecho público tendiendo a proteger intereses individuales y colectivos, públicos o sociales, a través de la facultad sancionadora del Estado, lo que genera una relación directa entre el infractor y el Estado.

1.3. Contenido del Derecho Penal

Es importante resaltar que el derecho penal al estudiar las conductas que se encuentran plasmadas en la legislación identificadas o tipificadas como ilícitas, que generan una responsabilidad y consecuencia de afectación ante los bienes jurídicos tutelados de otra persona, lo que genera también es una responsabilidad ante el Estado de legislar a favor de la protección de los bienes jurídicos de las personas, así como del castigo o sanción interpuesta al responsable de esta vulneración. La mayoría de tratadistas han coincidido

[5] Silvestroni, Mariano. **Teoría constitucional del delito.** Pág. 90.

en indicar que el derecho Penal tiene relación con otras disciplinas jurídicas, si bien el derecho penal es un todo tiene relación con:

a. Derecho Constitucional, toda vez que el derecho penal como cualquier institución en un Estado de Derecho debe tener su fundamento en la Constitución Política de la República que señala generalmente las bases y establece las garantías a que debe sujetarse el derecho penal.
b. Derecho Civil, en virtud que ambos tienden a regular las relaciones de los hombres en la vida social y a proteger sus intereses, estableciendo sanciones para asegurar su respeto, las que se encuentran contenidas en el derecho civil son sanciones de carácter reparatorio, y la sanción penal a diferencia es retributiva atendiendo a la magnitud del daño causado y la peligrosidad social del sujeto.
c. Derecho Internacional, toda vez que en la actualidad las naciones se han unido como comunidad internacional volviéndose popular el concepto de "cooperación internacional" facilitándose la comunicación entre los diferentes países y asimismo las crecientes relaciones internacionales son propicias para la comisión de delitos que revisten características de tipo internacional lo que hace indispensable una acción en conjunto de los Estados que forman la comunidad internacional para la prevención y sanción de los delitos.
d. Derecho Comparado esto en virtud que el Derecho Comparado es el estudio, análisis y comparación de las legislaciones de diversos países lo que forma la comunidad internacional actualmente que se ha convertido en un medio importante para realizar reformas a la legislación penal de los países, adoptando las leyes o instituciones que mayor éxito han alcanzado en la lucha contra la criminalidad.

En el mismo sentido es importante hacer mención que tanto el contenido del derecho penal son las otras áreas de la ciencia del derecho que lo complementan para entender su finalidad, así como también es objeto de estudio de este apartado las fuentes de las que emana el derecho, en el entendido que es dónde se produce la norma jurídica y que en el derecho penal es necesario mencionar las siguientes:

A. La Ley: De conformidad con lo establecido por el Artículo 2 de la Ley del Organismo Judicial, la Ley es la fuente del ordenamiento jurídico y la jurisprudencia la complementará. La ley es la única fuente del derecho penal por excelencia, de la cual emana el poder para la creación de normas, su aplicación y sus sanciones. Es la fuente directa del derecho penal.
B. La Costumbre: En el estudio del Derecho la costumbre "es la norma habitualmente no expresada por escrito, que resulta de las prácticas reiteradas y generalmente asumidas por la mayoría de los que están en un lugar o participan en determinada situación"[6].
C. La Jurisprudencia: El Diccionario Panhispánico del Español Jurídico define la jurisprudencia como la doctrina establecida de forma reiterada por el Tribunal Supremo o el Tribunal Constitucional al interpretar la Constitución y las leyes, es la dogmática jurídica. La Jurisprudencia es la reiteración de decisiones sobre un mismo asunto de forma similar.
D. La Doctrina: "Es la opinión sostenida en las obras de juristas de reconocido prestigio, la interpretación que los jueces y funcionarios públicos realizan de las leyes en su aplicación a los casos particulares y en los negocios administrativos"[7].
E. Los principios Generales del Derecho: Es necesario primeramente definir que un principio según el Diccionario Panhispánico del Español Jurídico es un axioma que plasma una determinada valoración de justicia constituida por la doctrina o aforismos que gozan de general y constante aceptación. Son un medio o mecanismo de interpretación, sirven de herramientas para interpretar la ley y para interpretar las normas jurídico penales.

1.4. Principios Informadores del Derecho Penal

Un principio puede ser definido como aquella norma o idea fundamental que rige un pensamiento o conducta. En el caso del derecho penal existen principios delimitadores

[6] https://dpej.rae.es/lema/costumbre Diccionario Panhispánico del Español Jurídico. **Costumbre.** (Consultado: 15 de julio de 2023).
[7] https://dpej.rae.es/lema/doctrina Diccionario Panhispánico del Español Jurídico. **Doctrina.** (Consultado: 15 de julio de 2023).

o informadores que imponen barreras al ius puniendi, es decir la facultad punitiva del Estado para castigar las conductas que son consideradas ante las diferentes sociedades o constructos sociales como ilícitas.

Por las razones anteriores, en un Estado de Derecho, el Derecho Penal necesita principios o directrices que indiquen el camino a seguir y que limiten la potestad punitiva del Estado para evitar los males que puede causar el actuar de un hecho. Según el estudio de la ciencia del derecho penal, los diferentes tratadistas concuerdan que tiene como principios informadores los siguientes[8]:

1.4.1 Principio de Legalidad

El principio de legalidad[9], siendo uno de los principios reconocidos por los tratadistas casi universalmente, establece que nadie podrá ser penado por acciones u omisiones que no estén expresamente calificadas como faltas o delitos en una ley anterior a su perpetración.

Este principio o sus consecuencias vienen contemplados en los tratados internacionales en materia de Derechos Humanos, Constitución, Código Penal y Código Procesal Penal y es considerado uno de los pilares de cualquier estado democrático y de Derecho.

La imposición de este principio se convirtió tan necesaria por el deseo de las personas de buscar un control del poder punitivo del Estado, debido a la gravedad de los medios que este emplea en la represión o sanción del delito, por lo que la aplicación de este derecho debe estar confinada dentro de los límites que no permitan la arbitrariedad de quien ostente el poder penal.

---

[8] González Cauhaopé-Cazaux Eduardo. **Apuntes de Derecho Penal Guatemalteco. La Teoría del Delito.** Pág. 15.
[9] **Ibid.** Pág. 16.

Las principales consecuencias o garantías que emanan del principio de legalidad que se estudian en la presente investigación son las siguientes:

I. **La garantía de reserva absoluta de ley**

Estipula que tan sólo una ley emanada del Congreso de la República puede definir tipos penales y establecer sanciones, de esta manera se evita la creación de tipos penales mediante disposiciones reglamentarias.

II. **La garantía de la exigencia de certeza en la Ley**

Consiste en que la razón de ser del principio de legalidad es evitar que el ciudadano pueda ser "sorprendido" y sancionado por incurrir en una conducta que ignoraba que era prohibida, la autoridad por su parte deberá abstenerse a lo estrictamente señalado en el texto legal y no podrá imponer una sanción cuando la conducta realizada no se enmarque plenamente en lo descrito en el tipo, por ello para que el principio de legalidad sea plenamente efectivo es necesario que el legislador establezca con certeza cuáles son las conductas prohibidas, evitando al máximo arbitrio del Juez.

III. **La garantía de la prohibición de la analogía**

Se encuentra contemplada taxativamente en el Artículo 7 del Código Penal en el que se establece lo siguiente: "Artículo 7.- Exclusión de la analogía. Por analogía, los jueces no podrán crear figuras delictivas ni aplicar sanciones."

Cabe necesario acotar que la analogía es un método de integración del derecho y no de interpretación y que consiste en atribuir a situaciones particularmente idénticas (una prevista y otra no prevista en la ley), las consecuencias jurídicas que se señala en la regla prevista al caso concreto. El derecho penal describe una serie de conductas

punibles y bajo ningún concepto un juez está autorizado a aumentar el alcance de la punibilidad.

El Tratadista Muñoz Conde denomina al principio de legalidad como "principio de intervención legalizada, explica que el principio establece que la intervención punitiva del Estado, tanto al configurar el delito como al determinar, aplicar y ejecutar sus consecuencias debe estar regida por el imperio de la ley, entendida esta como expresión de la voluntad general"[10].

En el mismo sentido que el tratadista anterior, Bacigalupo manifiesta que: "La Ley penal tiene una función decisiva en la garantía de la libertad". Esta función suele expresarse en la máxima ***nullum crimen, nulla poena sine lege,*** lo que quiere decir que "sin una ley que lo haya declarado previamente punible ningún hecho puede ser merecedor de una pena en el derecho penal"[11].

Finalmente, con base en las ideas del tratadista Bacigalupo, el principio de legalidad debe entenderse como "la garantía de la objetividad del juicio sobre el hecho porque solo con la distancia de una ley previa es posible juzgad correctamente los hechos"[12].

No obstante, es importante indicar que el principio de legalidad conlleva también en determinadas consecuencias, pues el principio legalista contiene prohibiciones que someten al legislador y al Juez y se expresa en exigencias a los mismos, las que se pueden apreciar si se considera que una pena se habrá aplicado conforme a este principio, sólo si está establecida en una ley previa. En otras palabras, el razonamiento judicial debe comenzar con la ley, pues sólo de esta manera la condena se podrá fundar en la ley penal.

---

[10] Muñoz Conde, Francisco. **Introducción al Derecho Penal.** Pág. 80.
[11] Bacigalupo, Enrique. **Principios del derecho penal, parte general.** Pág. 55.
[12] **Ibid.** Pág. 59.

En Guatemala, el Artículo 5 de la máxima del ordenamiento jurídico siendo la Constitución Política de la República de Guatemala establece el principio de legalidad, enunciado bajo el epígrafe de Libertad de Acción, el cual consiste en que: "Toda persona tiene derecho a hacer lo que la ley no prohíbe; no está obligada a acatar órdenes que no esté basadas en la Ley y emitidas conforme a ella. Tampoco podrá ser perseguida ni molestada por sus opiniones o por actos que no impliquen infracción a la misma."

1.4.2 Principio de Intervención Mínima

El derecho penal es la forma más violenta que dispone el Estado para responder a las actuaciones de los ciudadanos que se determinan contrarias a la Ley. En ese orden de ideas, el principio de intervención mínima "impide en un Estado democrático la expansión del derecho penal, debiendo quedar reducido a su mínima expresión"[13]. Algunas consecuencias de este principio limitador del poder de sanción estatal son las siguientes:

- La exclusiva protección a bienes jurídicos: Este principio es consecuencia del desarrollo del postulado proclamado que sólo deben considerarse delito las conductas socialmente dañosas: *"nullum crimen sine iniura".* El derecho penal de un estado social se justifica como sistema de protección de la sociedad, los intereses sociales que por su importancia pueden merecer la protección del derecho se denominan "bienes jurídicos".

Se establece de esta forma una primera limitación al poder sancionador del Estado, solo podrán calificarse como delito aquellas conductas que lesionen o pongan en peligro bienes jurídicos ello obliga a determinar cuáles son los intereses sociales que tienen suficiente importancia como para ser convertidos en bienes jurídicos penalmente protegidos. Por ello el derecho penal sólo debe proteger aquellos valores contenidos en la Constitución que al ser afectados lesionan los mínimos requisitos para desarrollar la vida en comunidad.

[13] González Cauhaopé-Cazaux Eduardo, **Op. Cit.** Pág. 18.

- **La subsidiariedad y utilidad del derecho penal:** Este principio se explica en virtud que el derecho penal ha de ser el último recurso, la última *ratio* al que debe recurrir el Estado para proteger un bien jurídico.

Directamente vinculado a la idea de subsidiariedad está el principio de utilidad, siendo esto que, el recurso a la vía penal ha de ser efectivo para proteger el bien jurídico tutelado, en caso contrario no se justifica el recurso a esta vía por ello antes de crear cualquier tipo penal es necesario determinar si la penalización es una forma útil para proteger un bien jurídico.

- **Responsabilidad de los hechos:** El principio de intervención mínima obliga al Estado a sólo perseguir aquellas acciones concretas que impidan la normal convivencia social, sólo se juzgará a las personas por hechos concretos que lesionen o pongan en peligro bienes jurídicos.

- **Proporcionalidad de las penas:** El principio de intervención mínima implica limitaciones en las sanciones que el Estado puede imponer, toda vez que debe existir proporción entre la lesión o peligro al bien jurídico y la sanción impuesta.

1.4.3 Principio de Culpabilidad

El concepto de culpabilidad se convierte en un límite a la capacidad sancionadora del Estado. El estado solo podrá imponer una sanción penal cuando pruebe la culpabilidad conforme a la Ley, tal y como lo estipula taxativamente el Artículo 14 numeral 2 del Pacto Internacional de Derechos Civiles y Políticos: "...2. Toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad conforme a la Ley."

Del principio de culpabilidad se extrae el principio de personalidad, la exigencia de dolo o imprudencia y la exigencia de compresión.

El principio de personalidad consiste en que se impide castigar a alguien por hechos ajenos. El principio de la exigencia de dolo o imprudencia consiste en que no puede existir un delito si no hay dolo o imprudencia en su autor, no basta que se produzca un resultado lesivo o que realice un comportamiento peligroso, para que haya delito el autor debe haber requerido el resultado o al menos haberlo producido por no haber puesto el debido cuidado.

En cuanto al principio de la exigencia de comprensión de ilicitud establece que para que una persona sea culpable es necesario que conozca que la conducta que va a realizar es prohibida y que pueda respetar dicha prohibición.

1.5. Función del Derecho Penal

Se le apunta una función específica al derecho penal, siendo está principalmente la función protectora de bienes jurídicos, en la que se afirma que la función primordial del derecho penal estriba en "la protección de bienes jurídicos e intereses con relevancia constitucional, a través de las normas de derecho penal lo que se pretende es proteger valores e intereses que en lo interno de una sociedad se consideran esenciales a efectos de lograr una convivencia pacífica de todos los miembros que la componen"[14].

El derecho penal ha tenido tradicionalmente como fin el mantenimiento del orden jurídico previamente establecido y su restauración a través de la imposición y la ejecución de la pena cuando es afectado o menoscabado por la comisión de un delito, corresponde al derecho penal castigar los actos delictivos que lesionan o ponen en peligro intereses individuales, sociales o colectivos, de ahí es que proviene el carácter sancionador del Derecho Penal atribuido en este caso al Estado.

---

[14] González Castro José Arnoldo. **Programa de Formación Inicial de la Defensa Pública. Teoría del Delito.** Pág. 16.

1.6. Características del Derecho Penal

Se entiende por características a todas las cualidades esenciales y diferenciadoras de los seres y de las cosas. Los tratadistas guatemaltecos en su obra doctrinaria hacen ver que el derecho penal posee ocho características siendo estas las siguientes[15]:

a. El derecho penal es una ciencia social y cultural en contraposición a las ciencias naturales, toda vez que son el producto de la voluntad creadora del hombre.
b. El derecho penal es normativo lo cual implica que como ciencia jurídica esté compuesto por normas que regulan el comportamiento externo de las personas dentro de una sociedad.
c. El derecho penal es de carácter positivo lo que se refiere a que la norma penal una vez promulgada por el Estado en el ejercicio de su poder punitivo es de observancia obligatoria para toda la sociedad, convirtiéndose en una norma de derecho vigente.
d. El derecho penal pertenece al derecho público, porque siendo el Estado su único titular, solamente a él le corresponde la facultad de establecer delitos y penas.
e. El derecho penal es valorativo toda vez que comprende el hecho que el Estado al estar llamado a proteger bienes jurídicos realiza un juicio de valor mediante la norma penal respecto a los bienes jurídicos a proteger.
f. El derecho penal es finalista pues al pertenecer a las ciencias sociales obedece a una teleología que se encamina a la aplicación de sus conocimientos siendo principalmente la seguridad jurídica que debe garantizar el Estado.
g. El derecho penal es fundamentalmente sancionador, la norma no solo prescribe la conducta de los ciudadanos en sociedad, sino que además impone penas como una consecuencia lógica sobrevenida de una infracción o afectación.
h. El derecho penal en esencia debe ser preventivo y rehabilitador, siendo su máxima en la sociedad guatemalteca, buscando la reinserción del delincuente y previniendo futuros delitos.

[15] De León Velasco y De Mata Vela. **Ob. Cit.** Pág. 38.

1.7. Fines del Derecho Penal

De la investigación realizada y los conceptos plasmados en este trabajo de investigación se puede concluir que el derecho penal forma parte del sistema de control social y, al igual que los otros subsistemas dentro de él, persigue asegurar el orden social, sirviéndose de los instrumentos fundamentales para ello siendo las normas, sanciones y el proceso.

CAPÍTULO II:

2. Delito

En términos generales el delito se puede definir como toda conducta que la ley sanciona con una pena. Un delito es una infracción a la ley del estado, una lesión a un derecho por obra de una acción u omisión humana. Para estudiar en que consiste un delito se debe partir desde sus características, así como las diferentes acepciones que se encuentran tanto legal como doctrinariamente.

2.1. Teoría del Delito

"La teoría del delito es un instrumento conceptual para determinar si el hecho que se juzga es el presupuesto de la consecuencia jurídico-penal previsto en la ley"[16]. Tiene una finalidad práctica, su objeto es establecer un orden racional y fundamentado de los problemas y soluciones que se presentan en la aplicación de la ley penal.

La teoría del delito se estructura como un método de análisis de distintos niveles, cada uno de estos niveles presupone el anterior y todos tienen la finalidad de ir descartando las causas que impedirían la aplicación de una pena y comprobando positivamente si se dan las que condicionan esta aplicación.

La importancia del sistema de la teoría del delito en su concepción clásica consiste en que este permite inferir consecuencias lógicas que no estarían expresas en la ley y posibilita un tratamiento igual de cuestiones iguales y desigual de las desiguales, en este sentido la teoría del delito presupone que el legislador ha adoptado sus decisiones de una manera razonable a partir de un punto de partida conocido y cognoscible.

---

[16] Bacigalupo Enrique, **Manual de Derecho Penal.** Pág. 67.

Sin embargo, la historia dogmática demuestra que esta explicación no es realista toda vez que en efecto el pensamiento del legislador se expresa en su lenguaje y este como todo lenguaje natural no es univoco, sino todo lo contrario. Un sistema dogmático del delito no es otra cosa que una hipótesis posible de la voluntad del legislador expresada en ley y, sobre todo, un orden de problemas y soluciones referidos a los casos en los que la ley debe aplicarse.

2.2. Definición de Delito

De Mata Vela y De León Velasco en su libro Derecho Penal Guatemalteco en el capítulo tercero definen el concepto del delito, haciendo alusión que actualmente en el Derecho Penal Moderno y especialmente en el medio de cultura jurídica guatemalteca se habla de "delito, crimen, infracción penal, hecho o acto punible, conducta delictiva o hecho antijurídico, hecho o acto delictuoso, ilícito penal, hecho criminal, contravenciones o faltas"[17].

La técnica moderna plantea dos sistemas para la definición del delito, siendo el sistema bipartito en el que se emplea un solo término para las transgresiones a la Ley Penal graves o menos graves, utilizándose la expresión delito y se emplea el término falta o contravención para designar las infracciones leves a la Ley Penal, castigadas con una menor penalidad que los delitos o crímenes, sistema que es utilizado en el ordenamiento jurídico guatemalteco.

El segundo sistema utiliza un solo término para designar todas las infracciones o transgresiones a la Ley Penal, graves, menos graves o leves (crímenes o delitos y faltas o contravenciones) utilizando la expresión reato. Cabanellas en su doctrina nos recuerda que la palabra delito proviene del latín *delictum*, expresión latina que también hace referencia de un hecho jurídico y doloso castigado con una pena, haciendo referencia al

[17] **Ibid.** Pág. 120.

quebrantamiento de una norma legal mediante una acción o conducta externa que apareja como consecuencia una sanción de carácter penal[18].

Los penalistas guatemaltecos De Mata Vela y De León Velasco en su obra doctrinaria han indicado que múltiples han sido los esfuerzos por parte de algunos autores por indagar sobre la naturaleza del delito, teniendo un resultado negativo pues es claro que la definición de delito siempre ha estado subordinada a la realidad social y humana de la que deriva, evolucionando a través del tiempo y el lugar pues lo que ayer se consideró delito actualmente puede que ya no lo sea, o viceversa, todo ello respondiendo a las necesidades y fines que la sociedad establezca en un momento dado.

2.3. Naturaleza del Delito

Los tratadistas guatemaltecos De León Velasco y De Mata Vela establecen que, para poder definir la naturaleza jurídica del delito es menester remontarse a los postulados de las dos más importantes Escuelas del Derecho Penal que han existido, siendo la Escuela Clásica y la Escuela Positiva del derecho Penal.

Postulados de la Escuela Clásica

Los máximos exponentes de esta escuela indican que la máxima perfección de la idea del delito no es sino "una idea de relación, la relación de la contradicción entre el hecho del hombre y la ley, al definir el delito sostienen que es la Infracción de la Ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo moralmente imputable y políticamente dañoso"[19]. De tal manera asienta la doctrina clásica que el delito no es sino un acontecimiento jurídico,

[18] Cabanellas **Ob. Cit.** Pág. 115.
[19] Jiménez de Asúa, Luis. **Principios de Derecho Penal. La Ley y el Delito.** Pág. 251.

infracción a la Ley del Estado, un choque de la actividad humana con la norma penal siendo en esencia un "ente jurídico".

En relación al delincuente se limitaron a decir que la imputabilidad moral y su libre albedrío son la base de su responsabilidad penal, en relación a la pena sostuvieron que era un mal a través del cual se realizaba la tutela jurídica, concluyeron y aseguraron que el Derecho Penal era una ciencia eminentemente jurídica y que para estudiarla se debía utilizar el método lógico abstracto, racionalista o especulativo.

Postulados de la Escuela Positiva

Los principales representantes de esta escuela al contrario a los clásicos parten del estudio del delincuente y estudian el delito como la acción humana resultante de la personalidad del delincuente. Los positivistas describen el delito no como un ente jurídico sino como una realidad humana, un fenómeno natural o social. En relación al delincuente sostenían que el hombre es imputable no porque sea un ser consciente, inteligente y libre sino sencillamente por el hecho de vivir en sociedad.

En relación a la pena consideraron que "era un medio de defensa social y que debía imponerse en atención a la peligrosidad social del delincuente y no en relación al daño causado, proponiendo las famosas medidas de seguridad con el fin de prevenir el delito y rehabilitar al delincuente"[20].

2.4. Criterios para definir el delito

Se han establecido criterios respecto a las ideas penales sobre que es el delito y primordialmente a corroborar o no la validez de estas ideas ante el derecho penal moderno, siendo los criterios principales los siguientes[21]:

[20] De Mata Vela y De León Velasco. **Op. Cit.** Pág. 163.
[21] **Ibid.** Pág. 166

2.4.1. Criterio Legalista

Establece que el delito es lo que está prohibido por la Ley lo que resulta ser demasiado amplio en la actualidad y no resuelve el problema sobre lo que prohíbe la ley, y el delito vendría a ser lo que quiera el legislador y ello podría conducir a absurdas exageraciones.

2.4.2. Criterio Filosófico

Este criterio hace referencia principalmente a dos puntos, toda vez que identificaban el delito con el pecado, como una conducta contraria a la moral y la justicia, y enfocándolo inmediatamente después como violación o quebrantamiento del deber, sosteniéndose que el delito es la violación de un deber, un quebrantamiento libre e intencional de los deberes. A lo que los tratadistas guatemaltecos concluyeron que no puede darse validez a este criterio en principio porque el pecado tiene una orientación divina que nada tiene que ver con la ciencia jurídica y en segundo plano porque las infracciones al deber atienden más a normas de conducta moral careciendo de sanción estatal.

2.4.3. Criterio Natural Sociológico

En este postulado de criterio, los positivistas italianos definen el delito en principio como presupuesto para que exista el delincuente, construyendo la definición del delito natural como la ofensa a los sentimientos altruistas fundamentales de piedad y prohibidad en la medida en que son poseídos por un grupo social determinado.

2.4.4. Criterio Técnico Jurídico

Este nace en Alemania y se aparta de los pensamientos de los positivistas italianos, emplea el método analítico para dedicarse de lleno al examen lógico del delito a lo que

en la doctrina se ha denominado "La construcción Técnico Jurídica de la Infracción" que se sintetiza en la teoría jurídica del delito, basándose en la tipicidad se define al delito como una acción típica, contraria al derecho, culpable, sancionada con una pena adecuada y suficiente a las condiciones objetivas de penalidad.

2.5. Elementos del Delito

Los elementos del delito "son el conjunto de características que componen el delito, es decir aquellas que tiene cualquier hecho delictivo para ser considerado como tal. Dichos elementos se estudian según la teoría general del delito dentro del derecho penal"[22].

No existe un consenso exacto y universal respecto a cuáles son los elementos del delito, ya que existen variaciones al respecto en los distintos ordenamientos jurídicos de los países. La doctrina ha dividido los elementos característicos del delito en dos esferas, siendo los elementos positivos o negativos dependiendo si conducen respectivamente a la condena o a la absolución del acusado.

2.5.1. Elementos Positivos del Delito:

Siendo los siguientes:

a. Acción o Conducta Humana

Se puede definir como el elemento positivo del delito siendo todo comportamiento derivado de la voluntad, es siempre el ejercicio de una voluntad final. Todo delito implica

[22] https://cienciasdelderecho.com/los-elementos-del-delito/ Escuela de Postrados de Ciencias del Derecho. **Los Elementos del Delito.** (Consultado: 20 de julio de 2023).

una acción u omisión voluntaria llevada a cabo por un individuo y que da origen al delito. Dichas acciones deben ser intencionales, voluntarias y conscientes.

En la acción tenemos dos fases siendo la fase interna y externa. La primera ocurre siempre en la esfera del pensamiento del autor en dónde se propone la realización de un fin. En la segunda consiste en que "después de la realización interna el autor la realiza en el mundo externo, su proceso de ejecución del acto"[23].

La omisión puede producir resultados jurídicos, el autor de una omisión debe estar en condiciones de realizarla, la acción y la omisión son subclases del comportamiento humano determinadas por el tipo. La omisión que importa al derecho penal es aquella que alguien debió realizar, las clases de omisión penalmente relevantes son:

- Omisión Propia: La simple infracción de un deber.
- Delitos de omisión con un resultado: La omisión se conecta a un resultado.
- Delitos impropios de omisión o de comisión por omisión: La omisión se conecta a un resultado prohibido, pero en el tipo legal no se menciona expresamente la forma de comisión omisiva.

b. Tipicidad

Se llama tipicidad a la "adecuación de la acción a los delitos tipificados en la ley, ósea al tipo de delito del que se trata, cuáles son sus características y elementos prohibitivos, entre otros. Todo lo que sea ilegal debe estar contemplado en la Ley. El tipo penal es un concepto jurídico producto de la interpretación de la Ley Penal, el tipo es la descripción de la conducta prohibida por una norma"[24]. Es pues la tipicidad un elemento positivo del delito que consiste en que la conducta humana encuadra en un tipo penal, esta nace del

[23] De León Velasco y De Mata Vela. **Ob. Cit.** Pág. 143-144
[24] Bacigalupo, Enrique. **Lineamientos de la Teoría del Delito.** Pág. 17

principio de legalidad, todos los delitos provocados por la acción u omisión voluntaria del sujeto deben estar regulados por la ley.

c. Antijuridicidad o antijuricidad

Cuando se habla de "antijuridicidad", se refiere exactamente a lo opuesto al derecho, a que un acto es en esencia contrario al ordenamiento jurídico vigente. Así, los delitos son "actos antijurídicos declarados como tales cuando se los compara con lo contemplado en el ordenamiento jurídico de la nación. Los elementos antijurídicos "carecen de justificación posible ya que incumplen una norma jurídica explícita"[25].

"La cuestión de antijuricidad no es otra que la de saber si la realización del tipo está o no amparada por una causa de justificación"[26].

Se concluye pues que, la antijuridicidad o antijuricidad un elemento positivo del delito siendo aquel desvalor que posee un hecho típico contrario a las normas del Derecho general. Es lo contrario a Derecho, tiene consecuencias jurídicas y no debe tener causas de justificación.

d. Culpabilidad

La culpabilidad "es la capacidad del ser humano para reaccionar ante las exigencias normativas, derivadas de la prevención general, es lo fundamental, y permite la atribución de una acción a un sujeto y por consiguiente determina su responsabilidad"[27].
Para que una persona sea culpable es necesario la imputabilidad o capacidad de culpabilidad, el conocimiento de la antijuridicidad, y la exigibilidad de un comportamiento

---

[25] https://concepto.de/elementos-del-delito/ Enciclopedia Concepto. **Elementos del delito.** (Consultado: 22 de julio de 2023).
[26] Bacigalupo, Enrique. **Ob. Cit.** Pág. 45
[27] De León Velasco y De Mata Vela. **Ob. Cit.** Pág. 181

distinto. El primero hace referencia a la capacidad de ser sujeto del Derecho Penal, sin ellas no puede hablarse de culpabilidad. La segunda hace referencia a que si el individuo puede conocer a grandes rasgos el contenido de las prohibiciones el individuo imputable puede motivarse, y la tercera hace referencia que hay ciertos ámbitos de exigencia fuera de los cuales no puede exigirse responsabilidad alguna.

La culpabilidad del delito tiene tres formas generales de culpa o responsabilidad siendo las siguientes:

- **Imprudencia:** "Infracción o incumplimiento del deber objetivo-general del cuidado o diligencia impuesto por una norma, escrita o no, de cuidado, prudencia o diligencia"[28].

- **Negligencia:** "Es la omisión de la atención debida por inacción o descuido o por acción incorrecta, inadecuada o insuficiente"[29].

- **Impericia:** "La falta de sabiduría, práctica, experiencia o habilidad"[30].

e. La Imputabilidad

Es la capacidad para conocer y valorar el deber de respetar la norma. Es "la capacidad de la persona de actuar con culpabilidad en el derecho, la posibilidad de imputación"[31]. Por lo que es imputable todo aquel que posea en el tiempo de la acción realizada las condiciones psíquicas exigidas por la ley para poder desarrollar su conducta socialmente.

---

[28] https://dpej.rae.es/lema/imprudencia Diccionario Panhispánico del Español Jurídico. **Imprudencia.** (Consultado: 22 de julio de 2023).
[29] https://dpej.rae.es/lema/negligencia Diccionario Panhispánico del Español Jurídico. **Negligencia.** (Consultado: 22 de julio de 2023).
[30] https://concepto.de/impericia/ Enciclopedia Concepto. **Impericia.** (Consultado: 22 de julio de 2023).
[31] https://dpej.rae.es/lema/imputabilidad Diccionario Panhispánico del Español Jurídico.**Imputabilidad.** (Consultado: 22 de julio de 2023).

f. Punibilidad

La punibilidad se refiere a una serie de circunstancias necesarias para la imposición de una pena, o bien excluyen la sanción penal pese a tratarse de una conducta típica, antijurídica y culpable, es por tanto "una forma de recoger y elaborar una serie de elementos o presupuestos que el legislador por razones utilitarias, diversas en cada caso y ajenas a los fines propios del derecho penal puede exigir para fundamentar o excluir la imposición de una pena"[32].

2.5.2. Elementos Negativos del Delito

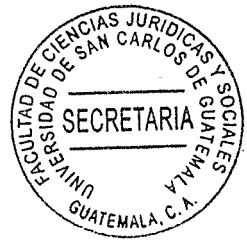
Los elementos negativos del delito "tienden a destruir la configuración jurídica del mismo, su consecuencia principal es eliminar la responsabilidad penal del sujeto"[33]. El Código Penal de Guatemala, Decreto 17-73 del Congreso de la República en su título tercero de su parte general denomina a los elementos negativos del delito como causas que eximen la responsabilidad penal, siendo tres clases:

a. Ausencia de Acción

Cuando la voluntad falta no hay acción penalmente relevante, como sucede en los casos de: fuerza irresistible, movimientos reflejos, estados de inconsciencia. Si la conducta está ausente, no habrá delito. La ausencia de conducta es un aspecto negativo, impeditivo de la formación de la figura delictiva.

---

[32] De León Velasco y De Mata Vela. **Ob. Cit.** Pág 167
[33] **Ibid.** Pág. 231.



b. Causas de Inimputabilidad

Se encuentran establecidas en el Artículo 23 del Código Penal estableciendo quienes son inimputables y por ende tampoco responsables penalmente, siendo los menores de edad y quien en el momento de la acción u omisión, no posea, a causa de enfermedad mental, de desarrollo síquico incompleto o retardo 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.

c. Ausencia de Antijuricidad o Causas de Justificación

Las causas de justificación se encuentran establecidas en el Artículo 24 del Código Penal, son aquellas en las que una conducta normalmente prohibida por la ley penal, no constituiría delito por la existencia de una norma que lo autoriza. Las causas de justificación lo que hacen es permitir la agresión a bienes jurídicos, o por lo menos no la prohíben, en virtud de ciertas circunstancias que al legislador le parecen más importantes que la protección de un bien jurídico individual. El Artículo 24 del Código Penal guatemalteco tipifica las siguientes: legítima defensa, estado de necesidad.

d. Causas de Inculpabilidad

Las causas de inculpabilidad, son aquellas situaciones que eliminan la reprochabilidad de la actitud subjetiva asumida por el autor frente al hecho antijurídico. Estas se encuentran reguladas en el Artículo 25 del Código Penal, siendo las siguientes: miedo invencible, fuerza exterior, error, obediencia debida y omisión justificada.

2.6. Clasificación de los delitos

Los tratadistas guatemaltecos, han clasificado los delitos de la siguiente forma:

2.6.1. Por su gravedad

Clasifican por su gravedad en delitos y faltas siendo este el sistema bipartito que sigue el Código Penal guatemalteco. Los delitos o crímenes son infracciones graves a la ley penal, mientras que las faltas o contravenciones son infracciones leves a la ley penal, de tal manera que los delitos son sancionados con mayor dureza que las faltas ello en atención a su mayor gravedad.

En Guatemala se castiga los delitos principalmente con pena de prisión, pena de multa, pena mixta y extraordinariamente con la pena de muerte aunque esta no es aplicable en virtud del Pacto de San José, mientras que las faltas sólo se sancionan con pena de arresto y pena de multa.

2.6.2. Por su estructura

Por su estructura se clasifican en dos vías: simples y complejos. Son delitos simples los que están compuestos de los elementos descritos en el tipo y violan un solo bien jurídico protegido. Son delitos complejos aquellos que violan diversos bienes jurídicos y se integran con elementos de diversos tipos delictivos.

2.6.3. Por las formas de la culpabilidad

Pueden dividirse en delitos dolosos y delitos culposos o imprudentes. En los primeros el autor ha querido la realización del hecho típico, existe coincidencia entre lo que el autor

hizo y deseaba realizar. En los segundos el autor no ha querido la realización del hecho, el resultado no es producto de la voluntad, el autor ha faltado al cuidado en su actuar.

2.6.4. Por la forma de la acción

Por comisión los cuales surgen de la acción del autor cuando la norma le prohíbe realizar algo y se realiza, por omisión que son abstenciones del autor a un mandato.

2.6.5. Por la calidad del sujeto activo

Se puede clasificar en comunes los que pueden ser realizados por cualquiera, y especiales siendo estos los que solamente pueden ser cometidos por un número limitado y específico de personas que tengan las características especiales requeridas por la ley.

2.6.6. Por la forma procesal

Se encuentran taxativamente contenidos en el Código Procesal Penal siendo de tres tipos: de acción pública, que son los que para su persecución no requieren de denuncia previa; dependientes de instancia privada, estos son los que no pueden ser perseguidos de oficio y requieren de una denuncia inicial; de instancia privada, siendo estos los que además de la denuncia, el denunciante debe seguir dando el impuso procesal como querellante.

2.6.7. Por el resultado

Se divide en formales que exigen la producción de determinado resultado y están integrados por la acción, imputación objetiva y el resultado y los de actividad que son aquellos en lo que la realización del tipo coincide con el último acto de la acción y por tanto no se produce un resultado que puede ser separable de ella.

2.6.8. Por el daño que causan

Divididos en delitos de lesión en los que hay un daño apreciable al bien jurídico, se relaciona con los delitos de resultado y los delitos de peligro en los que no se requiere que la acción haya ocasionado un daño sobre un objeto, sino que es suficiente con que el objeto jurídicamente protegido haya sido puesto en peligro de sufrir la lesión.

2.6.9. Por su ilicitud y motivaciones:

Se clasifican en comunes, políticos y sociales. Delitos comunes todos aquellos que lesionan o ponen en peligro valores de la persona individual o jurídica. Delitos políticos los que atacan o ponen en peligro el orden político del Estado. Delitos sociales los que atacan o ponen en peligro el régimen social del Estado.

2.7. De la pena

Los doctrinarios De León Velasco y De Mata Vela exponen en su obra que la pena es "una consecuencia eminentemente jurídica y debidamente establecida en la ley, que consiste en la privación o restricción de bienes jurídicos, que impone un órgano jurisdiccional competente en nombre del Estado al responsable del ilícito penal"[34].

Se define la pena como "la privación de bienes jurídicos que el estado impone al autor de un delito en la medida tolerada por un sentimiento social, medio de seguridad jurídica y que tiene por objeto resocializarle, para evitar nuevos ataques a bienes jurídicos penalmente tutelados"[35]. En la actualidad se puede concebir formalmente a las penas como aquellas restricciones y privaciones de bienes jurídicos señalados específicamente en la Ley Penal, siendo una consecuencia eminentemente jurídica.

---

[34] **Ibid.** Pág. 248
[35] Zaffaroni, Eugenio Raúl. **Ob. Cit.** Pág. 77

CAPITULO III

3. Ciberdelincuencia aspectos generales

La criminalidad informática, también denominada por la doctrina penal como cibercriminalidad o ciberdelincuencia, constituye en una especie de fenomenología delictiva que hace parte del nuevo derecho penal en comparación con los delitos tradicionales, una fenomenología que también se enmarca en la moderna criminalidad organizada transnacional que se ha vuelto en el tópico que con tanto empeño quieren combatir las naciones por medio de la cooperación internacional.

Las sociedades de la información por la evolución de las Tecnologías de la Información, la ausencia de fronteras y la inmaterialidad de la comunicación a través de estas "conducen en el ámbito del Derecho Penal a la escasa relevancia de los límites temporales y espaciales que han constituido tradicionalmente su límite"[36].

3.1. Definición de Ciberseguridad

"La ciberseguridad, surge para neutralizar las amenazas derivadas de la utilización del ciberespacio y se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información consistentes en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados.

Donde los controles de ciberseguridad son eficaces, "el ciberespacio es considerado confiable, flexible y seguro y dónde los controles de ciberseguridad están ausentes, incompletos o mal diseñados, el ciberespacio es considerado tierra de nadie"[37].

---

[36] Fernández Bermejo Daniel y Martínez Atienza Gorgonio. **Ciberdelitos.** Pág. 29.
[37] **Ibid.** Pág 22.

La ciberseguridad "es la práctica de defender las computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de los ataques maliciosos. También se le conoce como seguridad de tecnología de la información o seguridad de la información electrónica"[38].

La ciberseguridad se encarga de la seguridad en el medio digital, diseñando normas o procedimientos destinados a conseguir un sistema de informática seguro y confiable para cada uno de los usuarios del internet y se encuentra enfocada esencialmente en la información que se encuentra en formato digital y los sistemas interconectados que la procesan o transmiten, se concreta en un conjunto de actuaciones orientadas a asegurar los sistemas que constituyen el ciberespacio, preservando la confidencialidad, disponibilidad e integridad de la información proporcionada por los usuarios.

3.2. Definición de ciberespacio

El ciberespacio es el conjunto de medios y procedimientos basados en las Tecnologías de la Información y la Comunicación, configurados para la prestación de servicios, y está constituido por *hardware, software,* internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socioeconómica de cualquier nación y en especial aquellos ligados a sus infraestructuras críticas[39].

Aunque el ciberespacio es un elemento de naturaleza variable debido al avance de las Tecnologías de la información es importante aproximarse a él a través de los elementos que lo componen siendo importante en principio determinar la naturaleza jurídica del ciberespacio.

---

[38] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security Kaspersky Lab. **¿Qué es la ciberseguridad?** (Consultado: 25 de julio de 2023).
[39] **Ibid.** Pág. 22.

Partiendo de un punto de vista tradicional, los Estados tienen como límite espacial de sus competencias sus propios territorios, compuesto de las dimensiones terrestre, marítimo y área, espacios que se pueden delimitar por un entorno físico, natural o artificial con dimensiones y fronteras. No obstante en el desarrollo de las tecnologías de la información ha llevado a hablar de nuevos dominios como el ciberespacio.

La naturaleza jurídica del ciberespacio es de carácter dual[40], la parte virtual del ciberespacio es ilimitada porque trasciende las limitaciones geográficas y físicas teniendo incidencia directa en materia de fronteras y jurisdicciones, teniendo el ciberespacio como un espacio común que no forma parte de ningún estado y como consecuencia ningún Estado puede ejercer soberanía sobre él.

Por otra parte, el componente físico del ciberespacio, las comunicaciones, almacenamiento y recursos de computación sobre los que funcionan sus sistemas de información se ha denominado ciber infraestructura, lo que significa que el ciberespacio es una fusión entre zonas del espectro electromagnético y una infraestructura física espacial. Se puede concluir que el ciber espacio es un dominio conformado por un vasto conjunto de redes cuya manifestación es el internet sin que sea la única.

3.3. Definición de ciber amenaza

Las ciber amenazas representan en la actualidad uno de los principales riesgos para las empresas, así como para las personas individuales, por lo que la comunidad jurídica internacional desde los años noventa empezó una discusión sobre la aplicación de las distintas normas de Derecho Penal Internacional a este dominio del ciberespacio.

[40] **Ibid.** Pág. 20

Las investigaciones realizadas por la comunidad internacional y expertos referentes al tema han identificado que existen diversos tipos de ciber-amenazas, las cuales serán objeto de estudio dentro de este trabajo de investigación.

Tipos de ciber amenazas

Las amenazas a las que se enfrenta la ciberseguridad son tres[41]:

1. El delito cibernético.
2. Los ciberataques, son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas.
3. El ciberterrorismo, que tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor ara desestabilizar a un país o aplicar presión a un gobierno.

El Consejo de Europa define el ciberterrorismo como al "terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos", analizando las ciber amenazas terroristas, se presupone que las consecuencias más significativas de este tipo de delitos son económicas y de imagen.

Los agentes malintencionados consiguen el control de los sistemas informáticos a través de alguno de estos métodos comunes utilizados para amenazar la ciberseguridad siendo los siguientes[42]:

---

[41] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. Kaspersky Lab. **¿Qué es la ciberseguridad?** (Consultado: 25 de julio de 2023).

[42] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security Kaspersky Lab. **¿Qué es la ciberseguridad?** (Consultado: 25 de julio de 2023).

a. Inyección de código *SQL*

Es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción maliciosa, esto brinda acceso a la información confidencial contenida en la base de datos.

b. Malware

Término que hace referencia al *software* malicioso, siendo una de las ciber amenazas más comunes. El *malware* es el *software* que un cibercriminal o un *hacker* ha creado para interrumpir o dañar el equipo de un usuario legítimo y con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima. Puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos. Los tipos de *malware* más comunes son: virus, troyanos, *spyware, ransomware, hadware, botnets.*

c. Phishing

Es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de *phishing* se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito y otra información personal.

En el año 2022 Prensa Libre publicó un Artículo en el que hace de conocimiento que "los ataques de *malware y phishing*, fueron los ciberataques que más aumentaron en el año 2022 en Guatemala, ello gracias a que *Kaspersky* la empresa de ciberseguridad y privacidad digital presentó el panorama de ciberataques en Latinoamérica siendo Guatemala el país que más ataque se *phishing* presentó"[43].

[43] Jumique, Andrea. **Ataques de *malware* y *phishing*, los ciberataques que más aumentaron en el 2022 en Guatemala,** 30 de diciembre 2022.

3.4. Definición de ciberdelito

En la actualidad por los avances de las Tecnologías de la Información este concepto se ha revestido de popularidad en todos los campos de las ciencias tanto sociales como naturales, lo que ha logrado establecer un criterio para definir que es un ciberdelito.

En el mismo sentido es importante hacer la acotación que el aumento de los delitos relacionados con los sistemas ha creado la necesidad de definir este tipo de flagelos que se cometen el mundo del ciberespacio pero que sus consecuencias jurídicas trascienden a la esfera de la realidad, algunos autores han intentado definirlos mientras que otros consideran que no es necesario debido a que se trata de delitos tradicionales cometidos a través del uso de medios informáticos.

Los ciberdelitos, delitos cibernéticos, delitos electrónicos o delitos informáticos han sido definidos de distintas formas, previo a dar la conclusión y definición propia del entendimiento de este concepto es menester citar algunas definiciones de tratadistas internacionales expertos en la materia.

Para Tellez Valdéz se definen como "actitudes ilícitas en las que se tienen a las computadoras como instrumento o fin". También indica que son: "Las conductas típicas, antijurídicas y culpables en las que se tiene a las computadoras como instrumento o fin"[44].

Es preciso concluir que, la definición de delitos informáticos y una debida regulación en el Código Penal de Guatemala es importante ya que no todas las conductas ilícitas que se puedan cometer utilizando medios informáticos encuadran en los delitos regulados en la legislación actual y es menester recordar que en materia penal no es permitida la analogía, siendo imposible para el Juzgador en el ejercicio de su función encuadrar este

[44] Tellez Valdéz, Julio. **Derecho Informático.** Pág. 105

tipo de conductas principalmente por contar con características y elementos distintivos a las figuras penales tradicionales.

3.5. Elementos del ciberdelito o del delito informático

En el derecho penal la ejecución de la conducta punible supone la existencia de dos sujetos a saber, siendo uno un sujeto activo y el otro un sujeto pasivo, quienes pueden ser a su vez una o varias personas naturales o individuales o personas jurídicas.

- **Sujeto activo,** es quien realiza toda o una parte de la acción descrita por el tipo penal.
- **Sujeto pasivo,** es la persona titular del bien jurídico que el legislador protege.

Los sujetos pasivos o víctimas de los delitos informáticos pueden ser no sólo personas físicas sino también personas jurídicas como empresas, el Estado y los usuarios o instituciones que integran el sistema financiero.

- **Bien jurídico protegido,** el objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo, jamás debe dejar de existir ya que constituye la razón de ser delito y no suele estar expresamente señalado en los tipos penales.

Hace algunas décadas los delitos cibernéticos eran cometidos por personas que tenían conocimiento especializado en sistemas informáticos, actualmente no necesariamente quien comete un delito informático debe tener conocimientos especializados, por ejemplo, basta que una persona tenga un teléfono inteligente para compartir datos, imágenes, audios o videos de otra persona sin su consentimiento y con el propósito de causarle un daño.

Los delincuentes toman ventaja de la tecnología, algunas veces no actúan solos y forman redes u organizaciones de delincuentes.

Además, los sujetos activos de los delitos informáticos pueden ser empleados, funcionarios, servidores públicos, que en virtud de sus funciones tienen acceso a ciertos sistemas informáticos, de tecnología o de información.

3.6. Características del Ciberdelito

De las características inherentes a los riesgos informáticos los tratadistas en la materia han concluido en las siguientes[45]:

a. **Son riesgos automáticos:**

La cibercriminalidad se caracteriza porque las conductas punibles son realizadas mediante tratamientos automatizados, interactivos y continuos de datos e información registrados en sistemas informáticos interconectados a nivel global, lo que implica acelerar los procesos, aumentar su impacto y alcance y una menor actividad humana en la creación, producción y prevención de los riesgos y sus efectos.

En términos prácticos esto les supone a los atacantes la posibilidad de realizar agresiones informáticas complejas de manera simultánea y repetida, sin malgastar recursos de manera innecesaria para su comisión u omisión en sistemas que cada vez son de más fácil acceso. Son ataques poco costosos en comparación con el valor de realización inherente a los delitos tradicionales.

[45] Posada Maya, Ricardo. **Los cibercrímenes. Un nuevo paradigma de la criminalidad.** Pág. 72

Lo anterior se concluye en que las redes por su propio diseño poseen ciertas vulnerabilidades que son relativamente fáciles de explotar tales como la suplantación de identidad por parte de una máquina como lo es el *spoofing* y la inyección o escucha de paquetes como lo es *sniffing*. En definitiva, es posible afectar el control o correcto intercambio de datos entre los puntos de acceso y los clientes de la red, todo esto, incluso de manera automática quebrando sus sistemas de seguridad.

b. Son riesgos descentralizados:

Actualmente es de conocimiento de todos que los datos como personas naturales al igual que los datos de las personas jurídicas, incluso aquellos datos de carácter personal privados o semiprivados sobre todo los de índole económico se encuentran en poder de terceros que administran enormes bases de datos. ¿Cómo se usa esto? ¿Para qué se usan? ¿Se encuentran debidamente protegidos para que no tengan acceso a terceros con intenciones fraudulentas? Preguntas que hacen ver el enorme riesgo en el que nos encontramos. Esta misma consideración se puede hacer respecto de los titulares de los sistemas informáticos que tratan dicha información y que sufren los ataques de cibercriminales que actúan con fines terroristas o con ánimo de lucro.

La tercerización de la información implica que los titulares de los datos difícilmente puedan tomar medidas preventivas de seguridad para protegerlos adecuadamente. Esta es precisamente una de las relaciones más paradójicas del moderno tratamiento de datos, pues cualquiera puede tener los datos de otro, aunque resulte más difícil obtener los propios.

Un ejemplo de riesgos descentralizados o por fuera del dominio de su titular es, la administración del almacenamiento de datos informáticos en la nube. Los riesgos materiales que ofrece esta capacidad de cómputo a través del internet dependen entre otras cosas de la adecuada gestión del proveedor, pues solo de esta manera el cliente

tendría un acceso confiable y seguro de la información sin injerencia preventiva o de seguridad en el dominio de los peligros

c. Son riesgos anónimos:

La cibercriminalidad y su impunidad se basa principalmente en actuaciones, incidentes o ataques amparados por el relativo anonimato que les provee la red a los delincuentes cibernéticos o cibercriminales, y aun cuando el anonimato y la confidencialidad de la navegación en la red puede llegar a ser un derecho fundamental relativo, el cambio de la identidad natural por la digital facilita la realización de actividades criminales.

Las actividades criminales más comunes que se han realizado por medio de esta facilidad del anonimato son el terrorismo, la pornografía o la pedofilia siendo esto el famoso *grooming* y las defraudaciones económicas que las personas no harían en la vida física, agregando que estos comportamientos usualmente se realizan en terminales públicas que carecen de control o regulación por parte del Estado.

d. Son riesgos técnicos:

Los delitos informáticos se caracterizan objetiva y subjetivamente por realizarse o ejecutarse en un especial contexto informático, cuyo refinamiento y desarrollo en términos de innovación tecnológica supera la capacidad preventiva y sancionadora del derecho punitivo contemporáneo.

Lo anterior suele denominarse **cadencia legal,** y resulta en la incapacidad formal y material del derecho para predecir estos avances y posibles peligros con la debida anticipación lo que coadyuva el crecimiento de una gran cifra de cibercriminalidad informática.

e. Son riesgos masivos o de efectos catastróficos:

Si bien es cierto que la mayoría de ciber crímenes afectan a una persona o a un grupo particular con efectos limitados, también se advierten con frecuencia ataques informáticos masivos o a gran escala y con gran lesividad que afectan a grandes sectores de la población, producen daños económicos sociales y políticos considerables, paralizan los sistemas informáticos y las comunicaciones globalizadas o perturban la infraestructura crítica de los países en perjuicio de grandes centros urbanos postindustriales.

3.7. Clases de Ciberdelito

A partir del desarrollo acelerado de la internet, también emerge el lado oscuro y surgen nuevos términos como ciberdelito que tienen cuatro características específicas siendo que se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

Actualmente existen diversos tipos de modalidades de delitos informáticos[46], no obstante, los ciberdelitos y contravenciones más comunes que se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin autorización del usuario y con fines mayoritariamente económicos y de daño:

A. Ataques en la navegación, se da cuando se desvía el navegador del usuario a páginas que causan infecciones con programas maliciosos como virus, gusanos y

[46] Instituto de la Defensa Público Penal. **Delitos Informáticos.** Pág 35

troyanos, programas que pueden borrar el sistema operativo del usuario, infectar su teléfono y computadora, activar la *webcam*, extraer datos, entre otros.

B. Ataques a los servidores, estos pueden dañar o robar los datos del usuario y negarle el acceso a su información.

C. Corrupción de bases de datos, estos interfieren en bases de datos públicas o privadas para generar datos falsos o robar información del usuario.

D. Virus informáticos, en los que se encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que aparentan ser de la compañía de telefonía móvil a la que está suscrito el usuario.

E. Programa espía, consisten en que alguno de los dispositivos del usuario tiene instalado un *software* que le permite encender y grabar con la cámara y el micrófono, así como acceder a la información personal del usuario sin su autorización y sin que tenga conocimiento de lo que está sucediendo en ese momento.

Además de la clasificación descrita con anterioridad, el gobierno de Argentina, ejemplifica algunos ciberdelitos que usan la ingeniería social para engañar a los usuarios de internet:

a. *Phishing o vishing,* en este flagelo informático los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y solicitan los datos que sean necesarios para suplantar la identidad del usuario víctima de este engaño y de esa forma operar con sus cuentas bancarias, perfiles en plataformas de redes sociales, servicios y aplicaciones en la web.

b. *Ciberbullying,* es uno de los más populares flagelos principalmente en las poblaciones de jóvenes adultos o de adolescentes, consiste en el acoso por mensajería instantánea y en las redes sociales con la intención de perseguir, acechar, difamar y atentar contra el honor e integridad moral de una persona. Se hace a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, de la creación de memes que denigran a la persona por alguna situación o padecimiento o el etiquetado en publicaciones.

c. *Grooming,* es cuando un adulto mediante engaños y mentiras se gana la confianza y establece algún tipo de amistad con una niña, niño o adolescente a través del internet, ya sea mediante las redes sociales o por aplicaciones de mensajería instantánea con el fin de obtener imágenes o videos con connotación o actividad sexual. "Estas imágenes o videos están destinados al consumo de pederastas o a redes de abuso sexual a menores con el objeto de llevar a cabo chantaje, abuso y/o explotación sexual o prostitución infantil"[47].

d. *Sextorsión,* es uno de los ciberdelitos más comunes y en mayor crecimiento, consiste en pedir dinero a cambio de no difundir en las redes sociales imágenes generadas para un intercambio erótico que en su momento fue consentido. De conformidad con el marco legal en Guatemala, las personas que cometen *sextorsión* pueden incurrir en el delito de Violación a la Intimidad Sexual tipificado en el Artículo 190 del Código Penal.

e. Ciberodio, esto hace referencia a que son contenidos inapropiados que pueden vulnerar a las personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, xenofobia, racismo, discriminación o maltrato animal.

f. Pornografía Infantil, se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita. También se encuentran clasificados en cuanto a la privacidad de las personas:

En Guatemala, el Código Penal en su proximidad a los delitos que tienen relación con medios informáticos los únicos que se encuentran son los siguientes:

a) Artículo 274 "A" Destrucción de registros informáticos;
b) Artículo 274 "B" Alteración de programas;

---

[47] https://www.gob.mx/profeco/es/articulos/grooming-y-ciberacoso-en-ninos?idiom=es Gobierno de México. ***Grooming* y Ciberacoso en Niños.** (Consultado: 26 de julio de 2023).

c) Artículo 274 "C" Reproducción de Instrucciones o programas de Computación;
d) Artículo 274 "D" Registros Prohibidos;
e) Artículo 274 "E" Manipulación de Información;
f) Artículo 274 "F" Uso de Información;
g) Artículo 274 "G" Programas Destructivos;

No obstante, al no estar las anteriores, clasificadas específicamente como ciberdelitos o delitos informáticos el Código Penal señala otras conductas que podrían incluirse de este tipo siendo las siguientes:

a) Violación a Derechos de Autor, contenida en el Artículo 274 del Código Penal;
b) Violación a los Derechos de Propiedad Industrial contenida en el Artículo 275 del Código Penal;
c) Pánico Financiero contenido en el Artículo 342 "B" del Código Penal;
d) Ingreso a espectáculos y distribución de material pornográfico a personas menores de edad contenida en el Artículo 189 del Código Penal;
e) Violación a la intimidad sexual contenida en el Artículo 190 del Código Penal;
g) Comercialización o difusión de pornografía de personas menores de edad contenida en el Artículo 195 Bis;
h) Posesión de material pornográfico de personas menores de edad contenido en el Artículo 195 ter;

Quedando evidenciado que, de conformidad con el ordenamiento jurídico vigente, no existe una legislación penal que tipifique específicamente los delitos cometidos por medio de plataformas electrónicas que tengan sus consecuencias jurídicas en el mundo material, existiendo únicamente la tipicidad de delitos tradicionales.

CAPÍTULO IV

4. Convenio sobre la Ciberdelincuencia

El Convenio de Budapest sobre la Ciberdelincuencia es un tratado internacional adoptado por el Consejo de Europa el 23 de noviembre de 2001 y constituye el primer instrumento jurídico internacional que define y aborda específicamente los delitos informáticos estableciendo una serie de medidas para prevenir y combatir los delitos informáticos.

El convenio incluye la armonización de las leyes penales en materia de delitos informáticos, intercambio de información y cooperación entre autoridades, asistencia técnica y la formación en materia de delitos informáticos, así como la sensibilización del público sobre los riesgos de los delitos informáticos.

4.1. Antecedentes

El Convenio de Budapest se abrió a la firma en 2001, siendo un amplio acuerdo internacional sobre ciberdelincuencia que establece obligaciones de derecho penal y procesal sustantivo para armonizar la legislación penal y mejorar la cooperación en las investigaciones que trascienden las fronteras. "Fue el primer tratado internacional destinado a abordar la ciberdelincuencia y constituye el tratado sobre ciberdelincuencia más ampliamente ratificado en la actualidad, con 66 Estados Parte y más de 20 Estados y organizaciones observadores"[48].

[48] Véase en https://www.coe.int/en/web/cybercrime/parties-observers Council of Europe. **Parties/Observers to the Budapest Conveniton and Observer Organisations to the T-CY Versión en español.** (Consultado: 26 de julio de 2023).

Resulta evidente que la crisis propiciada por la pandemia del COVID-19 ha puesto de relieve que la vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. "El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo, los daños económicos por ataques cibernéticos podrían sobrepasar el 1% del Producto Interno Bruto (PIB) en algunos países, y los ataques a la infraestructura crítica, podría alcanzar hasta el 6% del PIB"[49].

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest, es un acuerdo internacional destinado a combatir los ciberdelitos o delitos cometidos por medio del internet, busca establecer una legislación penal y procedimientos comunes entre los países miembros del Consejo de Europa y los invitados a participar en el mismo.

4.2. ¿En qué consiste específicamente el Convenio de Budapest sobre ciberdelincuencia?

De acuerdo a la definición oficial el Convenio de Budapest CETS No. 185, sancionado el 23 de noviembre de 2001 por el Comité de ministros del Consejo de Europa es: El primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de seguridad de la red. También tiene una serie de poderes y procedimientos como la búsqueda de redes informáticas y la intercepción.

El objetivo principal de este tratado es armonizar todas las legislaciones internas para que tipifiquen en un mismo sentido las conductas delictivas y establecer formas eficaces de actuar en conjunto y lograr su sanción y prevención.

---

[49] Centro de Observancia en Seguridad Ciudadana. **La ciberseguridad en Guatemala.** Pág. 1.

El Convenio de Budapest tomando en consideración la emergencia de amenazas cibernéticas y la especificidad de nuevos delitos, este instrumento internacional se compone de cuatro capítulos sobre los cuáles contiene: "a) Terminología, b) medidas que deben adoptarse a nivel nacional, c) cooperación internacional, y d) disposiciones finales. En el que uno de los puntos principales de este texto internacional son las tipificaciones de los ciberdelitos que pueden cometer contra la confidencialidad de los sistemas y datos informáticos e incluso violaciones de los derechos de autor"[50].

A pesar de ser un tratado debatido y redactado en el contexto del Consejo de Europa, con el paso de los años el Convenio de Budapest se ha consolidado como el principal texto legal sobre cooperación internacional con fines de persecución penal y lucha contra los ciberdelitos. En este sentido, es importante señalar que a pesar del tenor punitivo bajo el cual fue elaborado el Convenio de Budapest, su relevancia hoy en día se debe al constante trabajo de actualización y a partir de cierto nivel de interlocución con otras discusiones como las relacionadas con la defensa de los derechos humanos en la era digital.

El Convenio estipula que cada parte deberá adoptar las medidas legislativas y de todo tipo que sean necesarias para tipificar como delito en el derecho interno de cada nación los actos que se encuentran tipificados en el cuerpo legal del convenio, los cuales se detallaran más adelante.

El convenio objeto de estudio regula en su texto disposiciones sobre uniformidad de la terminología en el ámbito de la informática. En lo referente a los delitos informáticos describe elementos tipo a ser tomados en cuenta en las legislaciones propias de los países suscriptores; hace un particular énfasis en la necesidad de perseguir criminalmente delitos tales como la pornografía infantil, fraude informático y delitos contra la propiedad intelectual.

[50] Martins dos Santos, Bruna. **Op. Cit.** Pág. 6.

De igual manera contiene aspectos referentes al proceso penal en ámbitos como la competencia para la persecución de este tipo de ilícitos, acuerdos relacionados a la asistencia jurídica internacional para el juzgamiento y procura de medios de prueba, así como reglas para definir las cuestiones de extradición.

En los últimos años, "el tratado se ha consolidado de hecho como una base legal inicial para la definición de las estructuras de cooperación internacional, así como una guía para la posterior elaboración de legislaciones nacionales"[51].

4.3. Primer Protocolo Adicional

Este se refiere a la incriminación de los actos de carácter racista cometidos a través de sistemas informáticos, y que entró en vigor en el año 2006. El texto elaborado en su mayor parte por un comité de redacción y posteriormente a la evaluación de los estados miembros tiene como principal objetivo "promover la mayor armonización entre legislaciones relevantes en el ámbito del derecho criminal sobre la lucha contra el racismo y la xenofobia en internet"[52].

4.4. Segundo Protocolo Adicional

El segundo Protocolo adicional se refiere a un esfuerzo de actualización de las disposiciones del convenio que es relativamente más reciente, ya que fue adaptado en diciembre del año dos mil veintiuno por los Estados miembros del Comité Europeo.

Surgió de una decisión de la comunidad internacional sobre la necesidad de endurecer las normas, especialmente en lo que se dice respecto a la divulgación de informaciones

[51] **Ibid.** Pág. 6
[52] Martins dos Santos, Bruna. **Ob. Cit.** Pág. 9

de registro de nombres de dominio, medidas de cooperación directa con proveedores de servicios para la obtención de informaciones de usuarios y datos de tráfico.

De acuerdo con los estudios y estadísticas, el segundo protocolo surge como una actualización necesaria para convertir el Convenio de Budapest en un instrumento transfronterizo a los datos y la cooperación legal mutua y establece parámetros más claros para la cooperación directa entre las autoridades y los proveedores de servicios digitales, inclusive en el nivel de los proveedores de servicios de infraestructura de internet. El segundo Protocolo Adicional del Convenio de Budapest viene a complementar respecto a los puntos o conductas que pudieron quedar sin tener una tipificación y sanción por parte de la comunidad internacional.

4.5. Marco Jurídico Internacional sobre el Convenio de Budapest

Desde la aparición de los ciberataques realizados por delincuentes, por el crimen organizado o por terroristas, las naciones y organizaciones han ido reaccionando de forma progresiva para enfrentarse contra esta amenaza global. De esta forma, se han creado estrategias y sistemas de respuesta para garantizar la seguridad de sus ciudadanos y empresas. Así, se han ido modificando y adaptando la legislación de los distintos países y organizaciones.

El marco jurídico legal en países latinoamericanos en materia de ciberdelincuencia ha sido influenciado por el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, acuerdo que establece un marco regulatorio legal internacional común contra la delincuencia cibernética.

Sin embargo la Asamblea General de las Naciones Unidas el 14 de Julio de 2021, el Grupo de Expertos Gubernamentales "sobre la promoción del comportamiento

responsable de los Estados en el Ciberespacio en el contexto de la seguridad internacional, reafirmo que la soberanía de los Estados y las normas y principios internacionales le son aplicables a la realización por los listados de actividades relacionadas con las Tecnologías de la Información y su jurisdicción sobre la infraestructura tecnológica que se halle en su territorio"[53].

Entre los países latinoamericanos y europeos que han tenido avances en sus cuerpos legales internos tenemos:

- España:

¿Cómo rige en España? España firmó el tratado el 23 de noviembre de 2001 y lo ratificó mediante el instrumento de ratificación del convenio el 1 de octubre de 2010 en el que el país se compromete a observarlo y cumplirlo en todas sus partes. Sin embargo, las reformas al ordenamiento penal –derivadas de la ratificación- solo se hicieron realidad hasta el 24 de diciembre de 2010 cuando entró en vigencia la LO 5/2010 de 22 de junio.

Esta reforma fue inspirada en la Decisión Marco 2005/222/J AI, sustituida por la Directiva 2013/40UE que, en cierta forma, impulsó la Reforma al Código Penal Español de 2015 que introdujo Artículos importantes para la tipificación de los diferentes tipos de cibercrimen.

En 2019, España aprobó la Estrategia Nacional de Ciberseguridad, la cual busca "garantizar el uso fiable y seguro del ciberespacio, protegiendo los derechos y libertades de los ciudadanos, y promoviendo el progreso económico".

[53] Centro de Observancia en Seguridad Ciudadana, **La ciberseguridad en Guatemala.** 2.

La lucha del Estado contra la ciberdelincuencia es frontal. Aun así, solo en 2018 se registraron 110.613 ciberdelitos que costaron millones de euros a las víctimas, según cifras del Observatorio Español de Delitos Informáticos.

Además de lo anterior, España "firmó el segundo protocolo adicional al Convenio de Budapest en virtud que su incorporación al ordenamiento español facilitará la investigación y el enjuiciamiento de pruebas electrónicas transnacionales"[54].

- México:

En México como en otros países de América Latina, la adopción del internet sigue creciendo, y en este contexto los riesgos y amenazas también han aumentado en número y frecuencia y han hecho más vulnerables a las personas que llevan a cabo sus actividades en el ciberespacio.

México al igual que Guatemala, solo actúa como Estado observador, habiendo solicitado el país su adhesión en 2006. A pesar de no estar inscrito en el convenio, México tiene un debate interno importante al ser uno de los países con mayor cantidad de ataques cibernéticos, teniendo además un Marco Jurídico propio conformado principalmente por el Código Penal Federal y la Ley de Seguridad Nacional.

Un estudio realizado por RED y Derechos digitales analizó la legislación mexicana y planteó los posibles conflictos con lo estipulado por el Convenio de Budapest, principalmente por la amplia tipificación de los crímenes relacionados a la ciberdelincuencia.

---

[54]https://www.exteriores.gob.es/RepresentacionesPermanentes/ConsejodeEuropa/es/Comunicacion/Noticias/Paginas / Articulos/Espa%C3%B1a-firma-el-Segundo-Protocolo-Adicional-al-Convenio-de-Budapest.aspx.
Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. España firma el segundo protocolo adicional al Convenio de Budapest. (Consultado: 16 de julio de 2023).

En México, en el fuero federal, esto es, en el Código Penal Federal se han tipificado conductas que constituyen delitos informáticos. Lo mismo sucede en el fuero común, algunos códigos de las entidades federativas tipifican ciertos delitos informáticos. Lo cierto es que se requiere de una homologación en la legislación mexicana tratándose de delitos informáticos, ya que como se expone, no todos los delitos informáticos están previstos en el Código Penal Federal ni los códigos penales locales tipifican los mismos delitos informáticos.

Algunos de los delitos tipificados en México, en los cuales se emplean los sistemas informáticos, electrónicos, Internet, computadoras, programas informáticos como medio o como fin se encuentran: la revelación de secretos, el acceso ilícito a sistemas y equipos informáticos, el acoso sexual, el engaño telefónico, la extorsión telefónica, falsificación de títulos, pornografía, suplantación de identidad, entre otros. Otros delitos en cuya comisión se emplean las Tecnologías de la Información y la Comunicación son el delito de fraude, el robo, el delito equiparado al fraude, entre otros.

Además, tratándose de delitos informáticos, como sucede con el resto de los delitos, existe la posibilidad que con una sola acción se cometan diversos delitos o que un delito sea cometido a través de diversas conductas y entonces estaremos frente a un concurso de delitos.

En México, algunas leyes especiales, prevén delitos informáticos especiales, tal es el caso de los delitos previstos en las leyes del sistema financiero mexicano, por ejemplo, el acceso ilícito a sistemas y equipos informáticos por funcionarios, empleados, servidores de las instituciones que integran el sistema financiero mexicano, para modificar, copiar, destruir información contenida en esos sistemas y equipos.

La violencia digital, conocida también como ciber violencia se refiere a aquellas conductas o acciones que se ejecutan a través de los medios digitales y que atentan

contra la intimidad sexual, la integridad, la dignidad y la vida privada de las personas, causándoles un daño sexual, moral, psicológico o económico.

Las conductas que constituyen violencia digital son:

- Grabar videos, audios, o tomar fotografías reales o simuladas de contenido sexual íntimo de una persona sin su consentimiento y mediante engaños.
- Exponer, distribuir, difundir, exhibir, reproducir, transmitir, comercializar, ofertar, intercambiar y compartir videos, audios, fotografías de contenido sexual íntimo de una persona, sin su consentimiento, a través de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.

- Argentina

La adhesión de Argentina al Convenio "se llevó a cabo incluso ante las advertencias de la sociedad civil y el mundo académico sobre la amplitud y ambigüedad del texto y sus consideraciones sobre los riesgos que suponía para las actividades de investigación en seguridad informática desarrolladas en el país"[55].

En Argentina, según datos de la Dirección Nacional de Ciberseguridad, los delitos informáticos de 2021 aumentaron en un 160% en comparación a los ocurridos en 2020. De los 591 incidentes, más de 331 (56%) fueron relacionados a fraude informático.

A pesar de las advertencias, Argentina ratificó el acuerdo en junio de 2018. En noviembre de 2017 fue publicada la Ley 27.411, que aprobó las observaciones del Convenio de Budapest, no obstante, descartó algunas de las disposiciones del tratado debido a posibles discrepancias con los Artículos de la legislación nacional, siendo los Artículos excluidos relativos principalmente a cuestiones jurisdiccionales y pornografía infantil.

[55] https://www.infobae.com/tecno/2018/05/13/ argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/ Infobae. Argentina se suma a la Convención de Budapest para tratar delitos informáticos.Consultado: 28 de julio de 2023).

El país ha informado de su participación activa en el Comité T-CY y ha celebrado la adopción del 2º Protocolo Adicional al Convenio de Budapest afirmando que "Para prevenir y perseguir el delito cibernético es fundamental contar con mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia internacional"[56].

En resumen, Argentina es país parte del Convenio, se adhirió y ratificó el convenio, la Ley creada que integra los delitos del Convenio de Budapest presentó reservas a algunas disposiciones mayormente con las medidas relativas a pornografía infantil.

- Chile:

Chile se integró al Convenio de Budapest en abril de 2017, unos días después fue publicado el Decreto 83, promulgando referido convenio. El documento del país en el convenio presentó reservas, dejando de lado disposiciones relacionadas a la aplicación de la ley nacional, cuestiones jurisdiccionales y pornografía infantil. El reglamento chileno sobre ciberdelincuencia se actualizó para adecuar la norma e instituciones a lo indicado por el Convenio de Budapest.

"La necesidad de reforzar el compromiso asumido a nivel nacional para garantizar la seguridad cibernética en el país (a través de la Política Nacional de Ciberseguridad) y de formar parte de un sistema rápido y eficaz de cooperación internacional, así como de establecer canales de intercambio de conocimientos sobre la lucha contra los crímenes cibernéticos son algunas de las principales razones alegadas por el Gobierno chileno para adherirse al tratado"[57].

Respecto a las reservas presentadas, cabe mencionar que en el caso chileno el documento de acceso al Convenio de Budapest depositado en el Consejo de Europa

[56] Martins dos Santos, Bruna. **Ob. Cit.** Pág 24
[57] **Ibid.** Pág. 24-25

dejó fuera, disposiciones relacionadas en su mayoría con medidas relativas a la posibilidad de aplicación de la ley nacional, pornografía infantil y cuestiones jurisdicción.

En chile según datos de la cuenta pública PDI 2022, "entre 2020 y 2021 los delitos informáticos aumentaron en un 8,2% y las denuncias relacionadas a pornografía infantil 22,8%. Por otra parte, los detenidos por crímenes informáticos alcanzaron un total de 11 en 2021, aumentando considerablemente los 2 de 2020"[58].

- Colombia

En Colombia, la primera figura delictiva informática fue consagrada en el Código Penal del 2000 en su Artículo 195 y fue denominada acceso abusivo a sistema informático protegido con medida de seguridad, ello a partir de la Convención de Budapest del 2001.

El Centro Cibernético Policial reportó en 2022 un alza de 17% en las denuncias por delitos informáticos, entre los más comunes destacan el *grooming, ciberbullying* y distribución de pornografía infantil.

La integración de Colombia en el tratado fue justificada con la creciente ola de delitos cibernéticos producto de la pandemia, además de las críticas que venían desde 2018 para tener una legislación más completa. La legislación colombiana no integró el Artículo 20 y 21, los que se refieren a la intercepción y recolección de datos.

En mayo de 2022 el gobierno colombiano emitió el Decreto 338, relacionado a seguridad digital. En el decreto se busca fortalecer la gobernanza y penalización de delitos

[58] https://idealex.press/el-convenio-de-budapest-y-la-ciberseguridad-en-america-latina/ Idealex Press. **El Convenio de Budapest y la Ciberseguridad en América Latina** (Consultado: 10 de agosto de 2023).

cibernéticos, materializando los esfuerzos estatales contra la ciberdelincuencia en sus proyectos como la disponibilidad de sistemas y servicios informáticos, pretendiendo acercar a los usuarios al entorno digital.

En el caso colombiano, la discusión y elaboración de políticas públicas para temas relacionados a crímenes cibernéticos han favorecido perspectivas relacionadas con la defensa y seguridad cibernética y apuntan a facilitar el uso de la información en los procesos judiciales y a prevenir o anticipar la consumación de crímenes cibernéticos. de Budapest sobre la Ciberdelincuencia.

La facilitación de investigación de ciberdelitos de carácter transnacional a través de la formalización de canales de intercambio de información entre los países firmantes del Convenio han "sumado a la posibilidad de acceso a los proyectos y programas de acceso y transferencia de conocimiento sobre los temas del Convenio fueron algunos de los otros beneficios alegados por el gobierno colombiano"[59].

- Brasil

Brasil se integró al convenio en noviembre de 2022, a pesar de ser un país incorporado hace pocos meses, debatía su adhesión desde el 2019, año en el que fue invitado, a pesar de ser, desde hace más de 20 años, una demanda de sectores como Ministerios, agencias gubernamentales, el Ministerio Público federal y una parte del Congreso Nacional.

La discusión sobre ciberseguridad es un conflicto en Brasil desde principios de siglo, el país ha tenido múltiples proyectos de ley para tipificar los delitos informáticos, en 2011 se dio la publicación del Marco Civil de Internet, el que se mantuvo como la legislación principal en ciberdelincuencia. En diciembre de 2021 se publicó el Decreto Legislativo

[59] Martins dos Santos, Bruna. **Ob. Cit.** Pág 28-29

número 37 de 2021, que incorporaba la normativa del Convenio de Budapest a la legislación brasileña, a diferencia de Argentina, Brasil no excluyó especificaciones del tratado.

"Las discusiones en torno al tema han estado bastante presentes en el escenario legislativo brasileño y anteceden a la aprobación de leyes clave sobre el ámbito digital promulgadas en el país como el Marco Civil de Internet y la Ley General de Protección de Datos Personales, así como algunas leyes ordinarias que implicaron cambios en el Código Penal brasileño para incluir tipificaciones sobre delitos cibernéticos"[60].

En Centro América los Países que han tenido avances con legislar en cuánto a delitos cibernéticos son los siguientes[61]:

- Costa Rica:

Es uno de los países pioneros en la protección y tratamiento de los datos personales de sus habitantes a nivel centroamericano ello mediante la Ley No. 8968 "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales del año 2011, además de legislar sobre diversos mecanismos de protección a los datos personales se crea el órgano rector siendo la Agencia de Protección de Datos de los Habitantes, además cuenta desde el año 2017 con una Estrategia Nacional de Ciberseguridad, contando también con un Ministerio de Ciencia y Tecnología. En el año 2010 se creó la Comisión Nacional de Seguridad en Línea. Producto de sus múltiples iniciativas contra la ciberdelincuencia, Costa Rica se convierte en el segundo país de Centroamérica en adherirse al Convenio de Budapest en el año 2017.

Los delitos cibernéticos están tipificados en la Ley No. 9048 de Delitos Informáticos y conexos que reforma el título VI del Código Penal, esta ley busca mejorar la lucha contra

[60] Martins dos Santos, Bruna. **Op Cit.** Pág 19
[61] IPANDETEC. **Ob. Cit.** Pág. 12

la ciberdelincuencia y protege los actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, así como datos personales, la identidad y los derechos de los niños y niñas.

Costa Rica tiene un "capítulo de la Sociedad en Internet, donde tanto la academia, miembros de empresa privada, servidores públicos y otros ciudadanos pueden generar intercambio de opiniones en favor de la ciberseguridad de la nación"[62].

- El Salvador

El País es poseedor de un equipo en el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información, que es parte del Ministerio de Justicia y Seguridad Pública. No cuenta con una estrategia nacional de ciberseguridad, tampoco cuenta con una legislación que proteja los datos personales, se ha discutido una propuesta de Ley para proteger los datos de los ciudadanos y encargar a la Defensoría del Consumidor como ente rector.

El país cuenta con un viceministerio dedicado a la ciencia y a la tecnología, bajo el organigrama del Ministerio de Educación. Las autoridades salvadoreñas han planteado su intención de adherirse al Convenio de Budapest, sus parlamentarios se comprometieron a poner en primer lugar de sus agendas la adhesión al Convenio y legislar por la adaptación de las leyes nacionales a los estándares internacionales.

La Asamblea Nacional salvadoreña aprobó en el año 2016 una Ley especial contra los delitos informáticos y conexos. Esta ley tipifica distintos delitos como el acceso indebido a sistemas informáticos. La fiscalía General de El Salvador "tiene personal especializado para responder e investigar hechos que ocurren en la Ley"[63].

---

[62] **Ibid.** Pág 12.
[63] **Ibid.** Pág 16

El Estado de El Salvador cuenta con una política de ciberseguridad 2020-2030 cuyo objetivo principal es "establecer las líneas de acción y estratégicas que permitan definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, la gobernanza, desarrollo de las capacidades de ciberseguridad enfocadas en el aseguramiento de las infraestructuras, fortalecimiento de los mecanismos de respuesta ante incidentes y el desarrollo de habilidades técnicas y de gestión"[64].

- Honduras

Honduras a la fecha no cuenta con un equipo nacional de ciberseguridad que defienda a la población de la ciberdelincuencia, no cuenta con una política nacional cibernética que les permita asegurar el espacio cibernético en su país, actualmente no existe una ley vigente que regule la protección de datos personales, no obstante, ha hecho esfuerzo presentando proyectos de ley que se encuentran en procesos de debate.

Honduras no es signatario del Convenio de Budapest, sin embargo, recientemente congresistas están a la espera de la aprobación de una ley de ciberseguridad y recomendaron la adhesión al convenio. Honduras tiene una fiscalía Especializada para la protección de Propiedad Industrial y Seguridad Informática, encargada de realizar investigaciones y formular cargos a quienes se presuman haya quebrantado la ley penal[65].

- Nicaragua

Actualmente no cuenta con un equipo de respuesta a ataques cibernéticos, hasta la fecha no ha desarrollado estrategia alguna de ciberseguridad nacional, únicamente el Concejo nicaragüense de Ciencia y Tecnología y la Comisión de Gobierno Electrónico

[64] https://derechoynegocios.net/desafios-de-la-ciberseguridad-en-el-salvador-y-la-necesidad-de-suscripcion-del--convenio-de-budapest/ Alas Karla. **Desafíos de la Ciberseguridad en El Salvador y la necesidad de la suscripción del Convenio de Budapest.** (Consultado: 20 de agosto de 2023).
[65] IPANDETEC. **Ob. Cit.** Pág. 23

de Nicaragua son las principales instituciones del Estado que impulsan la seguridad digital y la prevención del flagelo del ciberdelito.

Nicaragua no es signatario de convenios o tratados internacionales contra la ciberdelincuencia, en su ordenamiento jurídico legal no están los delitos cibernéticos debidamente tipificados, pero existen otras figuras en Nicaragua que tratan de regular la materia.

Nicaragua no cuenta con tribunales o agencias de investigación especializada en informática, el Ministerio Público de Nicaragua es el ente encargado de investigar los supuestos delitos que suceden en el país.

- Panamá

El país cuenta con un equipo de expertos en respuesta a incidentes o ataques de expertos, creado en el año 2011 por el Ministerio de la Presidencia bajo la supervisión de la Autoridad Nacional para la Innovación Gubernamental.

El decreto ejecutivo número setecientos nueve del veintiséis de septiembre del año dos mil once crea el CSIRT Panamá, el equipo nacional de respuesta a incidentes de seguridad de la información del Estado Panameño. En el 2013 se apruebe la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas Panamá no cuenta con un ministerio TIC.

La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre del año 2013. Panamá aprobó el texto del Convenio sin reservas ni modificaciones y depositó el instrumento de adhesión en marzo del año 2014. El Ministerio Público de Panamá es el ente investigador, cuenta con una fiscalía de propiedad intelectual y seguridad informática, actualmente no existe juzgados informáticos.

Cooperación en Justicia -REMJA- OEA

Las Reuniones de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas (REMJA) es el principal foro político y técnico en materia de justicia y cooperación jurídica internacional de la OEA con sus Estados Miembro. Entre sus funciones tiene las siguientes:

- Intercambiar información y experiencias para coordinar políticas públicas, consolidar y fortalecer la cooperación entre países
- Recomendar a los Estados miembros acciones para que la cooperación y las políticas públicas sean más eficaces
- Crear grupos de trabajo para hacer el seguimiento de las recomendaciones de la REMJA en materia penal y delitos cibernéticos.
- Fortalecer la coordinación entre la REMJA y otros procesos de cooperación internacional.

4.6. Delitos y sanciones reguladas en el Convenio sobre la Ciberdelincuencia

En virtud de lo investigado en el presente trabajo académico de investigación, es menester indicar la división de los Artículos que se encuentran en el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, estando estructurado de la siguiente forma:

En el capítulo primero se encuentra la terminología, siendo el Artículo 1 las definiciones para los efectos del presente convenio.

En el capítulo segundo se encuentran las medidas que deben ser adoptadas a nivel nacional por los estados parte o los estados que se encuentran en calidad de

observadores, pero para ser reconocidos en su calidad deben de legislar para poder cambiar su estatus.

En este capítulo del convenio se empiezan a observar los primeros ciberdelitos regulados por ese cuerpo legal internacional, siendo los siguientes: acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, infracciones relativas a la pornografía infantil, infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

En los Artículos 11, 12 y 13 pertenecientes al título 5 del Convenio se establecen otras formas de responsabilidad y sanción, identificando la tentativa y complicidad, determinando la responsabilidad de las personas jurídicas y estableciendo las sanciones y medidas.

La sección dos del Convenio sobre la Ciberdelincuencia hace referencia al Derecho Procesal, teniendo en su Artículo 14 el ámbito de aplicación de las medidas de derecho procesal, en su Artículo 15 las condiciones y garantías.

En su Artículo 22 determina la competencia de aplicabilidad, el Artículo 23 establece los principios generales relativos a la cooperación internacional de los estados firmantes del gobierno, el Artículo 24 establece lo relativo a la extradición siendo la sanción principal para el delincuente que comete los delitos establecidos en el presente convenio.

El Convenio sobre la ciberdelincuencia reúne 48 Artículos, cuatro capítulos, y dos secciones.

CAPÍTULO V:

5. Enfoque Jurídico del Incumplimiento del Estado al no adoptar el Convenio de Budapest que establece los delitos sobre la ciberdelincuencia en el derecho penal

Derivado a los avances de las tecnologías de la información, la comunidad internacional ha creado por medio de la cooperación una serie de tipos penales y mecanismos que protegen a los ciudadanos de las diferentes sociedades y sancionan las conductas delictivas que se materializan por medios o dispositivos informáticos en los que sus consecuencias jurídicas trascienden al mundo real, siendo esto mediante el Convenio de Budapest, convención a la que actualmente se han adherido varios países del continente europeo no quedando fuera gran parte de países de América Latina.

La República de Guatemala al no adoptar en su ordenamiento jurídico los delitos contenidos en el Convenio sobre la Ciberdelincuencia, así como las sanciones establecidas, deja en estado de indefensión a los ciudadanos guatemaltecos, sin una vía de mecanismo para la restitución de sus derechos vulnerados o de su identidad suplantada por ciberdelincuentes, lo que en la actualidad constituye uno de los problemas más difíciles e importantes de las naciones del mundo toda vez que las Tecnologías de la Información avanzan día con día.

5.1. Generalidades:

El auge de los peligros en los que se ve expuesto el ser humano al hacer uso de las tecnologías de la información es cada vez más alarmante, países en América Latina, posterior al confinamiento aumentaron considerablemente las denuncias por delitos relacionados a la ciberdelincuencia, ello en virtud que migraron la mayoría de sus actividades al mundo digital, no siendo caso aparte Guatemala. Sin embargo, no solo

estos años fundamentan la necesidad de un país de unirse al convenio, sino más bien es debido al historial delictual en estas materias, el que crece exponencialmente desde inicios del siglo veintiuno.

En la población de cada sociedad, las actividades diarias se dan con gran participación mediante las Tecnologías de la Información y la Comunicación toda vez que han facilitado la forma de realizar tareas cotidianas.

El concepto de Tecnologías de la Información y la Comunicación se refiere al conjunto de herramientas que permiten la transmisión, el procesamiento y el almacenamiento de información. En este concepto se encuentran las computadoras y los elementos que la integran como los programas de cómputo *software* y el *hardware*; los teléfonos inteligentes; las tabletas; las redes como Internet; sistemas informáticos y otros.

Las *TICs* se emplean para ejecutar actividades cotidianas de trabajo, educación, entretenimiento, transacciones comerciales, financieras, etcétera, y son usadas por un gran número de individuos, desde menores de edad hasta personas de la tercera edad, así como por las empresas y el gobierno. Desafortunadamente estas herramientas también son objeto e instrumento de conductas ilícitas que causan afectación a otras personas físicas o morales, y a sus patrimonios. De ahí surge la necesidad de sancionar estas conductas, dando lugar a una clase más de delitos, los delitos informáticos que también han sido llamados ciberdelitos o delitos cibernéticos.

Los delitos informáticos se definen como aquellos actos ilícitos en los que se usan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, el Internet, entre otros, como medio o como fin. Por ejemplo, un programa de cómputo será un medio para cometer un delito cuando es utilizado para acceder sin autorización a información confidencial; ahora bien, un programa de cómputo

será el fin en un delito informático cuando recaiga sobre ese programa la conducta delictiva, como cuando se insertan virus para destruir el programa.

La tipificación de los delitos informáticos, su prevención, asistencia técnica, y combate es una tarea compleja para los países.

La Organización de las Naciones Unidas ha considerado que los delitos informáticos implican grandes retos para todos los Estados, toda vez que tienen lugar en el ciberespacio, y los delincuentes y las víctimas pueden encontrarse en cualquier parte del mundo.

Los países en las últimas décadas han incluido en sus legislaciones a los delitos informáticos y han considerado que estos delitos pueden atentar contra: la confidencialidad de la información, los sistemas informáticos, la propiedad intelectual, la integridad e intimidad de las personas, el patrimonio, y otros.

El objetivo principal de este instrumento, es establecer una política penal común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia, Esto se alcanza tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales y a través de una cooperación internacional armónica.

En la práctica, es el único instrumento internacional vinculante sobre este tema. Y pretende ser una guía para que los países desarrollen legislaciones nacionales integrales y alineadas contra el Ciber crimen, además, facilita la adopción de medidas para detectar y perseguir, nacional e internacionalmente, a los ciber delincuentes.

Se creó para ello una red 24/7 para garantizar una rápida cooperación internacional que reaccione frente a cualquier incidente y facilite la extradición de criminales cibernéticos.

Es el primer tratado internacional, aprobado por el Consejo de Europa en el año 2001, y, busca armonizar y coordinar los esfuerzos de las naciones para hacer frente a los delitos informáticos, instándolas a que aprueben las correspondientes legislaciones en sus países para que tipifiquen dichos delitos.

Este convenio cuenta en la actualidad con 65 miembros y trata en particular sobre las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de la seguridad en redes.

5.2. Antecedentes de la integración de Guatemala

En Guatemala se han dado los flagelos por medios electrónicos desde muchos años atrás, no obstante, es hasta el acaecimiento de la emergencia sanitaria mundial que se empieza a dar una mayor relevancia a esta situación.

De acuerdo al reporte del año 2020 del BID y la OEA, "Ciberseguridad. Riesgos y Avances y el camino a Seguir en América Latina y el Caribe" a medida que los Estados se vuelven cada vez más dependientes de las Tecnologías de la Información, es esencial que se observe un marco común de comportamiento estatal responsable en el contexto de la seguridad internacional.

En Guatemala, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales. Actualmente no existe una entidad que coordine a nivel nacional la política de prevención y respuesta a incidentes cibernéticos.

En el caso de Guatemala, se solicitó adherirse a este convenio en el año 2016 y para ello, según las fuentes consultadas, se han presentado en el Congreso de la República las siguientes iniciativas de ley:

"La primera en 2017 Iniciativa 5254, que trató sobre la Ley de ciberdelincuencia, dispone aprobar Ley Contra la Ciberdelincuencia, y su presentación al pleno el nueve de marzo, mientras que, en el año 2018, se presentó la iniciativa 5239, Ley contra actos terroristas, y dispone aprobar Ley Contra Actos Terroristas. (Capítulo 8 –Terrorismo Cibernéticos Medios de Comunicación), Dictamen de Comisión, Favorable del 6 de noviembre de ese año, y en 2019 se presentó la iniciativa 5601, Ley de Prevención y Protección contra la Ciberdelincuencia, que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia, dictamen favorable con Modificaciones del 18 de noviembre del año pasado"[66].

5.3. Guatemala como país observador

No obstante que el Convenio de Budapest fue celebrado a nivel del Consejo de Europa, no existe ningún impedimento legal para que otros países, como el caso de Guatemala, puedan adherirse a dicha normativa. Al contrario, tanto para Europa como para los países de América Latina y todos los países del mundo, la normativa se convierte en derecho positivo cuanto mayor sea el número de países que se adhieran a la misma.

Ejemplo de ello ha sido la ratificación, por parte del senado de Estados Unidos, en el mes de agosto del año dos mil seis. Así también, la Cámara de Diputados de México ha exhortado, a su organismo Ejecutivo, para que se adhiera formalmente al Convenio de Budapest. Argentina, al igual que otros países de América Latina, actualmente se encuentra en el procedimiento previo a la adhesión a la Convención.

La penetración de las redes informáticas trajo consigo los ciberataques que hoy, de acuerdo con el Informe de Riesgos Mundiales del 2019 se encuentran entre las amenazas globales más graves del planeta, junto a los fenómenos meteorológicos extremos, el fracaso de la protección climática y los desastres naturales. De ahí que

[66] https://mingob.gob.gt/guatemala-accede-al-convenio-sobre-ciberdelincuencia-de-budapest/ Ministerio de Gobernación de Guatemala. **Guatemala accede al convenio sobre ciberdelincuencia de Budapest.** (Consultado 25 de septiembre de 2023).

el concepto de ciberdelincuencia se convirtiera en una preocupación para los gobiernos de todo el mundo y se firmara el Convenio de Budapest sobre ciberdelincuencia para hacerle frente de forma eficaz.

Se desprende de la investigación realizada en el presente trabajo, que Guatemala ha sido invitado por la comunidad internacional para que forme parte de los países signatarios del presente convenio, no obstante, aceptando ser un país observador del convenio y comprometiéndose para realizar la integración del mismo al ordenamiento jurídico guatemalteco vigente, no se han generado avances en relación al tema.

Sin un marco legal adecuado y con un decreto que ha causado controversia, el tema del ciberdelito en Guatemala tendría que llevarse al diálogo y buscar la cooperación entre países. Guatemala no cuenta con un marco legal apropiado para enfrentarse a los ciberdelitos, los delitos contenidos en el Código Penal ya no se amoldan a la realidad actual de la población guatemalteca.

5.4. Marco jurídico sobre la ciberdelincuencia en Guatemala

En Guatemala actualmente no existe un marco legal para la tipificación o encuadramiento del ciberdelito, lo que complejiza su abordaje y medición en el país. Derivado de la crisis sanitaria mundial se registró un incremento en los ciberdelitos a nivel mundial, ante este hecho las personas se volvieron más vulnerables derivado que migraron la mayoría de sus actividades al mundo digital, lo que posibilitó el acceso a ciberdelincuentes a realizar flagelos en la vida de cada uno de los usuarios.

A la fecha se sigue trabajando en reforzar los sistemas informáticos del Ministerio de Relaciones Exteriores, con la ayuda de asesoría nacional e internacional, por lo que se cuenta con mayores medidas de seguridad para la protección de la infraestructura tecnológica. Asimismo, seguiremos trabajando en la adhesión de Guatemala al Convenio

de Budapest, el cual establece una política penal orientada a la protección contra la ciberdelincuencia.

Según estadísticas, las mujeres son las principales víctimas del ciberdelito, principalmente en el uso de las redes sociales, siendo los delitos como el ciberacoso, sexting y pornovenganza. En el mes de Marzo del año 2021 se presentó una iniciativa de ley con reformas al código penal, en relación a los delitos cometidos en contra de la niñez y adolescencia a través de medios tecnológicos y ninguna ha sido aprobada por lo que no aún no se cuenta con una normativa respecto al tema, lo que dificulta tener una sanción para estos tipos delictivos que se han convertido en flagelos muy comunes en la actualidad, siendo un claro tipo de negligencia por parte del Estado de Guatemala que tiene la obligación de velar por la seguridad de sus ciudadanos y no exponerlos a sufrir vejámenes que han surgido junto con la evolución de las tecnologías.

Durante el año 2018, el Ministerio de Gobernación aprobó y publicó la Estrategia Nacional de Seguridad Cibernética la cual tiene como su principal objeto el "Fortalecer las capacidades de la Nación creando el ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y ejercicio de los derechos de las personas en el ciberespacio", teniendo cuatro ejes para su ejecución siendo estos los siguientes:

1. Marcos Legales
2. Educación
3. Cultura y Sociedad
4. Tecnologías de Información

En la República de Guatemala existe un observatorio guatemalteco de delitos informáticos que compila información de las fuentes como el Ministerio Público, Policía Nacional Civil y la Superintendencia de Bancos y realiza análisis y encuestas respecto al tema.

Según la Superintendencia de Telecomunicaciones en Guatemala, para el año 2020 se han reportado veinte millones de usuarios de telefonía móvil con más de una suscripción por persona y tomando en cuenta que más de la mitad de los guatemaltecos tienen un celular con posible acceso a internet es importante dimensionar todos los actos ilegales que se pueden estar cometiendo por el medio tecnológico y de las telecomunicaciones. Para poder entender como en la República de Guatemala se aborda el tema sobre la ciberdelincuencia o cibercriminalidad, es necesario que se realicen algunas preguntas[67]:

1. **¿Cuenta el país actualmente con un equipo de respuesta a ataques cibernéticos?**

Actualmente Guatemala no cuenta con ningún equipo de carácter estatal para enfrentar los ataques cibernéticos.

2. **¿Cuenta el país con una estrategia de ciberseguridad?**

Si, el país cuenta con una Estrategia Nacional de Seguridad Cibernética, que data del año 2018.

3. **¿Cuenta el país con una legislación que proteja los datos personales?**

Actualmente en Guatemala se han presentado en el Congreso de la República tres iniciativas de Ley siendo estas las siguientes:

Ley de ciberdelincuencia en el año 2017.
Ley contra actos terroristas en el año 2018.
Ley de Prevención y Protección contra la ciberdelincuencia en el año 2019.

[67] IPANDETEC. **Op. Cit.** Pág. 17

En el año 2009 se presentó en el Congreso de la República la Iniciativa 4090 que dispone aprobar la Ley de Protección de Datos Personales, la que actualmente posee dictamen favorable se encuentra pendiente del tercer debate y aprobación final por el Pleno del Congreso.

El Decreto 57-2008 del Congreso de la República la Ley de Acceso a la Información Pública, siendo actualmente la única que regula lo referente a los datos personales y datos sensibles, así como establecer un mecanismo de protección de datos y tipifica delitos en la materia.

4. ¿Cuenta el país con una agencia o ministerio de gobierno especializado en tecnologías de la información?

Si, el Ministerio de Gobernación por medio del cuarto Viceministerio de Tecnologías de Información y Comunicaciones es el ente gubernamental especializado en tecnologías de la información.

5. ¿Participa el país en foros o encuentros regionales multisectoriales en materia de ciberseguridad?

Si, Guatemala es miembro del Foro Mundial de Ciber Expertos. El Viceministerio de Tecnología del Ministerio del Interior representa al País ante este organismo. El GFCE es una plataforma global para países, organizaciones internacionales y empresas privadas intercambien mejores prácticas y experiencia en el desarrollo de capacidades cibernéticas. El objetivo es identificar políticas, prácticas e ideas exitosas y multiplicarlas a nivel global.

Guatemala, por medio de su gobierno, acude y es representado anualmente en el Foro de Gobernanza de Internet que la Organización de Naciones Unidas realiza anualmente.

Este foro a su vez tiene iniciativas regionales y nacionales, siendo celebrado cada año el Foro de Gobernanza de Internet de Guatemala y el *Latin American and the Caribbean Internet Governance Forum.*

Guatemala además, pertenece al *FOPREL*, por lo que recientemente se reunieron con representantes de *GLACY*, reunión que tuvo por objeto intercambio de ideas, el análisis de las ventajas de adherirse al Convenio de Budapest.

6. ¿Cuenta el país con una legislación conexa que regule la materia?

El Código Penal, decreto 17-73 establece en su Artículo 274 de la literal "A" a la "H", se encuentra tipificado el delito de destrucción de registros informáticos, alteración de programas, reproducción de instrumentos o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos, entre otros. La ley contra la violencia sexual, explotación y trata de personas contempla que ciertos delitos sobre indemnidad sexual puedan ser utilizados medios incluyendo tecnológicos para ubicar o comunicarse con la víctima.

7. ¿Cuenta el país con grupos de trabajo multisectoriales que trabajen en ciberseguridad?

Guatemala tiene un capítulo de la Sociedad de Internet donde tanto la academia, miembros de la empresa privada, servidores públicos, entre otros ciudadanos pueden generar intercambios de opiniones a favor de la ciberseguridad de la nación.

El Observatorio sobre Ciberseguridad Global, un Grupo de Interés Especial de la Internet *Society* fue fundada para desarrollar los mecanismos adecuados de participación, la colaboración y el diálogo para proponer cómo construir la confianza, prosperidad y seguridad en internet, y equilibrar las cuestiones de seguridad nacional con los derechos

humanos y fundamentales tales como la privacidad, libertad de expresión y permitir la innovación para fomentar el despliegue de tecnologías emergentes bajo las más estrictas normas de privacidad, protección de datos y seguridad.

8. ¿Están los delitos cibernéticos debidamente tipificados en la legislación penal?

Actualmente el Código Penal Decreto 17-33 es el único antecedente que tipifica algunos delitos informáticos como la destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación. El delito de pornografía infantil, no está incluido como un delito cibernético sino dentro de la ley contra la violencia sexual, explotación y trata de personas.

9. ¿Cuenta el país con tribunales o agencias de investigación especializadas en informática?

No existen tribunales especializados, sin embargo, el Ministerio Público cuenta con la Dirección de Investigaciones Criminalísticas y de técnicos informáticos especializados para procesar las evidencias digitales. La policía nacional civil cuenta con un departamento especializado para brindar apoyo al Ministerio Público al momento de realizar las investigaciones sobre posibles delitos informáticos.

5.5. Iniciativas de Ley presentadas:

Actualmente en Guatemala se han presentado en el Congreso de la República tres iniciativas de Ley siendo estas las siguientes:

1. Ley de ciberdelincuencia en el año 2017.
2. Ley contra actos terroristas en el año 2018.
3. Ley de Prevención y Protección contra la ciberdelincuencia en el año 2019.

En el año 2009 se presentó en el Congreso de la República la Iniciativa 4090 que dispone aprobar la Ley de Protección de Datos Personales, la que actualmente posee dictamen favorable se encuentra pendiente del tercer debate y aprobación final por el Pleno del Congreso.

El Decreto 57-2008 del Congreso de la República la Ley de Acceso a la Información Pública, siendo actualmente la única que regula lo referente a los datos personales y datos sensibles, así como establecer un mecanismo de protección de datos y tipifica delitos en la materia.

5.6. Enfoque jurídico del incumplimiento del estado al no adoptar el Convenio de Budapest que establece los delitos sobre la ciberdelincuencia en el derecho penal

Deriva pues que del estudio efectuado en el presente trabajo de investigación se logra establecer que la República de Guatemala, siendo un país de América Latina rico en recursos naturales, así como en una diversidad de cultura, con una cantidad de población considerable, que participa activamente ante la comunidad internacional y que se encuentra actualmente como país observador de la Convención sobre la Ciberdelincuencia o Convenio de Budapest, no ha legislado respecto al tema para poder de esta forma resguardar los derechos humanos de su población.

A pesar que la cantidad de delitos establecidos en el Convenio sobre la Ciberdelincuencia no resulta en una enorme lista para modificar el ordenamiento jurídico actual de la República de Guatemala, como país se ha quedado atrás, pues no existe un marco legal para la tipificación del ciberdelito, lo que complejiza su abordaje y medición en el país.

En el punto máximo de crisis de la pandemia del Covid-19 se registró un incremento en los ciberdelitos en la República de Guatemala, esto de conformidad con los Artículos de

investigación publicados en los periódicos de circulación nacional por investigaciones realizadas por instituciones de seguridad digital como lo es *Kaspersky*. En 2022, Guatemala fue el país con más amenazas cibernéticas en la región, especialmente las amenazas financieras y las estafas conocidas como *"phishing".*

"En los últimos ocho meses, en América Latina, se reportaron 38 millones de ataques, que figuran a 110 ataques por minuto. Del 2020 al 2022 creció el número de casos de *phishing* debido a que el tiempo que pasamos frente a las pantallas aumentó debido a la pandemia. En Guatemala hubo un incremento del 188 por ciento hasta agosto de este año. Es el país de Latinoamérica que tuvo más ciberamenazas de este tipo"[68].

En el devenir histórico actual muchos han sido los acontecimientos históricos a los que hemos estados expuestos actualmente, los ciberataques se han incrementado en el país derivado de la pandemia y del conflicto entre Rusia-Ucrania. Lo que persiguen los delincuentes son los datos de las personas y los ponen a disposición de alguien que quiere obtener un crédito, siendo este el caso más común que se ha dado e informado en el sistema bancario de Guatemala.

"El sector financiero es el más atacado a nivel global. Según estadísticas el **55% de los ataques cibernéticos** están dirigidos al sector financiero porque los atacantes buscan un crédito económico" explica Sandra Lemus, Oficial de Ciber resiliencia y Seguridad de la Información de la SIB.

Agrega que l**os ataques cibernéticos son todos aquellos intentos de perpetrar infraestructura e información y valerse de esta información para hacer un daño a un cuentahabiente o a una institución financiera.**

---

[68] Jumique Castillo, Andrea. **Prensa Libre.** Sección Tecnología. Guatemala, Guatemala, **Ataques de *malware* y *phishing*, los ciberataques que más aumentaron en el 2022 en Guatemala.** Pág. 45 (30 de diciembre 2022).

Guatemala al no adoptar en su ordenamiento jurídico los delitos contenidos en el Convenio sobre la Ciberdelincuencia, así como las sanciones establecidas siendo principalmente la extradición con los países de la comunidad internacional, deja en estado de indefensión a los ciudadanos guatemaltecos, sin una vía de mecanismo para la restitución de sus derechos vulnerados o de su identidad suplantada por ciberdelincuentes, lo que en la actualidad constituye uno de los problemas más difíciles e importantes de luchar de las naciones del mundo toda vez que las Tecnologías de la Información avanzan día con día, por lo que la ciencia del derecho deberá ir de la mano de estos avances evolucionando para poder salvaguardar los derechos o restituir los ya conculcados de los usuarios del internet.

CONCLUSIÓN DISCURSIVA

El andamiaje jurídico guatemalteco regula en el Código Penal algunos delitos que pueden ser realizados con apoyo de herramientas de uso digital, no obstante el Estado de Guatemala no ha cumplido con su mandato constitucional contenido en el Artículo 2 de la Constitución Política de la República de Guatemala, específicamente sobre brindar seguridad a sus ciudadanos, toda vez que al no observar los delitos contenidos en el Convenio de Budapest e integrarlos al andamiaje jurídico guatemalteco deja a la población en un estado de indefensión y no permite que tengan un acceso a una tutela judicial efectiva toda vez que no hay métodos para sancionar estos flagelos.

De lo anterior parte la necesidad de la realización de este proyecto de investigación puesto que en la actualidad nos encontramos ante un nuevo escenario estratégico, criminológico y político-criminal, una revolución informática en virtud de los avances tecnológicos lo que ha supuesto la entrada de nuevos valores y bienes susceptibles de protección jurídica.

De la investigación realizada se logró determinar que el objetivo principal del Convenio sobre la Ciberdelincuencia es establecer una política penal común y alineada entre países orientada a la protección de la sociedad contra la ciberdelincuencia, lo que se alcanza tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales a través de una cooperación internacional armónica.

Se concluye que no tipificar delitos informáticos puede llevar a Guatemala a ser destino de delincuentes cibernéticos, dejando a los ciudadanos guatemaltecos sin la protección de sus derechos ni la restitución de los mismos al momento de ser vulnerados pues no existe un mecanismo para lograrlo, para lo que Guatemala deberá por medido de las instituciones u organismos correspondientes adoptar o tipificar los delitos contenidos en el Convenio así como las sanciones, crear las instituciones que correspondan para poder cumplir con proveerle a los ciudadanos seguridad jurídica en resguardo a sus derechos.


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

BIBLIOGRAFÍA:

BACIGALUPO, Enrique. **Lineamientos de la Teoría del Delito.** Editorial Hammurabi, S.R.L. 2ª. Edición. Buenos Aires, Argentina, 1989.

BACIGALUPO, Enrique. **Manual de Derecho Penal. Parte General.** Editorial Temis, S.A. 3ª. Reimpresión. Santa Fe de Bogotá, Colombia, 1996.

CABANELLAS DE TORRES, Guillermo. **Diccionario Jurídico Elemental.** Argentina. 14ª Edición. Editorial Heliasta, 2000.

CENTRO DE OBSERVANCIA EN SEGURIDAD CIUDADANA. **La ciberseguridad en Guatemala.** Guatemala, 2021.

DE LEÓN VELASCO, Héctor Aníbal y De Mata Vela, José Francisco. **Derecho Penal Guatemalteco. Parte General y Parte Especial.** Guatemala 12ª Edición F&G Editores y Editorial Llerena, 2000.

GONZÁLEZ CAUHAPÉ-CAZAUX, Eduardo. **Apuntes Derecho Penal Guatemalteco La Teoría del Delito.** 2ª Edición. Guatemala, 2003.

https://dpej.rae.es/lema/derecho-penal Diccionario Panhispánico del Español Jurídico. **Derecho Penal.** (Consultado: 2 de julio de 2023).

https://dpej.rae.es/lema/derecho-publico Diccionario Panhispánico del Español Jurídico. **Derecho Público.** (Consultado: 15 de julio de 2023).

https://dpej.rae.es/lema/doctrina Diccionario Panhispánico del Español Jurídico. **Doctrina.** (Consultado: 15 de julio de 2023).

https://dpej.rae.es/lema/costumbre Diccionario Panhispánico del Español Jurídico. **Costumbre.** (Consultado: 15 de julio de 2023).

https://cienciasdelderecho.com/los-elementos-del-delito/ Escuela de Postgrados de Ciencias del Derecho. **Los Elementos del Delito.** (Consultado: 20 de julio de 2023).

https://concepto.de/elementos-del-delito/ Enciclopedia Concepto. **Elementos del delito.** (Consultado: 22 de julio de 2023).

https://dpej.rae.es/lema/imprudencia Diccionario Panhispánico del Español Jurídico. **Imprudencia.** (Consultado: 22 de julio de 2023).

https://dpej.rae.es/lema/negligencia Diccionario Panhispánico del Español Jurídico. **Negligencia.** (Consultado: 22 de julio de 2023).

https://concepto.de/impericia/ Enciclopedia Concepto. **Impericia.** (Consultado: 22 de julio de 2023).

https://dpej.rae.es/lema/imputabilidad Diccionario Panhispánico del Español Jurídico. **Imputabilidad.** (Consultado: 22 de julio de 2023).

https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security Kaspersky Lab. **¿Qué es la ciberseguridad?** (Consultado: 25 de julio de 2023).

https://www.gob.mx/profeco/es/articulos/grooming-y-ciberacoso-en-ninos/ es Gobierno de México. **Grooming y Ciberacoso en Niños** (Consultado: 26 de julio de 2023).

https://www.coe.int/en/web/cybercrime/parties-observers Council of Europe. **Parties Observers to the Budapest Convention and Observer Organisations to the T CY. Versión en Español.** (Consultado: 26 de julio de 2023).

https://www.mingob.gob.gt/guatemala-accede-al-convenio-sobre-ciberdelincuen-de-budapest/ Ministerio de Gobernación de Guatemala. **Guatemala accede al Convenio sobre Ciberdelincuencia de Budapest.** (Consultado: 25 de septiem de 2023).

INSTITUTO DE LA DEFENSA PÚBLICO PENAL. **Delitos Informáticos.** Guatemala.

IPANDETEC CENTROAMÉRICA. **Centroamérica Cibersegura.** Febrero 2020.

JIMÉNEZ DE ASÚA, Luis. **Principios de Derecho Penal. La Ley y El Delito.** Buenos Aires, Argentina, 1997.

JUMIQUE CASTILLO, Andrea. **Prensa Libre.** S.Tecnología. Guatemala, **Ataques de malware y phishing, los ciberataques que más aumentaron en el 2022 en en Guatemala.** Pág. 45 (30 de diciembre 2022).

LÓPEZ MAYORGA, Leonel Armando. **Introducción al Derecho I.** Guatemala Décima Tercera Edición. Editorial Levi, 2013.

MARTINS DOS SANTOS, Bruna. **Convenio de Budapest sobre la Ciberdelincuencia en América Latina. Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México.** Derechos Digitales con el apoyo de International Development Research Centre (IDRC), Mayo 2022.

NORIEGA SALAZAR, Hans Aarón. **DELITOS INFORMÁTICOS.** 1ª Edición. Ciudad de Guatemala, Instituto de la Defensa Público Penal, 2011.

OSSORIO, Manuel. **Diccionario de Ciencias Jurídicas, Políticas y Sociales.** Editorial Heliasta. Guatemala, 2018.

POSADA MAYA, Ricardo. **Cibercrímenes. Un nuevo paradigma de la Criminalidad.** Ediciones Uniandes. Bogotá Colombia, 1974.

TELLEZ VÀLDEZ, Julio. **Derecho Informático.** Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. 4ª. Edición, Editorial Mc Graw Hill. México, 1987.

ZAFFARONI, Eugenio Raúl. **Tratado de Derecho Penal. Parte General.** Tomo I. Buenos Aires. Ediar, 1996.

Legislación:

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

Convenio sobre la Ciberdelincuencia. Budapest Hungría, 23 de noviembre de 2001.

Pacto Internacional de Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas, 16 de diciembre de 1966.

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

Código Procesal Penal de Guatemala, Decreto Legislativo Número 51-92 del Congreso de la República de Guatemala, 1994.

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