Facultad de Ciencias Jurídicas y Justicia

Licenciatura en Ciencias Jurídicas y de la Justicia

Regulación de la ciberdelincuencia en el derecho guatemalteco

(Tesis de Licenciatura)

Katherine Maribel Oajaca Alvarado

Guatemala, noviembre 2023

Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas y de la Justicia

Regulación de la ciberdelincuencia en el derecho guatemalteco

(Tesis de Licenciatura)

Katherine Maribel Oajaca Alvarado

Guatemala, noviembre 2023

Para los efectos legales y en cumplimiento a lo dispuesto en el artículo 1°, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Katherine Maribel Oajaca Alvarado,** elaboró la presente tesis, titulada: **Regulación de la ciberdelincuencia en el derecho guatemalteco.**

AUTORIDADES DE UNIVERSIDAD PANAMERICANA

M. Th. Mynor Augusto Herrera Lemus
Rector

Dra. Alba Aracely Rodríguez de González
Vicerrectora Académica

M. A. César Augusto Custodio Cóbar
Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque
Secretario General

FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Dr. Enrique Fernando Sánchez Usera

Decano de la Facultad de Ciencias Jurídicas y Justicia

Guatemala, 5 de mayo de 2023

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como asesor del estudiante **Katherine Maribel Oajaca Alvarado ID 000120972.** Al respecto se manifiesta que:

a) Brindé acompañamiento al estudiante en referencia durante el proceso de elaboración de la tesis denominada **Legislación contra la ciberdelincuencia en Guatemala.**
b) Durante ese proceso le fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.
c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito DICTAMEN FAVORABLE para que se continúe con los trámites de rigor.

Atentamente,

Lic. José Antonio Pérez Castañeda
Abogado y Notario

José Antonio Pérez Castañeda

Guatemala, 10 de julio del 2023

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como **revisor metodológico** de la tesis del estudiante Katherine Maribel Oajaca Alvarado, ID **000120972**, titulada: "Regulación de la ciberdelincuencia en el derecho guatemalteco". Al respecto me permito manifestarles que, la versión final de la investigación fue objeto de revisión de forma y fondo, estableciendo que la misma constituye un estudio serio que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

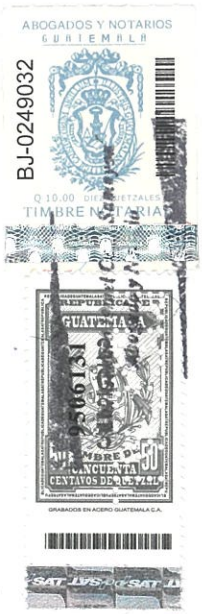
Se hace la salvedad que se modificó el título aprobado en la fase de asesoría que anteriormente se denominaba como: "Legislación contra la ciberdelincuencia en Guatemala", en virtud que era necesario adecuar dicho título al contenido del trabajo de investigación.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE** para que se continúe con los trámites de rigor.

Se hace la aclaración que el estudiante es el único responsable del contenido de la tesis ya indicada.

Licda. Nancy Kumanechy Jimenez Aviche
ABOGADA Y NOTARIA

Lcda. Nancy Kumanechy Jimenez Aviche.
Revisora



En el municipio de Nueva Santa Rosa, del departamento de Santa Rosa, el día veintisiete de octubre del año dos mil veintitrés, siendo las quince horas, yo, **GENARO ISRAEL CANO SAMAYOA**, Notario, número de colegiado: treinta mil ciento noventa y uno (30,191), me encuentro constituido en la primera avenida diez guión cuarenta "B", zona uno de este municipio, soy requerido por **KATHERINE MARIBEL OAJACA ALVARADO** de treinta años de edad, soltera, guatemalteca, perito contador, de este domicilio, quien se identifica con el Documento Personal de Identificación (DPI) con Código Único de Identificación (CUI) dos mil trescientos dieciocho, cincuenta mil setecientos treinta y cinco, cero seiscientos catorce (2318 50735 0614), extendido por el Registro Nacional de las Personas de la República de Guatemala, quien requiere mis servicios profesionales con el objeto de hacer constar a través de la presente **DECLARACIÓN JURADA** lo siguiente: **PRIMERO:** La requirente, **BAJO SOLEMNE JURAMENTO DE LEY**, y enterada por el infrascrito notario de las penas relativas al delito de perjurio, DECLARA ser de los datos de identificación personal consignados en la presente y que se encuentra en el libre ejercicio de sus derechos civiles. **SEGUNDO**: Continúa declarando bajo juramento la requirente: i) ser autor del trabajo de tesis titulado: "**REGULACIÓN DE LA CIBERDELINCUENCIA EN EL DERECHO GUATEMALTECO**"; ii) haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y iii) aceptar la responsabilidad como autor del contenido de la presente tesis de licenciatura. No habiendo nada más que hacer constar, finalizo el presente instrumento en el mismo lugar y fecha de inicio, veinte minutos después, la cual consta en una hoja de papel bond tamaño oficio, impresa en ambos lados, que firmo y sello, a la cual le adhiero los timbres para cubrir los

impuestos correspondientes que determinan las leyes respectivas: un timbre notarial del valor de diez quetzales con serie BJ y numero cero doscientos cuarenta y nueve mil treinta y dos (BJ-0249032) y un timbre fiscal del valor de cincuenta centavos con número de registro nueve millones quinientos seis mil ciento treinta y uno (9506131). Leo íntegramente lo escrito la requirente, quien enterada de su contenido, objeto, validez y demás efectos legales, la acepta, ratifica y firma con el Notario que autoriza. **DOY FE DE TODO LO EXPUESTO.**

f)

ANTE MÍ:

Lic. Genaro Israel Cano Samayoa
Abogado y Notario

UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Ref. O.I. 257-2023
ID: 000120972

ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: **KATHERINE MARIBEL OAJACA ALVARADO**
Título de la tesis: **REGULACIÓN DE LA CIBERDELINCUENCIA EN EL DERECHO GUATEMALTECO**

El Decano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciada en Ciencias Jurídicas y de la Justicia, así como los títulos de Abogada y Notaria, la estudiante ya mencionada, ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.
Segundo: Que tengo a la vista el dictamen favorable emitido por el tutor, Licenciado José Antonio Pérez Castañeda, de fecha 5 de mayo del 2023.
Tercero: Que tengo a la vista el dictamen favorable emitido por la revisora, Licenciada Nancy Kumanechy Jimenez Aviche, de fecha 10 de julio del 2023.
Cuarto: Que tengo a la vista el acta notarial autorizada en el municipio de Nueva Santa Rosa, departamento de Santa Rosa, el día 27 de octubre del 2023 por el Notario Genaro Israel Cano Camayoa que contiene declaración jurada de la estudiante, quien manifestó bajo juramento: *ser autor del trabajo de tesis, haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y aceptar la responsabilidad como autor del contenido de su tesis de licenciatura.*

Por tanto,

Autoriza la impresión de la tesis elaborada por la estudiante ya identificada en el acápite del presente documento, como requisito previo a la graduación profesional.

Guatemala, 8 de noviembre de 2023

"Sabiduría ante todo, adquiere sabiduría"

UNIVERSIDAD PANAMERICANA · Dr. Enrique Fernando Sánchez Usera · DECANO · FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA ·

Dr. Enrique Fernando Sánchez Usera
Decano de la Facultad de Ciencias Jurídicas y Justicia

Nota: Para efectos legales, únicamente el sustentante es responsable del contenido del presente trabajo.

Índice

Resumen

En este estudio se abordó el tema de la regulación de la ciberdelincuencia en el derecho guatemalteco. El objetivo general fue examinar la regulación contra la ciberdelincuencia en Guatemala, para conocer la importancia de contar con normativa específica en esta materia. El primer objetivo específico consistió en analizar la ciberdelincuencia en Guatemala. Asimismo, el segundo objetivo se refirió al análisis jurídico de la ciberdelincuencia. Luego de analizar las legislaciones aplicables se concluyó que el cibercrimen en Guatemala se ha convertido en un problema cada vez más grave en los últimos años. Con la llegada de internet, los delincuentes han encontrado una nueva forma de cometer delitos, dejando a su paso víctimas de fraude, y otras actividades maliciosas. Es imperante contar con la legislación adecuada e innovadora para investigar, regular y sancionar este tipo de crimen.

A nivel mundial se han perfeccionado las relaciones humanas generando diversas formas de comunicación a través de la transmisión de información por diversos medios, entre ellos los sistemas digitales en donde la tecnología ha cobrado vital importancia en la capacidad de interactuar, en este orden de ideas las personas adquieren e innovan en diversos tipos de tecnología con el fin de alcanzar los objetivos en los cuales se desempeñan cotidianamente como lo son el comercio, la interacción social y diversas actividades humanas, en este mecanismo

surgen diversos tipos de delincuencia definidas bajo el término de ciberdelito o ciber crimen, es decir que los delincuentes encuentran la forma de causar perjuicio a los usuarios.

Palabras clave

Digital. Tecnología. Interacción. Ciberdelito. Pena.

Introducción

En esta investigación se abordará el tema de regulación de la ciberdelincuencia en el derecho guatemalteco. El objetivo general de la investigación será examinar la legislación contra la ciberdelincuencia en Guatemala, permitirá conocer la importancia de contar con normativa específica en esta materia. El primer objetivo específico es analizar la ciberdelincuencia en Guatemala, mientras que el segundo será el análisis jurídico de la ciberdelincuencia. Las razones que justifican el estudio consisten en la actualización, debido a que cuando a Guatemala, le fue aprobada la solicitud para incorporarse al Convenio de Budapest, número 185, convenio sobre la ciberdelincuencia, adquirió el compromiso de legislar contra la ciberdelincuencia y este ha sido el motivo por el cual contaba con la Ley de Prevención y Protección contra la ciberdelincuencia.

La investigación contribuirá como material de estudio y referencia en normativa jurídica contra la ciberdelincuencia. En cuanto al contenido, en el primer subtítulo se estudiará la ciberdelincuencia, con base a la legislación vigente contra la ciberdelincuencia, en el segundo se efectuará el análisis jurídico contra la ciberdelincuencia y finalmente en el tercer subtitulo se refiere al análisis jurídico del Convenio sobre la ciberdelincuencia Budapest número 185. Al igual que el mundo, el cibercrimen va en aumento en Guatemala. El departamento de

investigación de delitos cibernéticos e informática forense a cargo de la división de investigación criminal especializada de la policía nacional civil, reportan un considerable incremento.

Estos incluyen acceso ilegal, espionaje ilegal, ataques a la integridad de los datos, ataques a la integridad del sistema y mal uso del dispositivo. La ley aprobada contenía varios artículos que profundizaban en las definiciones de algunos términos y creaba nuevos delitos como el "ciberacoso o *cyberbullying*". Este establece específicamente que el acoso es la intimidación de una persona o grupo de personas por medios informáticos. Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, incluyen acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema.

Señala que se comete acoso por medios informáticos al intimidar o asediar a una persona o grupo de personas. Así como divulgar información confidencial de otras personas que afecte su honor o su salud física o psicológica. Guatemala se convierte así en el tercer país de la región en contar con una ley contra la ciberdelincuencia, después de El Salvador y Costa Rica, resaltó el Congreso de la República de Guatemala. En años anteriores, el gobierno había implementado una estrategia nacional de ciberseguridad, pero carecía de un marco legal en la materia. La reciente aprobación por parte del Congreso de la República de Guatemala al

Decreto 39-2022, que se refiere a la Ley prevención y protección contra la ciberdelincuencia es una muestra de innovación.

Ciberdelincuencia

En el ámbito del derecho penal el estudio de la delincuencia debido al avance tecnológico es muy importante, la evolución de la legislación debe contar con mecanismos de prevención jurídica que coadyuven a contrarrestar los diferentes tipos de delitos. Con el continuo desarrollo tecnológico y la capacidad de adaptación de la sociedad a un nuevo mundo de capacidades virtuales, se deben desarrollar las herramientas necesarias de actualización que permitan perseguir y sancionar hechos criminales cometidos en relación al uso de la tecnología. Uno de estos tipos de delitos especiales es la ciberdelincuencia, referente al tema, la Oficina de las Naciones Unidas contra la Droga y el Delito (2022) proporciona la siguiente definición:

> La ciberdelincuencia es un concepto complejo que engloba una variedad de actividades ilícitas que tienen como blanco las TIC o que las utilizan para cometer los delitos. Los ilícitos considerados ciberdelitos son aquellos facilitados por la cibernética o basados en ella. Los delitos facilitados por la cibernética son delitos tradicionales facilitados (de alguna manera). En el caso de los delitos facilitados por la cibernética, desempeñan un papel fundamental en el método de operación (el *modus operandi*) del delincuente o los delincuentes. Por el contrario, en los delitos basados en la cibernética, que incluyen aquellos que solo se pueden cometer utilizando computadoras y redes. (p.8).

La ciberdelincuencia es un fenómeno criminal que ha surgido de la evolución tecnológica por lo cual necesita ser analizado de manera especial, esto para comprenderlo y proporcionar el tratamiento jurídico especializado otorgando marcos referenciales y sistemas de control adaptados a las circunstancias evolutivas, pues al contar con situaciones

de cambio constante, las herramientas legales deben tener la capacidad de adaptación, la especialidad teoría y técnica de los administradores de justicia implica el conocimiento de aspectos informáticos para tener la facultad analítica del mismo, el instructivo la Ciberdelincuencia de la Cooperación Española (2020) dentro de su marco conceptual establece:

> Ciberdelincuencia es cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación. Es importante señalar que las Tecnologías de la Información y la Comunicación, son una combinación de medios informáticos con medios de comunicación y comprenden: Sistemas Informáticos, Redes Sociales, ordenadores, foros virtuales, etc. (p.7).

De acuerdo a la cita anterior establecer el límite de lo que abarca la ciberdelincuencia es bastante complejo debido a que involucra a las Tecnologías de la Información y la Comunicación, estas son muy amplias debido a que involucra; a los sistemas informáticos, redes sociales virtuales y a las telecomunicaciones. La Oficina de las Naciones Unidas contra la Droga y el Delito (2022), lo ha adaptado bajo el término de "ciberdelincuencia organizada y se entiende un delito cibernético (un delito basado en la cibernética o un delito facilitado por ella." (p.8). La delincuencia organizada también ha ido evolucionando y especializándose para ser más eficiente su actividad criminal.

La ciberdelincuencia ha sido estudiada por diferentes instituciones que tienen injerencia en temas de seguridad, las entidades que se encargan perseguir los delitos de diferente tipo, incluyen en sus acciones los

acontecidos en el área virtual, esto se debe al impacto en el ámbito de seguridad y jurídico, que lleva consigo la persecución de delitos utilizando el ciberespacio, los diferentes estados del mundo han buscado una solución a la criminalidad en aspectos tecnológicos, procurando mantenerse a la vanguardia y con el fin primordial de prevenir este tipo de conducta delictiva, por esa razón la Organización Internacional de Policía Criminal (2021), ha elaborado su propio concepto explicándolo de la siguiente forma:

> La ciberdelincuencia se define como delitos cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos o proveedores de servicios. El concepto habitualmente abarca categorías de delitos como acceso ilícito, interferencia en los datos y sistemas informáticos, fraude y falsificación, interceptación ilícita de datos, dispositivos ilícitos, explotación infantil e infracciones en materia de propiedad intelectual. (p.II).

Los ciberdelincuentes pueden operar desde otros países, lo que dificulta que las fuerzas del orden los investiguen y procesen. Pueden usar redes anónimas para evitar la detección, Pueden usar el cifrado para ocultar sus actividades, al profundizar en la anterior cita es notorio que se comienza a incluir en la figura jurídica de ciberdelincuencia todos aquellos delitos que se pueden organizar, planificar y ejecutar a través del ciberespacio y de las tecnologías de la información y la comunicación, estas personas utilizan diversas técnicas para obtener acceso no autorizado a información confidencial, como datos de identificación personal, información financiera, secretos comerciales y otros datos valiosos.

Delitos informáticos

Los delitos informáticos conforman a la ciberdelincuencia, es decir son conceptos jurídicos inseparables y que pueden ser tomados como sinónimos. De ello se desprende una serie de definiciones que se relacionan directamente con el ramo del derecho penal, incluyendo dentro de sus términos todos los tipos penales considerados delitos, pero estos últimos se ejecutan dentro del área virtual, con ello surge la necesidad de crear el tipo penal que coadyuve y defina la capacidad legislativa en materia de prevención y control de estas actividades delictivas en el ciberespacio, referente al concepto de delitos informáticos, Juárez (2019) proporciona la siguiente aportación:

> Los delitos informáticos son también denominados por la doctrina como ciberdelitos, delincuencia informática o criminalidad informática. Para poder entender que es delito informático, se debe partir del Convenio sobre la Ciberdelincuencia del Consejo de Europa, suscrito en Budapest el 23 de noviembre de 2001, y los define como todo acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, estableciendo conductas propias de este tipo de delitos, que traen consecuencias de tipo penal para quien incurra en ellas. En este sentido se define como toda aquella acción típica y antijurídica, que se sirve o utiliza una computadora para su realización, dirigida a obtener el acceso no autorizado a registros o de un sistema informático. (p. 6).

Es importante considerar lo que indica la anterior cita con respecto a los delitos informáticos, que en la doctrina se les denomina ciberdelitos. En el momento que se realice acción típica y antijurídica utilizando una computadora para transgredir la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos con la finalidad de obtener el

acceso no autorizado a los registros y programas, se califica esta actividad como un delito del tipo penal de delitos informáticos o ciberdelitos. Los delitos informáticos no suelen afectar únicamente y exclusivamente a personas individuales pues incluye todo tipo de personas jurídicas que tengan acceso a la tecnología.

La importancia de analizar los ciberdelitos o delitos informáticos desde el derecho penal sustantivo en el ámbito de actuación y de sanción, radica en la aplicación de un sistema tecnológico, innovador y actualizado, convirtiendo esto en un interés de prevención y seguridad nacional. Es decir que el gobierno debe tener la capacidad técnica y administrativa de investigar, custodiar, prevenir, analizar y sancionar todo tipo de conducta que atente contra la seguridad de la persona que utiliza algún tipo de herramienta tecnológica, tomando en cuenta el tipo de tratamiento que deben recibir los delincuentes que causan perjuicio en el uso tecnológico, Noriega (2011), jurídicamente brinda el siguiente análisis:

> …este tipo de conductas implica el ataque o intencionalidad de daño, a un sistema operativo de la computadora, la intromisión o acceso a bases de datos o archivos que las mismas contengan, o bien la utilización de este aparato tecnológico y de comunicación como medio o instrumento para la realización de delitos. (p.23).

La intencionalidad del daño o la utilización de aparatos tecnológicos y de comunicación, para la realización de delitos, es considerado desde el derecho penal como ciberdelitos o delitos informáticos. La definición jurídica de los delitos informáticos o ciberdelitos, son diferentes de

acuerdo a la región donde se ejecutan estas actividades delictivas, en este orden de ideas cada área geográfica, al igual que otro tipo de delitos encuadrados en el derecho penal tienden a tener ciertas características según la nación en donde son ejecutados, por consiguiente la legislación debe adaptase a la capacidad regulatoria, esto se debe a que los problemas delictivos ocurren de acuerdo al lugar y van evolucionando de conformidad a los fines de las estructuras criminales.

El delito informático o ciberdelitos es una clase de delito especial, que merece un abordaje. Sin embargo, las consideraciones en normativas a nivel internacional han consensuado este aspecto para unificar lo más relevante en esta materia, debido a que cada región cuenta con diferentes tipos de criminalidad que se aplican de acuerdo a los intereses de los criminales que transgreden la ley, por consiguiente, en la búsqueda de soluciones las organizaciones internacionales han sostenido una continua búsqueda de innovación que permita enmarcar situaciones que pongan en riesgo la seguridad, la legislación colombiana, según el autor Téllez (2009) en sus aportes indica:

> Que el concepto de delito informático varía un tanto según la legislación de cada país en el que se realice, sin embargo, existe un amplio consenso en definirlo como una actividad que puede ser calificada como ilícita con carácter delictivo, que se desarrolla usando tecnologías de la información y contraviene la legislación o código penal de un Estado. El delito informático debe ser tipificado en alguna norma o decreto, para el caso particular de Colombia en el año 2009 se expide la Ley 1273 Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (p.9).

Cuando la acción ilícita se realice utilizando tecnologías de la información, ocasionando vulneración de los diferentes bienes jurídicos tutelados, lo más probable es que esta situación se podría llegar a tipificar en el delito informático, sin embargo, para llegar a todo este análisis jurídico, el país o Estado debe de tener legislado este tipo de criminalidad, innovando continuamente en la capacidad de adecuarse para cumplir con el principio de legalidad mediante el uso de internet y una computadora. Villavicencio (2014) establece que: "esta forma de criminalidad no solo se comete a través de estos medios, pues éstos sólo son instrumentos que facilitan, pero no determinan la comisión del hecho delictivo" (p.286).

Los delitos informáticos corresponden a las acciones ilícitas que tienen el objetivo de afectar un sistema informático, repercutiendo en bases de datos con consecuencias materiales, por lo tanto, se entiende que son conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. Es imperante lograr un equilibrio entre la protección de los ciudadanos y la defensa de sus derechos pues los archivos y sistemas requieren seguridad mejorada también puede conducir a mejores relaciones comerciales.

Cibercriminalidad y cibercrimen

La cibercriminalidad tiene relación con los términos anteriormente estudiados como el delito informático y ciberdelincuencia, donde el primero está enfocado al tipo penal previamente legislado y el segundo es una clasificación que abarca todas las actividades relativas al uso indebido del ciberespacio, delitos que pueden no estar legislados en consecuencia al cambio constante en las capacidades de la sociedad para desarrollar avances en el uso de tecnologías y su forma de aplicación. A pesar de que existe una aproximación con los términos se diferencian de acuerdo a la ciencia o especialidad jurídica que los estudia y este es el caso de la cibercriminalidad, por ello Arias (2021), con relación al tema desarrolla lo siguiente:

> Más allá de la etiqueta que, en un futuro, decida utilizar el legislador penal…, lo cierto es que en la actualidad esta forma de criminalidad (se llame Cibercriminalidad, ciberdelincuencia o delincuencia informática) no constituye una categoría normativa y su uso, por tanto, no permite un concepto unívoco. Esto hace que el término sea más usado en criminología (o por profesionales de la informática y seguridad tecnológica) que, en sentido estricto, por juristas. Ello no obsta a que, gradualmente, la Cibercriminalidad comienza a integrar una serie de conceptos y supuestos bien definidos que, con el tiempo, terminarán por constituir una categoría delictiva, más o menos nítida, como hoy lo puede ser el delito informático… (p.183).

Es comprensible que tratar de abordar la ciber criminalidad, desde el ámbito de la criminología es lo más viable, debido a que tratarlos desde el abordaje del derecho penal es complejo porque para que exista esta última debe de existir el tipo penal. La criminología no se limita únicamente al tipo penal, su estudio de las conductas desviadas, ilícitas o delictivas es

tan amplio que aporta un análisis científico jurídico de prevención y contención. Este aporte criminológico con el tiempo se convierte en conceptos y supuestos bien definidos que integran y renuevan el catálogo de delitos que conforma al derecho penal dando vida por ejemplo a la cibercriminalidad como lo es actualmente el delito informático o ciberdelitos.

El cibercrimen hace referencia a los delitos informáticos, actualmente es más común y tiene mejor aceptación hablar de referido termino, que informática criminal o digital, por mencionar los antiguos vocablos que se acuñaban a inicio del presente siglo de la era digital, pues todo tipo de crimen cometido en el área virtual es considerado un delito, la clasificación de delitos se extiende a todas las acciones que pueden perjudicar la convivencia en sociedad atentando contra la seguridad de los usuarios, es decir que se refiere a toda acción que pueda perjudicar a otros y salga del marco legal para ahondar aún más en esta terminología es de vital importancia tener una noción de cibercrimen, al referente el autor Llinares (2012) y expone:

> El término cibercrimen es un comportamiento concreto que reúne una serie de características criminológicas relacionadas con el ciberespacio (sentido tipológico), o para tratar de identificar un tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas en el ciberespacio que afectan a bienes jurídicos dignos de protección (sentido normativo). El término cibercrimen describiría conductas como la consistente en acceder ilícitamente a un sistema informático ajeno, o la del adulto que propone a través de Internet un contacto con un menor con la intención de consumar

> posteriormente un abuso sexual. Y describiría los tipos penales que sanciona el acceso informático ilícito o que castiga el denominado *online child grooming*. (p.39).

Conforman al cibercrimen, todas aquellas conductas o acciones desviadas que pueden estar establecidas en la legislación penal de cada país como delitos, también pueden existir ciertas conductas criminales, que se desarrollan sin estar tipificadas como delitos, por eso al estudiar el cibercrimen desde el ámbito criminológico, su esencia de prevención se adentra al ciberespacio, un mundo infinito aún por descubrir en el cual siempre surgirán nuevos cibercrímenes. En este contexto se debe de ubicar al cibercrimen dentro del estudio criminológico para un mejor análisis debido a que con el tiempo se ha determinado que la criminología y el derecho penal no son sinónimos pues su aplicación es distinta.

Es importante conocer en qué momento se desarrolla el cibercrimen, de conformidad con lo citado anteriormente, esta figura criminológica es la encargada de encuadrar el comportamiento de las conductas criminales cometidas de manera virtual, pero para estudiarla desde ámbito criminológico y desde la perspectiva penal. Concerniente al momento en que se suscita el cibercrimen, Romero et al (2021), con respecto al tema aportan:

> El cibercrimen ocurre cuando tecnologías de la información son utilizadas para cometer o conceder una vulneración. Este tipo de figura abarca fraudes financieros, sabotaje de datos y/o redes, robo de información privada, denegación de servicio o penetración externa al sistema de información, acceso no autorizado y virus informáticos. (p.64).

El estudio del cibercrimen es el análisis de acciones que conllevan la planificación de un delito, con la finalidad de vulnerar la seguridad individual o publica para la obtención de información y darle diferentes usos, a los que se han destinado legalmente. La seguridad informática, es la forma de combatir ciberdelitos, todos pertenecientes a las conductas desviadas, por eso es importante promover la seguridad de la tecnología de la información, como prevención y contención de la ciberdelincuencia. Respecto a los conceptos de ciberdelincuencia, delitos informáticos, cibercrimen, ciber criminalidad, se pueden a llegar a utilizar como sinónimos sin perder la esencia de los mismos el auto, de tal cuenta que el autor Llinares (2012) realiza la siguiente comparación y expone:

> La utilización en el ámbito científico de neologismos procedentes de la traducción al castellano de términos de otras lenguas resulta, en muchos casos, inevitable y, en múltiples ocasiones, arriesgada, dado que generalmente no es posible una identificación completa de sentidos mediante la traducción de términos procedentes de otros idiomas. Quienes, en Estados Unidos, Inglaterra, Australia y muchos otros países han tratado, desde muy diversas ciencias sociales, no suelen hablar de cybercriminality, ni de cyberdelinquency, sino de cybercrime; en castellano, se utilizan indiscriminadamente, los términos cibercrimen, ciberdelitos, cibercriminalidad, ciberdelincuencia, en muchos casos para referirse todos ellos a un mismo significado y en otras pretendiéndole otorgar sentidos distintos. (p.33).

En la cita anterior se esclarece la similitud o diferencia de los conceptos de cibercrimen, ciberdelito, cibercriminalidad y ciberdelincuencia, coincidiendo en que pueden variar sus definiciones dependiendo del área territorial, del país, o continente. Independiente en donde se desarrolle la actividad delictiva lo que sí es certero es cada uno de estos delitos que se realizan a través de la informática o telecomunicaciones, a nivel

internacional y la ratificación de convenios internacionales que han venido a crear obligaciones para los países que los suscriben, esto ha venido a ser una medida de presión para la creación de normas penales especiales que traten estos delitos informáticos que no existían con anterioridad en ninguna parte del mundo sino hasta que surgieron las Tecnologías de la Información y la Comunicación. La ciberseguridad mejorada puede proteger la seguridad nacional.

Informática forense

La informática forense forma parte de la investigación criminal, también es parte de las ciencias forenses, es la encargada de realizar el análisis científico para determinar si los equipos tecnológicos usados en la comisión de un delito fueron los que se encuentran en cadena de custodia, así mismo la informática forense puede identificar al autor del delito informático, Puga (2019), al respecto dicho autor lo define así:

> Es la disciplina que se refiere al estudio y análisis de los datos digitales de un sistema de dispositivos u ordenadores a efecto de establecer circunstancias dentro una investigación criminal. La investigación en delitos informáticos a través del uso internet inicia regularmente con la localización de la persona posible responsable, que en la mayoría de los casos resulta ser el usuario del ordenador o cliente final de un proveedor. Para llegar a él se debe determinar la dirección IP la cual da la posición del proveedor de internet o servicios, no directamente la ubicación del sospechoso; teniendo el nombre y ubicación del proveedor del servicio, a esta empresa se le solicita la información personal del cliente final, si se negare a proporcionar la información sobre el sospechoso puede ser obligado mediante orden judicial (p.231).

Las investigaciones criminales en la actualidad han evolucionado a comparación, a las realizadas con anterioridad, esto se evidencia debido a que a pesar de que la persona utilice medios tecnológicos para la realización de delitos, se puede ubicar al sujeto realizador a través de la dirección IP la cual da la posición del proveedor de internet o servicios (ISP), del nombre y ubicación del proveedor del servicio. Todo esto facilita el esclarecimiento de todo aquel delito, que se haya ejecutado utilizando las Tecnologías de la Información y la Comunicación. La informática forense no se limita exclusivamente a los delitos informáticos, su método de investigación es bastante amplio.

Abarca la investigación criminal para delitos de otra índole como: homicidios, femicidio y violencia psicológica. En el ámbito de la informática forense, se considera de gran importancia la validación de la cadena de custodia tanto en procesos penales como en investigaciones criminales. Es tan extenso la metodología de la informática forense que se hace necesario explicarlo de una manera clara, concisa y precisa para evitar que se confunda su contexto con el análisis forense, Hidalgo et al (2018) al respecto manifiesta:

> La informática forense involucra la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos y es usada para investigaciones criminales, corporativas o institucionales, evaluación de daños y análisis post-mortem como el fraude, el tráfico de drogas, la pornografía infantil, el espionaje, los ataques cibernéticos, la infracción de copyrigth, la recuperación de datos eliminados y la detección de instrucciones con sus mecanismos y técnicas. El análisis forense se refiere a casos en los que se ha producido un delito real en los que la computadora ha sido la víctima. (p. 11).

La informática forense también se puede utilizar en investigaciones privadas como lo son la investigación corporativa, esta se realiza en empresas, fábricas o industrias todas del sector privado, con esto se demuestra que todo lo concerniente a delitos informáticos también se puede desarrollar en este ámbito y no exclusivamente en el público. El análisis forense forma parte de la informática forense porque al ser víctima la computadora de un delito informático este debe de ser examinada para la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos, esto servirá para determinar en un proceso penal la responsabilidad penal y reparación del daño por parte del autor del delito.

De la informática forense se obtiene como resultado la evidencia digital, la cual dentro del proceso penal en juicio oral y público se convierte en evidencia según Cano (2009) de conformidad con la investigación aporta lo que a continuación se expresa:

> Cualquier información sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. En este sentido, la evidencia digital es un término utilizado de manera amplia para describir, cualquier registro generado por o almacenamiento en un sistema computacional que puede ser utilizado como evidencia en un proceso legal. (p.3).

En el proceso penal, según el manual de adquisición y captura de la evidencia digital, la recolección de datos debe realizarse de un modo que asegure la utilidad procesal, porque si la evidencia digital se obtiene sin utilizar la informática forense, se obtendría de una manera incorrecta, lo

cual provocaría duda de su obtención, contenido y veracidad. Lo que se almacene en un disco duro de una computadora o dispositivo digital, de conformidad con el referido manual el levantamiento debe ser realizado empleando las técnicas adecuadas, pues luego de su análisis científico en laboratorio de informática se convierte en evidencia digital, para tener este último nombre en el proceso penal es necesario que el indicio haya sido analizado por un perito en la materia en este caso en informática forense. En informática forense al emitir el dictamen forense da certeza científica pero la cual debe de ser estudiada.

Delitos en materia de ciberdelincuencia en el Código Penal guatemalteco

La historia de cómo surgieron los delitos informáticos en la legislación guatemalteca es de gran ayuda para comprender cómo fue la génesis de estos tipos penales que han ido en evolución de acuerdo al avance de la tecnología y las telecomunicaciones, por lo que Juárez (2019) hace alusión a los antecedentes y refiere:

> En la década de los años noventa frente a la utilización de nuevas tecnologías en diferentes ámbitos del país, nace la preocupación por regular nuevas formas de comisión de hechos delictivos, lo que provoca la reforma del Código Penal por el Congreso de la República a través del decreto 33-96 publicado en fecha 21 de junio de 1996, con el objetivo de regular delitos informáticos en beneficio de la población. Quedando tipificados en el Libro II, Título VI de los delitos contra el patrimonio, y el Capítulo VII que se refiere a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos. (p.9).

La tipificación de siete delitos en esa época de los noventa fue una gran novedad por la magnitud que significaba legislar el bien jurídico tutelado que protegiera a lo más valioso para esa época como; lo son el patrimonio, derecho de autor, propiedad industrial y que a la vez previniera los delitos informáticos. Sin embargo, era inconcebible que las personas que realizan actividades ilícitas no fueran evolucionando conforme iba avanzando la tecnología además de otros bienes jurídicos tutelados como la privacidad sexual y la indemnidad sexual por mencionar los más importantes, que han sido de mayor preocupación para el Estado proteger por los temas de niñez y adolescencia.

En el Código Penal guatemalteco, se encuentran regulados la mayoría de tipos penales, y los delitos penales no son la excepción, los cuales son tomados como básicos y elementales o considerados como los que en esa época más se acoplaban a ese contexto de la conducta delictiva, Noriega (2011) citó el Código Penal (1973) exponiendo la forma en que se norma y en relación al tema considera:

> Los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado. En ese sentido en materia de delitos informáticos se regulan los tipos siguientes: a) Destrucción de registros informáticos b) Alteración de programas c) Reproducción de Instrucciones o programas de Computación d) Registros Prohibidos. e) Manipulación de Información f) Uso de Información g) Programas Destructivos. (artículo 274).

En la cita anterior se encuentran los siete delitos informáticos elementales, pero existen otros tipos penales en el Código Penal guatemalteco identificados como violación a los derechos de propiedad industrial regulados en el artículo 275, pánico financiero, contenido en el artículo 342 "B", ingreso a espectáculos y distribución de material pornográfico a personas menores de edad, violación a la intimidad sexual, producción de pornografía de personas menores de edad, comercialización o difusión de pornografía de personas menores de edad, posesión de material pornográfico de personas menores de edad y alteración fraudulenta contenido en el artículo 275 Bis y el de comercialización de datos personales contenido en la Ley de Acceso a la Información Pública.

Actualmente fue reformado el Código Penal guatemalteco a través del Decreto número 11-2022, que incluye otros delitos informáticos, que regula delitos cometidos en contra de la niñez y adolescencia a través de los medios tecnológicos, esta figura jurídica se puede considerar como parte de la evolución que ha tenido la cibercriminalidad a nivel internacional y que Guatemala ha tenido que enfrentar. En cuanto a este nuevo tipo penal el Código Penal (1973) sanciona en su contenido y al respecto establece:

> La seducción de niños, niñas o adolescentes por el uso de las tecnologías de información… quien, a través de todo tipo o clase de medios tecnológicos, valiéndose o no del anonimato, contacte a cualquier niño, niña o adolescente con el propósito de solicitar o recibir material con contenido sexual o pornográfico, propio o de terceras personas, ya sea que incluya o no medios audiovisuales; Tener o facilitar con tercera persona relaciones sexuales; Facilitar

> la comisión de cualquier otro delito contra la libertad o indemnidad sexual del niño, niña o adolescente contactado. El responsable de una o varias conductas anteriormente indicadas. Será sancionado con prisión de seis (6) a doce (12) años, independientemente que logre su propósito. La pena será aumentada en dos terceras partes, cuando la víctima sea un niño… (Artículo 190 Bis).

En ocasiones algunos niños, niñas y adolescentes en Guatemala han sido víctimas de personas que han utilizado la tecnología, la informática y las telecomunicaciones para obtener beneficios personales de tipo sexual, esto conlleva la voluntad de querer hacer daño. Al regular este delito informático se busca proteger la libertad o indemnidad sexual del niño, niña o adolescente, debido a que ellos aún no tienen la mayoría de edad y tampoco la madurez mental para decidir sobre su sexualidad convirtiéndolos en víctimas idóneas de la ciberdelincuencia. En el artículo 190 Ter, se tipifico el delito informático de chantaje a niños, niñas o adolescentes mediante el uso de tecnologías de información o medios tecnológicos, contenido en el Decreto número 11-2022.

Análisis jurídico contra la ciberdelincuencia

Desde la perspectiva del ámbito jurídico legislar contra los delitos informáticos, ciberdelitos o ciberdelincuencia genera compromiso y deriva de ello la prevención y seguridad. La aplicación del derecho penal en esta nueva especialidad que se ha ido incursionando en el ámbito jurídico, facilita el acceso a la justicia, es necesario contar con el encuadre jurídico que proporcione las herramientas necesarias para garantizar la

investigación y persecución penal, estableciendo protocolos que permiten el adecuado desarrollo de un sistema de justicia eficiente en donde la población cuenta con la protección del Estado. En este orden de ideas la Oficina de las Naciones Unidas contra la Droga y el Delito (2022) preceptúa lo siguiente:

> Las leyes nacionales, regionales e internacionales pueden regir el comportamiento en el ciberespacio y regular los asuntos de la justicia penal relacionados con los delitos cibernéticos… Sin embargo, los principales delitos cibernéticos contemplados en las leyes nacionales no están armonizados entre países y complican la cooperación internacional en los asuntos de justicia penal… El delito cibernético se puede abordar… aplicando leyes existentes que contemplan delitos cometidos fuera de línea... Sin embargo, es posible que las leyes existentes no sean aplicables a los delitos cibernéticos porque estas leyes pueden haber precedido a internet y las tecnologías digitales… las leyes creadas para los delitos fuera de línea pueden tener un impacto limitado en los delincuentes cibernéticos… (p.66).

La legislación nacional, regional e internacional puede llegar a regular la conducta que se realice en el espacio virtual, sin embargo, los delitos de trascendencia en materia de ciberdelitos establecidos en las normas jurídicas de determinado Estado, no se encuentran legislados en los otros países lo cual llega a complicar el acceso a la justicia penal y la cooperación internacional que se llegará a suscitar de esta. También es notorio evidenciar que las leyes existentes en materia de delitos informáticos no sean aplicables a los ciberdelitos actuales, pues la normativa se realizó bajo circunstancias no registradas en el marco legal, ocasionando que, al aplicar estos tipos penales, los mismos se encuentran fuera del contexto actual permitiendo un efecto sancionatorio limitado.

La importancia de legislar contra la ciberdelincuencia radica en los daños que pueden ocasionar las acciones realizadas por los sujetos activos que lo practican, provocando pérdidas económicas o patrimoniales, sin embargo puede llegar a otros alcances más personales como la intimidad de la víctima o la integridad de esta, con sanciones que realmente otorguen la certeza jurídica de alcanzar el objetivo de evitar la impunidad y contribuir a la persecución penal en donde la población tiene acceso a la justicia, y las consecuencias penales son aplicables a quienes se dedican a realizar actividades delictivas a través del ciberespacio o atacando la informática. En este orden de ideas el autor Gómez (2010) argumenta:

> … los llamados «ciberdelincuentes» van siempre un paso…por delante de las autoridades encargados de perseguirlos. Pero no sólo esto; además el número de delitos informáticos aumenta año tras año a un ritmo vertiginoso, mucho más que el de usuarios nuevos que se conectan a internet. …se trata normalmente de estafas u otro tipo de ilícitos relacionados con el impago o no envío de productos y mercancías...desde el punto de vista meramente económico, todo ello origina grandes pérdidas monetarias a las víctimas en particular y al sistema económico en general... Existe un amplio abanico de conductas que, utilizando de alguna manera internet, lesionan algún bien jurídico-penal protegido. Robo de identidades, vulneración del derecho a la intimidad y destrucción de software por virus informáticos. (p.173).

La ley que aborda lo relacionado al ciber delito o delito informático regula las sanciones jurídicas, así mismo protege al usuario que utiliza las tecnologías de la información y la comunicación, también esta normativa jurídica sirve como prevención del daño que se pudiera ocasionar contra; la persona, los datos, el sistema, los servicios e infraestructuras. La ley contra el ciberdelito también tiene la característica que protege los

derechos humanos, y establece la investigación y el respectivo procedimiento judicial contra esta modalidad de delitos. Tiene dentro de sus atribuciones regular la cooperación internacional en materia penal concerniente al área de los delitos informáticos o ciberdelitos. Otra característica es el tema relacionado a la prueba, es decir todo lo que respecta al proceso penal, este tipo de ley especial penal la integra el derecho sustantivo, adjetivo y su enfoque preventivo.

La ley sobre el delito informático establece las sanciones sociales y legales, protege a los usuarios en general y, en particular, mitiga o previene el daño contra las personas, datos, sistemas, servicios e infraestructura. Además, protege los derechos humanos, permite la investigación y enjuiciamiento por los delitos cometidos en línea y facilita la cooperación entre países en materia de asuntos penales que involucran los delitos cibernéticos, establece reglas de conducta y normas de comportamiento para el uso de internet, computadoras y demás tecnologías digitales, así como las acciones del público, el Gobierno y las organizaciones privadas; las normas que rigen la práctica de la prueba y el procedimiento penal y otras materias de la justicia penal en el ciberespacio; la ley incluye el derecho sustantivo, procesal y preventivo.

Delitos cibernéticos que contenía el Decreto número 39-2022

Los delitos cibernéticos que establecen el Decreto número 39-2022, son aquellos que atentan contra sistemas tecnológicos en donde el elemento primordial es la informática y los medios de comunicación electrónicos, con el nombre Ley de Prevención y Protección contra la Ciberdelincuencia, pero se consideró que atentaba contra algunos artículos de la Constitución Política de la República de Guatemala, por tal motivo fue archivada a través del Acuerdo Legislativo 14-2022. Esta ley que fue guardada contenía una serie de tipos penales que la hacían funcional porque protegía bienes jurídicos tutelados nuevos y era preventiva, la normativa tipificaba en el título II, de los ciberdelitos, preceptúa:

> Acceso ilícito, acceso ilícito a datos con información protegida, interceptación ilícita, ataque a la integridad de los datos, ataque a la integridad del sistema, falsificación informática, apropiación de identidad ajena, abuso de dispositivos, fraude informático, agravantes generales, agravante especifico, acoso por medios cibernéticos o ciberacoso, engaño con fines sexuales de los delitos y faltas en la violación de la propiedad intelectual, responsabilidad civil de las personas individuales y penas accesorias, responsabilidad civil de las personas jurídicas y penas accesorias. (Artículo 8, 23)

Habeas data

La exhibición de documentos o *Habeas data* es un Derecho Constitucional y también es reconocida como una garantía, su función consiste en poder tener control y fiscalización de documentos que obran en determinado registro público, en la normativa jurídica archivada y conocida como Ley

de Prevención y Protección Contra la Ciberdelincuencia, se definía este vocablo y le corresponde la siguiente normativa:

> Garantía de naturaleza constitucional que tiene por objeto la protección de la integridad, confidencialidad y disponibilidad de la información y los datos de los particulares y de las personas jurídicas, tendiente a lograr su resguardo frente al poder público y ante terceros. Para efectos de su observancia contiene inmersos los derechos de autodeterminación informativa y la protección de datos personales. (artículo. 7, literal m).

La esencia principal del *habeas data* de acuerdo con la cita anterior es la protección, integridad, confidencialidad, disposición de la información, datos de los particulares y las personas jurídicas, las cuales se encuentran en resguardo y en registro público. El habeas data al ser de naturaleza constitucional, lleva inmerso otros derechos como el de protección de datos personales, al no contar con una normativa jurídica que funcione como prevención y protección como lo era la Ley de Prevención y Protección contra la Ciberdelincuencia, se facilita la vulneración de los derechos fundamentales de las personas individuales y jurídicas. Es importante conocer acerca del *habeas data* debido a que es una garantía de reciente uso en la terminología jurídica muy diferente al *habeas corpus*, en la protección de derechos el investigador Gomez et al citando a Laño (2021) al respecto al tema aporta:

> El *hábeas data* es una garantía que protege varios derechos, tales como la honra, la buena reputación, la intimidad, y también el derecho a la información (…), es un remedio urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y de su finalidad, que consten en el registro o banco de datos públicos o privado y en su caso para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. (p.39).

Engloba varios derechos, entre los más relevantes están: la honra, la buena reputación, la intimidad y el más importante el derecho a la información. Lo que permite el *hábeas data* es tener resguardo de los datos o información como el nombre, edad, estado civil, salario, entre otros aspectos que puedan poner en riesgo la seguridad de la persona. La ventaja es que protege todos aquellos datos que consten en registros o bancos de datos públicos o privados, pudiendo ser suprimidos, rectificados, o actualizados con el fin de guardar la integridad de la persona. Al ser una garantía constitucional se puede utilizar los demás mecanismos constitucionales para darle validez.

Aseguramiento de datos cadena de custodia

La cadena de custodia representa la base del proceso penal porque es en esta etapa permite identificar elementos que después serán considerados como prueba en un proceso penal. Se define como una garantía de evidencia, y el Manual de Procedimientos de Cadena de Custodia (2016) dentro de sus atribuciones establece:

> Un proceso continuo y documentado, aplicado por servidores públicos y/o particulares, cuyo objetivo es mantener la capacidad demostrativa y minimizar el riesgo de pérdida o daño de todos los elementos materiales probatorios y evidencia física, además de los lugares considerados como escena de los hechos y aquellos donde son almacenados, para que puedan ser utilizados en el marco de un proceso penal. El objetivo es asegurar dicha capacidad demostrativa desde que se conozca su existencia o se logra su obtención, hasta que se dispone finalmente de los elementos por orden de la autoridad competente. (p.17).

La cadena de custodia desempeña un papel fundamental en el proceso penal, ya que es en esta etapa donde se establece la integridad y autenticidad de las pruebas. Se considera una garantía de evidencia, y dentro del contenido que se debe aplicar el Manual de Procedimientos de Cadena de Custodia (2016) el cual regula que:

> Un proceso continuo y documentado, aplicado por servidores públicos y/o particulares, cuyo objetivo es mantener la capacidad demostrativa y minimizar el riesgo de pérdida o daño de todos los elementos materiales probatorios y evidencia física, además de los lugares considerados como escena de los hechos y aquellos donde son almacenados, para que puedan ser utilizados en el marco de un proceso penal. El objetivo es asegurar dicha capacidad demostrativa desde que se conozca su existencia o se logra su obtención, hasta que se dispone finalmente de los elementos por orden de la autoridad competente. (p.17).

Representa la esencia del proceso penal porque realizada de la manera correcta, puede probar la existencia de un delito. Constituyen la cadena de custodia, documentación y proceso continuo que deben realizar los servidores públicos denominados especialistas. Los objetivos de la cadena de custodia son mantener la capacidad probatoria y minimizar el riesgo de pérdida de instrucciones asegurando que se garanticen procesos penales efectivos, y esto se hace a instancias de las autoridades competentes. Hay dos elementos importantes en la cadena de custodia: los materiales de apoyo y la evidencia física en este sentido el resguardo de la evidencia forma el principal fundamento de la existencia de la prueba.

El aseguramiento de la evidencia digital es uno de los principios más importantes para evitar la contaminación de esta y que más adelante pueda dejar de ser considerada en un proceso penal, el aseguramiento se práctica

en la cadena de custodia, para ello la sección de laboratorio y asuntos científicos de la oficina de las naciones unidas contra la droga y el delito establece que la función de los servicios de criminalística comienza a desarrollarse en la escena del delito con el reconocimiento y la recogida de las pruebas materiales. Continúa con su análisis y la evaluación de los resultados en un laboratorio, y la presentación de las conclusiones a los jueces, fiscales, abogados y demás personas que necesiten la información concreta. Desde los que realizan la primera intervención en la escena del delito hasta los usuarios finales de la información.

El aseguramiento se refiere a tomar todas las medidas necesarias para evitar la contaminación o alteración de la escena criminal, debido a que de este lugar saldrán los indicios que serán llevados a laboratorio para su análisis y posteriormente ser tomados como evidencia. Las mismas medidas que se deben de tomar para los demás indicios son las que se deben de tomar para los indicios informáticos, si llegara a ocurrir una contaminación física de un medio informático o electrónico se puede alterar la evidencia. La alteración de la evidencia digital puede darse al colocar un imán lo cual provocaría electricidad estática alertando la información almacenada en este. De esa cuenta se manifiesta que el aseguramiento guarda relación con la cadena de custodia en materia de evidencia digital.

Dado que la cadena de custodia tiene que ver con el aseguramiento digital, de donde se obtiene la evidencia digital, es necesario poder definir el concepto legal de evidencia digital, con el objetivo de poder comprender su importancia. La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación, se puede concluir que la evidencia digital la conforma el almacenamiento de dispositivos y los registros que se obtengan durante la investigación. Pues los ciberdelincuentes utilizan una variedad de métodos para explotar las vulnerabilidades.

Al tener relación la cadena de custodia con el aseguramiento digital, de lo cual se obtiene la evidencia digital, es menester poder definir el concepto jurídico de evidencia digital, esto con la finalidad de poder comprender su importancia. La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación, la evidencia digital la conforma el almacenamiento de dispositivos, los registros, elementos tecnológicos utilizados para fines criminales, una red informática, que pudiera considerarse prueba dentro de un proceso de investigación. Al referirse a la cadena de custodia el autor Quispe (2020) expone en su argumentación:

> La identificación, recolección, adquisición y preservación; donde la recolección está ligada al indicio del hecho u objeto, la adquisición es acorde al lugar donde se encontraba (en términos generales una fotografía de donde se encontró lo que se recolectó) y la preservación es acorde al procedimiento de resguardo, con el fin primordial de la protección de evidencia. (p. 92).

El resguardo es parte fundamental de la protección que debe procurarse para garantizar la seguridad de la prueba, para llevar a cabo un proceso adecuado de presentación y posterior aplicación en un proceso de persecución penal. La protección de evidencia permitirá que, al momento de ser tomada y valorada, se establezca su veracidad sin posibilidad de sesgo o desvalorización, con respecto al ciber crimen se deben tomar en cuenta los elementos y consideraciones técnicas y especializadas para evitar la desaparición de datos, formulas o contenido digital, cuya participación es relevante y su eliminación o mal manejo pueda poner en duda la obtención y custodia del material obtenido.

Principios de la cadena de custodia

La cadena de custodia de la evidencia se caracteriza por una serie de principios, que aseguran su funcionalidad y confiabilidad en instancias de juicio fundamentándose en los siguientes principios legales identificados por el autor Quispe en su artículo modelo de cadena custodia identifica el primero como, el debido aseguramiento de la prueba, el cual surge de la necesidad de protección de los medios probatorios, del tiempo y del interés de las partes afectadas. Continúa con la licitud de la prueba que

corresponde a que los canales y medios de obtención de pruebas sean legales y estén debidamente establecidos, dando cumplimiento a la reacción eficaz de los entes encargados de realizar la adecuada investigación.

El principio de veracidad de la prueba cuyo contenido se basa en la obtención y preservación de una prueba libre de vicio y artimaña. Necesidad de la prueba, pues es la prueba quien acredita el hecho, es decir que la prueba sea útil a la investigación probando un hecho. Y por último define la obtención coactiva de la prueba, el Estado emplea la coerción para garantizar la recaudación de la prueba. Con respecto a la importancia en el proceso de investigación, para identificar la motivación y el lugar seleccionado en donde se puede llegar a ejecutar el acto delictivo, lo cual se relaciona directamente con el escenario y elementos que intervienen en la obtención de la prueba en tal sentido, el autor Haro (2021) en la investigación se tienen en cuenta los siguientes aspectos:

> Que a su vez pueden ser considerados en el estudio del ciberdelito, uno de los objetivos es determinar la identidad del autor. Su motivación, que se refiere al móvil que tiene el autor para cometer el delito, la posible víctima y selección del objetivo. Continuando con el *Modus Operandi* que indica la forma en la que se desarrolla la comisión del delito. A través de esto se puede llegar a identificar al autor. La firma es un hecho característico en la comisión del ciberdelito que lleva a cabo el autor para diferenciar "su obra" de otras. En el caso del cibercrimen se podría hablar de varios escenarios posibles, pueden verse implicados varios sistemas informáticos. De forma que a través de unos se consigue actuar sobre otros. (p. 5)

En este sentido es imprescindible contar con los elementos necesarios para llevar a cabo un proceso de investigación objetivo, y establecer el momento oportuno en donde surge el resguardo de la prueba, para poder establecer la fidelidad de esta y que pueda ser útil en un proceso penal. La cadena de custodia es un proceso controlado dirigido que, para poder lograr su objetivo, básicamente debe contener una serie de aspectos, asegurando la trazabilidad de las pruebas informatizadas. Los métodos utilizados son variados y autónomos, deben facilitar el trabajo del comité. Es necesaria la participación de expertos en informática forense, con el equipo adecuado, conservando todo el recurso, ubicando y calificando adecuadamente.

Logrando de esta forma autenticar y transmitir copias originales de la información, y los resultados del análisis de la investigación. Estableciendo la fidelidad de la prueba. Por tanto, pues, no se discutirán las demostraciones, ni serán excluidas como evidencia. Es fundamental comprender que desde el momento en que se identifica una prueba informática hasta que llega a las manos de un perito para su examen técnico, y luego la devolución de dicha prueba Para el autor Piccirilli (2016) “conforma un ciclo de vida pericial que básicamente comprende la etapa de Intervención en el lugar del hecho (puede estar presente o no el perito informático), la detección e identificación de la prueba a secuestrar u obtener” p.5.

La recolección, se refiere al registro de los detalles del equipamiento o prueba informática, identificada como de interés para el proceso. Esto puede complementarse con el acta policial. Continuando con la intervención o embalaje del elemento, identificación o rotulado del elemento, fajado de protección, traslado de la prueba, almacenamiento temporal, hasta la realización de la pericia y devolución de la prueba al Juzgado, estableciendo la identificación de nuevas pericias, concluyendo con la devolución de la prueba pericial al propietario, en la guía Ghosh (2004) indica que: "La prueba informática debe ser conservada exactamente como en su estado original, a lo largo de todo el ciclo de vida pericial, puede suceder que deba realizar algún cambio, y esto de manera inevitable" (Pág.3).

La prueba informática tiene una característica esencial, que la diferencia de otras pruebas, como un arma, droga o un cadáver. Esta diferencia se llama volatilidad. Para poder realizar una correcta preservación del elemento que nos ocupa, es fundamental contar no sólo con el protocolo que se propone en este trabajo, sino además con ciertos elementos físicos como el papel para envoltorio (puede ser papel madera u otro similar, pero que no contenga inscripciones previas, ni dibujos, gráficos o leyendas, cajas de cartón, para embalaje, papel especial de protección contra golpes, paneles de espuma antiestática, cinta de embalaje, pulsera antiestática para manipulación, bolsas de plástico de buen grosor, para embalaje, precintos

de seguridad (numerados y de distinto color) con el objeto de diferenciar las evidencias correctamente y evitar confusiones.

En su investigación de protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia – forensia y cibercrimen) El autor Piccirilli, (2016) indica que “se recomienda utilizar un sistema que incluya etapas en donde la primera etapa se base en el estudio y análisis del entorno, para identificar la evidencia digital a obtener”. p.3. Se refiere al análisis de puntos de conocimiento profesional para determinar los objetivos que debe cumplir la evidencia digital a obtener. La tercera etapa se basa en la adquisición de evidencia digital. Análisis basado en evidencia obtenida, conforme los lineamientos del cuestionario pericial ordenado. Corresponde a la forma de exponer la evidencia digital obtenida en la investigación realizada. Y por último la sexta etapa se basa en preservación. La prueba digital es procesada y entregada al juzgado.

Al continuar con el análisis de la evidencia obtenida se debe analizar básicamente los siguientes aspectos; tipo de evidencia digital que se dispone para su análisis. La herramienta por aplicar y la posible combinación de herramientas. En primer lugar, se debe analizar el dispositivo objeto de la pericia. Si es un disco rígido o un teléfono celular, en el primer caso, es posible que se necesite investigar sobre las características del sistema operativo instalado en el disco rígido, si existen archivos borrados en un disco rígido secuestrado verificar las fechas de

creación, modificación, borrado o último acceso a los archivos, los investigadores buscan archivos en espacios liberados por el sistema operativo (*free space*) que posee el disco rígido, analizar si los discos fueron cambiados, analizar la posibilidad de encontrar evidencia.

En los espacios liberados y parcialmente ocupados por otra información distinta a la original

Continúan con la búsqueda en archivos que poseen claves (*Passport*) y que no han sido provistas en forma previa al análisis de la información. En el caso de un teléfono celular, es posible que se necesite investigar mensajes de texto enviados y recibidos, correos electrónicos enviados y recibidos, contactos guardados en el dispositivo, imágenes, mensaje de voz, geo referenciación de los archivos, tomando en cuenta que no todas las marcas y modelos de teléfonos celulares tienen las mismas posibilidades de búsqueda y hallazgos, particularmente los de origen chino, que en algunos casos llegan a poseer hasta seis chips distintos. En el ámbito de la investigación criminal y la aplicación de la ley no se limitan a áreas geográficas en el mundo no digital.

El ciberespacio es un entorno interconectado con acceso a múltiples servicios e información, y un entorno de preocupación para la prevención, disuasión y disuasión de conductas delictivas. Además, la cadena de custodia es el proceso de registrar el recorrido completo de la evidencia a

lo largo del ciclo de vida de un caso, y se aplica a la evidencia creada a partir de dispositivos móviles y almacenamiento externo y elementos físicos de imágenes forenses. El mantenimiento cuidadoso de la cadena de custodia protege la integridad de la evidencia y hace que sea muy difícil para cualquiera argumentar que la evidencia ha sido alterada en el proceso.

El modelo Case, presentado por Eoghan Casey en 2004, es un modelo Informática forense aplicada, Cohen propuso un modelo muy general que se puede aplicar a sistemas y entornos autónomos. El cual consta de siete fases iniciando con la autorización y preparación, la identificación, documentación, recolección y conservación, inspección y análisis, reconstrucción, y presentación de informes. Es un procedimiento controlado, aplicado por los responsables de la justicia, desde su ubicación hasta su valoración, hasta la prueba física (prueba indicativa), relevante o no, hasta la conducta delictiva, destinada a garantizar la seguridad y la impecabilidad técnica en su manipulación bactericida y evitar su alteración, sustitución, contaminación o destrucción hasta su disposición final por orden judicial. Para tal efecto, es necesario establecer un registro riguroso y detallado que identifique las pruebas.

Si falta alguno de estos componentes, la evidencia recopilada del archivo de computadora no tendrá el valor probatorio esperado. Es importante considerar el valor de las pruebas recabadas durante la investigación, análisis y argumentación en que se apoyan. En este marco de referencia

adquirirán relevancia y pertinencia, por lo que es necesario evitar en lo posible los errores metodológicos propios de cada disciplina en particular, la cadena de custodia de muestras biológicas no es la misma que la de diferentes armas o documentos impresos o virtuales. Los certificados de incautación son un elemento común, pero garantizar la integridad de las pruebas mediante el uso de claves de identificación de los documentos de incautación, con el objeto de mantener la seguridad de la cadena de custodia de la informática forense.

La prueba documental informatizada tiene características especiales que requieren un manejo especial durante su recolección, conservación y transmisión. Consiste en evidencia digitalizada, codificada y protegida en un contenedor digital específico, es decir, toda la información se almacena (aunque se transmita a través de una red, se almacena en ondas electromagnéticas). Hay una diferencia entre un objeto que contiene información (magnético, óptico, disco cuántico, acido desoxirribonucleico o proteína) y su contenido con respecto a la información almacenada. Para este caso se considera todo el conocimiento relacionado con objetos o hechos, fácilmente codificado y almacenado.

Una colección físicamente identificable o lógicamente definible. Es susceptible de recolección mediante interceptación de dicho elemento y está condicionada por las mismas cuestiones legales que la escucha telefónica o la violación de correspondencia. El procesamiento es el paso

más complicado y constituye la primera decisión que debe tomar el recolector. Ante un equipo en funcionamiento, donde la información está siendo procesada, es decir, modificada, actualizada y nuevamente resguardada, debe decidir si apaga o no el equipo. Esta decisión es crítica y puede implicar la pérdida de información y la destrucción de la prueba documental informática pretendida.

La metodología utilizada describe claramente la base conceptual, la teoría y la jurisprudencia a nivel nacional e internacional. En este sentido, la prueba digital en el proceso penal plantea uno de los retos más importantes en la historia del ordenamiento jurídico penal. El problema radica en la recolección de datos y legislación aplicada pues se vincula con la recolección de elementos probatorios con intervención técnica. Y concluyendo que la afectación de la tecnología en la intimidad de los ciudadanos obliga a una regulación muy rigurosa que garantice la aplicación de justicia. Resulta interesante el concepto de la Corte Federal Constitucional Alemana que reconoce un nuevo derecho fundamental constituido por la garantía a la confidencialidad e integridad de la información

En sistemas informáticos como una derivación del derecho a la personalidad y la dignidad. Resulta relevante advertir el grado de amplitud (en virtud de algunos medios tecnológicos o en algunos casos en particular) de la injerencia a la intimidad. Para evitar el posible borrado o

deterioro de la información e identificación de dispositivos de almacenamiento de información digital y dispositivos móviles, y limitar cualquier tipo de alteración que ponga en riesgo, el autor Paternina (2018) en su exposición sobre las características y diversas acotaciones es a tomar en cuenta para la relación de integridad y resguardo correspondiente aporta la siguiente afirmación:

> Se debe tener en cuenta la marca, modelo, números seriales, capacidad de almacenamiento, características morfo-cromáticas entre otras condiciones de identidad. En caso de extraer discos duros, describir el equipo de cómputo del cual fue obtenido. Para garantizar la integridad de archivos digitales, en su recolección, se deben emplear programas que permitan calcular valores y almacenarlos en medios que en lo posible no permitan su modificación o daño. (p. 41)

Análisis jurídico del Convenio sobre Ciberdelincuencia Budapest número 185

El Convenio de Budapest sobre Ciberdelincuencia es un tratado en el campo de la justicia penal acordado por los estados miembros del Consejo de Europa y algunos estados no miembros, en la penalización de la mera tenencia de pornografía infantil en Argentina y España, a la luz del convenio para la ciberdelincuencia de Budapest y marco jurídico de ambos países. El autor Reale (2018) hace mención con respecto a: los cuerpos legales “Convenio para la Ciberdelincuencia de Budapest del Consejo de Europa, Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, la Convención de los Derechos del

Niño y sus protocolos facultativos" (p.15), como normativas que permiten la protección de derechos fundamentales.

Al referirse al ciberespacio el autor Souza (2018) indica que "es la creación de comunidades en un lugar específico, en la estructura de una red que potencialmente no tiene jerarquías, un encuentro de sujetos que, aunque no compartan la misma ubicación tienen la posibilidad de compartir experiencias al instante" (p. 7). Kofi Annan, en las funciones de Secretario General de las Naciones Unidas en el prefacio a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Nueva York: Naciones Unidas, 2004 indico en su discurso lo siguiente:

> Los grupos delictivos no han perdido tiempo en abrazar la economía globalizada de hoy y la tecnología sofisticada que la acompaña. Pero los esfuerzos para combatirlos han permanecido hasta ahora muy fragmentados y nuestras armas casi obsoletas. La Convención da una nueva herramienta para enfrentarnos al flagelo de la delincuencia como un problema mundial. Con la intensificación de la cooperación internacional, podemos tener un impacto real sobre la capacidad de los delincuentes internacionales para funcionar exitosamente y ello puede ayudar a los ciudadanos de todo el mundo en lo que a menudo es su amarga lucha por la seguridad y la dignidad en sus hogares y en sus comunidades. (p. 1).

A través de la ratificación de los convenios internacionales los estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la

introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos que pueda llegar a causar perjuicio en contra de un individuo. Como resultado los estados firmantes adquieren la responsabilidad de tomar estas medidas o de otra naturaleza que resulte necesarias para tipificar como delito en su derecho interno, el Convenio de Budapest (2001) por disposición legal y precepto refiere:

> La comisión deliberada e ilegítima de los actos de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en el convenio tales como, contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado anterior, con intención de que sean utilizados para cometer cualquiera de los referidos delitos (artículos 2, 5, 6).

Cooperación internacional en materia penal y procesal penal

Los Estados firmantes de convenios y tratados tiene la obligación de tomar las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona. En esa línea de pensamiento, los delitos relacionados con la pornografía infantil. Al

respecto, indica que cada Estado parte adoptará las normas que resulten necesarias para tipificar como delito en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos. La regulación legal que se aplica a través del Convenio de Budapest sobre la Ciberdelincuencia establece el delito y aporta la siguiente normativa:

> La producción de pornografía infantil con la intención de difundirla a través de un sistema informático. La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático; La difusión o la transmisión de pornografía infantil a través de un sistema informático; La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos. Se define pornografía infantil el material pornográfico que contenga la representación visual de un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor…; imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito (artículo 8, 9).

El Convenio sobre la Ciberdelincuencia de Budapest es un acuerdo internacional destinado a combatir los ciberdelitos, o los delitos cometidos por medio de internet, estableciendo una legislación penal sustantiva y procedimientos procesales comunes entre los países miembros del Consejo de Europa y los invitados a participar en el mismo. En consideración a la emergencia de amenazas cibernéticas y la especificidad de nuevos delitos, como instrumento internacional entrega una clasificación propia que especifica cada una de las circunstancias delictivas y se encuentra organizada en cuatro presupuestos principales al respecto el autor Duarte (2021) los clasifica en “delitos contra la confidencialidad, la integridad, la disponibilidad de los datos y los

sistemas informáticos, delitos informáticos, delitos según el contenido (por ejemplo, delitos relacionados con la pornografía infantil); y por ultimo delitos relacionados con infracciones a la propiedad intelectual". (p.114).

Legislación contra la ciberdelincuencia en Guatemala

El ciberespacio, por ende, brinda muchas oportunidades para todos sus usuarios y es un medio por el cual los mismos, personas u organizaciones, se pueden conectar para hacer diferentes actividades que serán de beneficio para los mismos. La seguridad cibernética es un problema global y el delito cibernético puede tener serias implicaciones para la seguridad nacional. La ciberseguridad mejorada también puede conducir a mejores relaciones comerciales, permitiendo los nexos necesarios entre diferentes sistemas de gestión de empresas tanto presencial como virtual, pues las empresas pueden sentirse más seguras al realizar transacciones en línea.

El ciberespacio es una dimensión más accesible económicamente que otros canales de difusión e información de utilidad comparable. Esto hace posible que puedan ser millones sus habitantes o usuarios. Es un entorno digital conceptualmente accesible y manipulable, en donde pobladores de cualquier parte del mundo pueden acceder a las distintas redes y sistemas de conectividad, tanto nacional como internacional, permite de esta forma la participación y gestión en sistemas digitales sin dificultad pues ni

siquiera las más complejas y completas son inaccesibles, dado el carácter de lenguaje de su forma de acceder y participar activamente en él.

Los ciberdelitos contra las personas y delito contra la diversidad sexual de niño, niña o adolescente están regulados en el capítulo III del decreto 39-2022, cuyo contenido enlaza la aplicación de Código Penal en los delitos sobre explotación sexual de niño, niña o adolescente, aumentando la pena en una tercera parte cuando los delitos se cometan utilizando sistemas informáticos o cualquier medio de comunicación electrónica; se regula el acoso por medio cibernéticos o ciberacoso, engaño con fines sexuales; sin embargo, se considera que en este tema existen algunas inconsistencias La legislación contra el delito cibernético puede mejorar el cumplimiento de normas internacionales y la persecución penal. Acotando la aplicación de los Decreto 57-2000, Ley de Propiedad Industrial y el Decreto 33-98, Ley de Derechos de Autor y Derechos Conexos.

En cuanto a los delitos y faltas en la propiedad intelectual, aumenta la pena en una cuarta parte si se comenten utilizando sistemas informáticos o tecnologías de la información o comunicaciones, Su alcance, efecto y aplicación se fundamenta en el principio penal de extraterritorialidad al regular la extradición de los responsables de los delitos cometidos en la dimensión del ciberespacio, sucesivamente, se hace un esfuerzo por adecuar la normativa al derecho internacional, específicamente a los principios generales para la asistencia mutua, relativos a la cooperación

internacional regulada por el debate sobre la ciberdelincuencia establecido en Budapest el 23 de noviembre de 2011, desarrollados en el Capítulo III. Cooperación internacional.

Prospectivamente, regula la cooperación en materia penal y procesal penal cuando se requiera internacionalmente sobre el tráfico e interceptación de comunicaciones observándose los tratados y convenios internacionales de los que Guatemala forma parte. Algo que resalta es la creación del Centro de Seguridad Interinstitucional de Respuesta Técnica ante Incidentes Informáticos, la cual estará bajo la coordinación del Consejo Nacional de Seguridad y se divide en dos coordinaciones, la primera es la coordinación de seguridad que corresponde al Ministerio de Gobernación y la segunda es la coordinación de defensa que corresponde al Ministerio de la Defensa Nacional con el fin de dar cumplimiento a las políticas de control.

En Guatemala, la Constitución Política de la República, promulgada por la Asamblea Nacional Constituyente el 31 de mayo de 1985 y que entró en vigencia el 15 de enero de 1986, reconoce la libertad de expresión del pensamiento como un derecho fundamental, y así mismo tiene una ley de orden constitucional en Guatemala. En el marco de la Organización de las Naciones Unidas y la Organización de los Estados Americanos, que protegen el ejercicio de este derecho universalmente, limitándose las facultades únicamente a aquellas partes determinadas conforme a la

misma disposición pueden derivar la responsabilidad posterior y corresponde a la protección de este derecho universalmente.

Limitándose las facultades únicamente a aquellas partes determinadas conforme a la misma disposición pueden derivar la responsabilidad posterior, se establece la Cooperación Internacional para Órganos de Aplicación de la Ley; crea la Red Internacional de Asistencia Mutua Contra los Delitos Informáticos adjunta al Ministerio Público con prestación de servicios las veinticuatro horas al día de los siete días de la semana como lo establece el Convenio de Budapest. Este ente ayudará en la asistencia inmediata para obtener indicios, medios de investigación y pruebas resultado de las acciones que constituyan delitos vinculados a datos informáticos. Es evidente el constante crecimiento tecnológico por lo que el autor Belanger (2017) con respecto al tema indica:

> Como en el auge tecnológico y el aumento de las organizaciones delictivas transnacionales, son necesarias las respuestas, esto exige a la comunidad internacional y crea una situación sin precedentes planteando continuamente nuevos retos a las instituciones encargadas de luchar contra el crimen que, a su vez, utiliza esta tecnología. Las investigaciones, los procesos penales, la represión del crimen para proteger a los ciudadanos y el mantenimiento de la paz y del orden público constituyen un objetivo importante en cualquier sociedad organizada. No sería realista que los esfuerzos por alcanzar este objetivo se limitaran a las fronteras nacionales. Así es desde hace mucho tiempo, pero es algo cada vez más obvio y urgente en la actualidad y ello plantea nuevos retos. (p.276).

Al regular el principio constitucional de *Habeas Data* se entiende que protege los principios y garantías inherentes a las personas en materia de Derechos Humanos, establecidas en la Constitución Política de la

República de Guatemala, en tratados y convenios internacionales y la Ley de Acceso a la Información Pública, que derivan del acceso a la internet, otras tecnologías de la información y las comunicaciones. Con respecto al convenio de Budapest el autor Acuña (2018) establece:

> El Convenio armoniza su contenido con otros instrumentos legales en materia internacional lo que garantiza que los Estados parte automáticamente concierten sus cuerpos legales al legislar con otros convenios y tratados en materia de derechos humanos. Viabiliza su regulación con los convenios o tratados celebrados entre dos o más países, incluyendo los celebrados a futuro, ningún tratado o convenio en la materia pueden contradecirlo. Como puede colegirse, existen motivos racionales de reflexión para que el Estado de Guatemala se adhiera, considerando que los esfuerzos para contrarrestar los ciberdelitos no circunscriben solo a una ley, debe desarrollar otras estrategias focalizadas a la prevención, tecnificación y logística para minimizar los efectos de los delitos informáticos. (p. 218).

El comité de Ministros del Consejo de Europa aprobó la solicitud presentada por el Estado de Guatemala para incorporarse a la Convención de Budapest, que en la actualidad es el único instrumento internacional vinculante que se presenta como una guía para que los países que se han adherido al tratado, puedan desarrollar legislación integral enfocada a la ciberdelincuencia, tipificando los delitos informáticos de forma análoga en los diferentes Estados miembros, equiparando la política penal, normas procesales y la colaboración internacional coordinada, adoptando medidas para prevenir, detectar y perseguir nacional e internacionalmente a los ciberdelincuentes. En Guatemala, algunas infraestructuras críticas llegan a ser propiedad del Estado, mientras que otras pertenecen al sector privado. Hernández (2020) hace mención de lo ulterior:

> A pesar de que Guatemala cuenta con una Ley Marco del Sistema Nacional de Seguridad, la aplicación de esta llega a ser un desafío. La idea de creación de esta ley fue la de sentar las bases para que las instituciones públicas y privadas pudieran tener una coordinación, desarrollando con ello resiliencia, defensa civil, y lo que nos importa: protección de las infraestructuras críticas junto con la tecnología. (p. 20).

En su calidad de fiscal de la nación Lima, Perú, al referirse sobre la necesidad de especialización para combatir la ciberdelincuencia, Zoraida Avalos indica que no se cuenta con juzgados especializados, permitiendo que los casos no sean judicializados y puedan presentarse algunas complicaciones ante el órgano jurisdiccional de turno para evaluar medidas restrictivas de derechos en el contexto de búsqueda de pruebas. Refiriéndose a medidas de conservación, con el fin de optimizar plazos y recursos para la indagación de los delitos informáticos estableciendo los mecanismos necesarios y herramientas legales aplicables para la determinar la culpabilidad.

Infiere la estafa agravada virtual y aquellos casos en los cuales la obtención de prueba digital sea determinante para la investigación, “conservación y revelación parcial rápidas de los datos relativos al tráfico”, “orden de presentación”, “registro y confiscación de datos informáticos”, “obtención real de datos relativos al tráfico” e “interceptación de datos relativos al contenido”, los cuales comportan un conocimiento especializado de las normas convencionales e instituciones dogmáticas sobre la ciberdelincuencia. Por tal motivo, es recomendable la adecuada especialización de los órganos jurisdiccionales que imparten

justicia, las personas que se encargan de administrar justicia deben contar con cierto grado de especialización en la materia.

La especificidad de las organizaciones criminales es crucial para llevar a cabo sus actividades ilícitas, ya que, si bien estas organizaciones se especializan en tipos específicos de delitos, pueden mutar si las circunstancias lo permiten, por ejemplo, en momentos específicos se especializan en allanamientos a instituciones bancarias, o robos en viviendas, y a veces pueden participar en la extorsión y el secuestro. La Subdirección General de Investigación Criminal, en su organigrama de funcionamiento, tiene implementados el Centro de Recopilación, División de Planificación contra el Crimen Organizado y la Policía Cibernética, cuyas funciones van desde la recolección de información de organizaciones criminales hasta la vigilancia.

La asistencia judicial, es uno de los mecanismos esenciales para combatir la criminalidad, se ha podido desarrollar gracias a la colaboración de los Estados, principalmente en el ámbito de la obtención de pruebas. En este sentido, la opinión de la Organización de Naciones Unidas en el informe Perspectivas Económicas de América Latina (2018), establece que el sistema de justicia enfrenta dos desafíos inmensos: la confianza entre los Estados y las herramientas apropiadas en el contexto de la modernidad mencionada. El desarrollo tecnológico, permite de alguna forma el evidente crecimiento de las organizaciones delictivas transnacionales y las

respuestas que esto exige a la comunidad internacional crean una situación sin precedentes y plantean continuamente nuevos retos para poder establecer mecanismos de innovación que vayan de la mano con los avances tecnológicos.

De conformidad con el Reglamento sobre la Aplicación de Métodos Especiales de Investigación de Interceptación Telefónica y Otros Medios de Comunicación, Acuerdo Gubernativo No. 188-2007, la Policía Nacional Civil es deber de la referida entidad establecer un equipo especial de técnicos y seleccionará a los policías responsables de la investigación para realizar la interceptación de comunicaciones, a cargo del caso luego de evaluar el informe preliminar de investigación y determinar la necesidad de este método en particular, el Ministerio Público presentará una solicitud de autorización al juez competente, de la Ley contra el Crimen Organizado.

Las instituciones encargadas de luchar contra el crimen que, a su vez, utilizan esta tecnología se adhieren a sistemas de innovación continua. No es posible imaginar una organización sin acceso a internet, correo electrónico, sitios web, bases de datos de clientes y otras herramientas digitales, todas almacenadas en medios digitales o teléfonos inteligentes. En la actualidad se programan reuniones, intercambios corporativos por correspondencia el uso aplicaciones o herramientas para simplificar el trabajo diario. Utilizando la inteligencia artificial. Estas herramientas se

utilizan de manera secular sin prestar atención a los riesgos que enfrenta la organización con respecto a la confidencialidad.

Los ciberdelitos no conocen fronteras. Los delincuentes, las víctimas y las infraestructuras técnicas están dispersos por múltiples jurisdicciones, lo que resulta muy problemático a la hora de realizar una investigación o emprender acciones judiciales. Por ello es fundamental la colaboración entre el sector público y el privado. Por su alcance mundial, se originó la Organización International de Policía Criminal permitiendo la creación de alianzas multisectoriales, como a posibilitar la cooperación de las fuerzas del orden a escala internacional, este tipo de entidad permite la investigación y persecución de acontecimientos a nivel mundial y permite el control de diversas actividades que ponen en riesgo la seguridad.

Conclusiones

En relación con el objetivo general que se refiere a examinar la regulación de la ciberdelincuencia en el derecho guatemalteco, se concluye que la regulación debe ser innovadora para proteger a los ciudadanos, disuadir a los delincuentes, mejorar las relaciones internacionales y proteger a los ciudadanos en materia de seguridad. La cooperación con otros países puede mejorar la ciberseguridad. La seguridad cibernética es un problema global y el delito cibernético puede tener serias implicaciones para la seguridad nacional, es menos probable que los delincuentes se involucren en delitos cibernéticos si saben que sus acciones tendrán graves consecuencias.

El primer objetivo específico que consiste en analizar la ciber delincuencia en Guatemala, al realizar el presente trabajo de investigación, se arribó a la siguiente conclusión. El delito cibernético, las personas pueden tomar medidas para protegerse y pueden estar más atentos a la hora de identificar y denunciar el delito cibernético. La legislación contra el delito cibernético puede mejorar las relaciones internacionales. La mejora en seguridad pública, puede contribuir la regulación en las relaciones comerciales. La cooperación con otros países puede eficientizar la comunicación. Con la evolución del mundo se generan nuevas situaciones de criminalidad que deben ser perseguidas y sancionadas.

Con relación al segundo objetivo específico que consiste en análisis jurídico de la ciberdelincuencia, se concluye que el ciberdelito es una preocupación creciente en Guatemala, y es necesaria una legislación al respecto para proteger a los ciudadanos. El delito cibernético puede conducir al robo de identidad, pérdidas financieras, acoso cibernético, acoso y la difusión de información y propaganda falsas. La legislación contra el delito cibernético puede disuadir a los delincuentes, dar cumplimiento a los convenios internacionales ratificados por Guatemala. Es importante lograr un equilibrio entre la protección de los ciudadanos y la defensa de sus derechos, al mismo tiempo que se consideran los costos asociados con la legislación sobre ciberdelincuencia.

Referencias

Acuña, L. (2018). Guatemala frente a la era de la globalización de la tecnología y del ciberdelito. *Formación Universitaria, 10(2) 1-22.* https://ipn.usac.edu.gt/wp-content/uploads/2022/09/Debate4-231.pdf

Arias, J. P. (2021). Cibercriminalidad: Hacia la nueva realidad-virtual-del derecho penal. *Revista Internacional de Doctrina y Jurisprudencia*, (26), 175-193.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887-901.

Cano Martinez, J. (2015). Computación forense-Descubriendo los rastros informáticos 2ª edición. *Medellín: Alfaomega*.

Duarte, C. E. (2021). Ciberdelincuencia: análisis del Convenio No. 85 de Budapest y el compromiso del Estado de Guatemala. *Revista Ciencia Multidisciplinaria CUNORI*, *5*(2),111-118. https://revistacunori.com/index.php/cunori/article/view/174

Gómez, A. D. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, (8), 169-203. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

Ghosh, A. (2004, Marzo). Guidelines for the Management of IT Evidence. In *APEC Telecommunications and Information Working Group 29th Meeting*. *From* http://unpan1. un. org/intradoc/groups/public/documents/APCITY/UNPAN016411. pdf.

Guatemala aprueba ley contra la ciberdelincuencia. *Ley contra la ciberdelincuencia* (2022, 27 de junio). Recuperado el 3 de Junio de 2023 de https://dplnews.com/guatemala-aprueba-una-ley-contra-la-ciberdelincuencia/

Haro Olmo, F. J. (2021). Crimen, cibercrimen y análisis forense informático. *Scientia Omnibus Portus*, *1*(1), 2.

Hernández, M. J. (2022). Infraestructuras críticas: análisis de la legislación vigente en España y Guatemala.

Hernández, S. R. (2003). *Metodología de la Investigación*. Ciudad de México: Mc Graw Hill

Hidalgo Cajo, S. Y. (2018). *Informatica Forense*. La Caracola Editores.

Interpol. (2021*) Guía sobre la Estrategia Nacional contra la ciberdelincuencia*.

Juárez, A. L. (2019). *Ciberdelitos en Guatemala*. El Jurista de los Altos.

Ley de Ciberdelitos en Guatemala. (2022, 27 de junio) ¿*Una nueva mordaza para la libertad de expresión?* Recuperado el 7 de mayo de 2023 de https://www.divergentes.com/ley-de-ciberdelitos-en-guatemala-una-nueva-mordaza-para-la-libertad-de-expresion/

Llinares, F. M. (2012). *El Cibercrimen en Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, Ediciones juridicas y sociales, S.A.

Ministerio Público. (2009). *Manual de Normas y Procedimientos para el Procesamiento de Escena del Crimen en Casos contra la Vida e Integridad de la Persona*, Instrucción general 16-2009. Guatemala.

Noriega Salazar, Hans Aarón, *Delitos Informáticos*, Instituto de la Defensa Pública Penal Guatemala 1ª Edición 2011.

Organización Internacional de Policía. (2023, 23 de marzo). *Organización International de Policía Criminal*. Recuperado el 5 de Junio de 2023 de https://www.interpol.int/es

Oficina de Delito. (2022, 27 de junio). *Ciberdelincuencia*. Recuperado 5 de mayo de 2023 de https://www.unodc.org/unodc/es/press/releases/2022/June/unodc-world-drug-report-2022-highlights-trends-on-cannabis-post-legalization--environmental-impacts-of-illicit-drugs--and-drug-use-among-women-and-youth.html#SnippetTab

Paternina Cuesta, R. A. *Estudio de vulnerabilidades en el proceso de cadena de custodia de evidencias en delitos informáticos en la ciudad de Cartagena*. Colombia.

Piccirilli, D. (2016). *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia–forensia y cibercrimen)* (Doctoral dissertation, Universidad Nacional de La Plata).

Policía Nacional Civil. (2022, 28 de junio). *Los ciberdelitos van en aumento y la Policía Nacional Civil cambia estrategia para investigarlos* Recuperado 3 de mayo de 2023 de

https://www.prensalibre.com/guatemala/justicia/los-ciberdelitos-van-en-aumento-y-la-pnc-cambia-estrategia-para-investigarlos/

Puga Rodríguez, R. D. (2019). *La evidencia digital en los delitos de pornografía infantil* (Master's thesis, Quito: UCE).

Romero Aponte, E. J. T. Ortiz Ballhaus, M. y Vásquez Contreras, I. (2021*). Análisis de los delitos cibernéticos en el estado de Puebla a la luz del derecho nacional e internacional*. México

Reale, J. M. (2018). *La penalización de la mera tenencia de pornografía infantil en Argentina*. Argentina

Téllez Valdés, Julio. "*Los Delitos informáticos. Situación en México", Informática y Derecho* Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996

Souza, R. A. (2018). De las redes hacia el ciberespacio. *Revista Digital Universitaria*, *19*(2). https://www.revista.unam.mx/ojs/index.php/rdu/article/view/1779

Villavicencio, F. (2014). Delitos informáticos. *Ius et Veritas*, (49), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Legislación nacional

Asamblea General de las Naciones Unidas. *(1948). Declaración Universal de los Derechos Humanos, Asamblea General de las Naciones Unidas*

Asamblea Nacional Constituyente. (1986). *Constitución Política de la República de Guatemala*

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

Congreso de la República de Guatemala. (1992) *Código Procesal Penal*. Decreto número
51- 92

Congreso de la República de Guatemala. (2003) *Ley de Protección Integral de la Niñez y Adolescencia*. Decreto número 17-73.

Congreso de la República de Guatemala. (1994). *Ley Orgánica del Ministerio Público. Congreso de la República de Guatemala*. Decreto número 40-94.

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

Legislación internacional

Consejo de Europa en Estrasburgo. (2003). *Convenio sobre la Ciberdelincuencia*. Budapest. Número 185