

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



**CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA
QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS
EN GUATEMALA**

HUGO DARÍO DE LEÓN PELLECCER

GUATEMALA, MAYO DE 2023

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

**CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA
QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS
EN GUATEMALA**



TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

HUGO DARÍO DE LEÓN PELLECCER

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, mayo de 2023

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

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
VOCAL I:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Licda.	Evelyn Johanna Chévez Juárez

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera fase:

Presidente:	Lic.	Luis Alberto Patzán Marroquín
Secretario:	Lic.	Osman Doel Loreto Fajardo
Vocal:	Licda.	Zindy Elizabeth Diaz Ruiz

Segunda fase:

Presidente:	Lic.	Abner Fernando Castillo Delgado
Secretario:	Lic.	Hector Daniel Morales Morales
Vocal:	Licda.	Rosa Elida Guevara Pineda

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



Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 13 de octubre de 2022

Atentamente pase al (a) Profesional, FRANCISCO JOSÉ CETINA RAMÍREZ, para que proceda a asesorar el trabajo de tesis del (a) estudiante HUGO DARÍO DE LEÓN PELLECCER, con carné 200314454, intitulado: **CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS EN GUATEMALA.**

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

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

Adjunto encontrará el plan de tesis respectivo.



CARLOS EBERTITO HERRERA RECINOS

Jefe (a) de la Unidad de Asesoría de Tesis

SAQO

Fecha de recepción 13 / 10 / 2022

(f)

Lic. Francisco José Cetina Ramírez
Abogado y Notario

Asesor(a)
(Firma y sello)

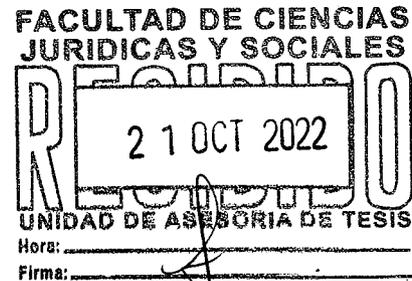


**LICENCIADO FRANCISCO JOSÉ CETINA RAMÍREZ
ABOGADO Y NOTARIO
COLEGIADO 13,776**



Guatemala 21 de octubre del año 2022

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



Doctor Herrera Recinos:

Respetuosamente me dirijo a su persona con el objeto de manifestarle que asesoré el trabajo de tesis del alumno **HUGO DARÍO DE LEÓN PELLECCER** según nombramiento de fecha trece de octubre del año dos mil veintidós, intitulado: **“CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS EN GUATEMALA”**, para el efecto procedí a la realización de los cambios y modificaciones necesarias y declaro que con el sustentante no me une parentesco alguno dentro de los grados de ley, por lo que emito el siguiente dictamen tomando en consideración lo siguiente:

- a) Se llevó a cabo un trabajo que denota un valioso aporte tanto técnico como científico y abarca un extenso contenido doctrinario y legal, habiendo sido el objeto de estudio del tema la creación del perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos.
- b) La metodología empleada durante el desarrollo del trabajo llevado a cabo tiene relación con los capítulos de la tesis y con su respectiva presentación, hipótesis y comprobación de la hipótesis. Para redactar la introducción y conclusión discursiva, se utilizaron los métodos inductivo y analítico, así como la aplicación de los métodos deductivo y sintético.
- c) En cuanto a los objetivos de esta se puede indicar que es fundamental determinar el perfil psicológico de las personas que cometen delitos informáticos en Guatemala, para demostrar la necesidad que existe en el modelo de investigación penal para deducir responsabilidad penal de una persona.
- d) Los capítulos de la tesis permitieron la comprensión de los criterios técnicos y jurídicos que fundamentan las aseveraciones realizadas. El aporte científico del tema es fundamental y se basó en un contenido actual. En cuanto a la conclusión discursiva, se relaciona con el contenido del trabajo de investigación y señala el adecuado nivel de síntesis legal relacionado con el objeto del tema. Además, la bibliografía que se utilizó para la elaboración de la tesis ha sido la acorde y adecuada a su contenido.

LICENCIADO FRANCISCO JOSÉ CETINA RAMÍREZ
ABOGADO Y NOTARIO
COLEGIADO 13,776



Doy a conocer que el trabajo de tesis del sustentante cumple de manera eficaz con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que **DICTAMINO FAVORABLEMENTE** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Atentamente.

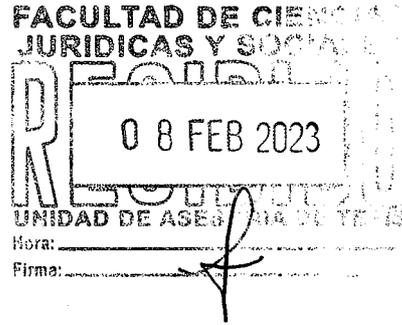
Licenciado Francisco José Cetina Ramírez
Asesor de Tesis
Colegiado. 13,776

Lic. Francisco José Cetina Ramírez
Abogado y Notario



Guatemala 08 de febrero del año 2023

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



Dr. Herrera Recinos:

Le doy a conocer que revisé virtualmente la tesis del alumno HUGO DARÍO DE LEÓN PELLECCER, con carné 200314454, que se denomina: "CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS EN GUATEMALA".

El trabajo de tesis efectivamente cumple con lo requerido en el instructivo respectivo de la Unidad de Asesoría de Tesis de la Facultad de Ciencias Jurídicas y Sociales y en ese sentido le doy a conocer que las correcciones indicadas fueron efectivamente atendidas, motivo por el cual es procedente emitir **DICTAMEN FAVORABLE**.

Muy atentamente.

"ID Y ENSEÑAD A TODOS"


 Licda. Rosa Viviana García Chavarría
 Docente Consejera de Estilo

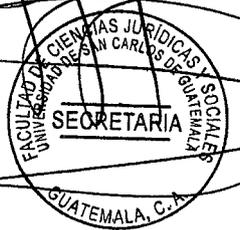
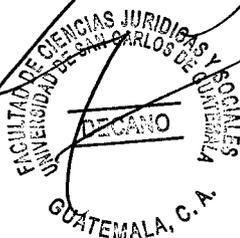




Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, diecisiete de abril de dos mil veintitrés.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante HUGO DARÍO DE LEÓN PELLECCER, titulado CREACIÓN DEL PERFIL PSICOLÓGICO PARA IDENTIFICAR A UNA PERSONA QUE HA COMETIDO UNA CONDUCTA DELICTIVA POR MEDIOS INFORMÁTICOS EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

CEHR/SAQO





DEDICATORIA

- A DIOS:** Por concederme vida, guiar mi camino, darme la fuerza y persistencia para seguir adelante en todo momento.
- A MI MADRE:** Zoila América Ana Pellecer Carrillo, por su amor incondicional, esfuerzo, dedicación, entrega, humildad, perseverancia y apoyo para no claudicar en el camino a mis metas.
- A MI PADRE:** Bernardo Armando de León López (+), por su amor, consejos, sabiduría, enseñanzas y aliento para seguir nutriéndome de conocimientos a lo largo de mi vida.
- A MIS ABUELOS:** Hugo Edmundo Pellecer García (+), María Zoila Carrillo Álvarez (+), María Magdalena López Sosa viuda de De León (+) por su cariño incondicional.
- A MI HERMANO:** Giovanni Orlando, por su amor, comprensión, por siempre estar a mi lado, y, ser mi guía y modelo a seguir.



A MIS TIOS:

Héctor Darío (+), José Daniel (+), en especial a Coralia Magalí y Sergio Otoniel, por quererme como a un hijo y contar con su apoyo incondicional.

A MI NOVIA:

Astrid Carolina Flores Rivera, gracias por ser mi mejor amiga, mi compañera de aventuras, viajes y sueños, por brindarme el aliento y los ánimos para dar ese esfuerzo extra cuando quería bajar los brazos. Te Amo.

A MIS AMIGOS:

Del colegio y de la universidad; en especial a Ulisses y Marthyn, gracias por los momentos compartidos y sus buenos deseos a lo largo de este proyecto.

A:

La Tricentenario Universidad de San Carlos de Guatemala en especial a la Facultad de Ciencias Jurídicas y Sociales; por abrirme sus puertas, por la formación académica y profesional.



PRESENTACIÓN

El presente trabajo de investigación plantea la investigación de la creación del perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala.

Para el desarrollo de la investigación, se utiliza la investigación de tipo explicativa, desarrollando como base de la investigación al derecho penal por desarrollar a los delitos informáticos así como el derecho informático; el presente trabajo de investigación de tesis fue realizado en el periodo comprendido del mes de enero del año 2016 al mes de diciembre del año 2017.

El objeto de la investigación es evidenciar la necesidad para la creación de un perfil psicológico con la finalidad de que se identifique a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala.

El sujeto que desarrolla la presente investigación de tesis, es la persona que comete una conducta delictiva por medios informáticos, a la cual, es preciso identificar por medio de la creación de perfiles psicológicos que demuestren su forma de actuar para sancionar a los mismos.

El aporte académico se representa al establecer la necesidad de formular perfiles psicológicos para identificar a toda persona que representa una amenaza de conducta contra la sociedad por ser considerada delictiva, utilizando para ello medios informáticos, ya que con ello, se mejorará la seguridad y la prevención informática a nivel país.



HIPÓTESIS

La presente investigación de tesis utiliza una hipótesis general, para demostrar la necesidad que existe en el modelo de investigación penal para deducir responsabilidad penal de una persona; el objeto del trabajo de investigación es demostrar que la creación de un perfil psicológico para la identificación de una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala, ayudará al Estado a combatir los delitos informáticos por personas anónimas.

El sujeto del presente trabajo de investigación es la persona que comete una conducta delictiva por medios informáticos, a quien se pretende identificar por medio de la creación de un perfil psicológico para facilitar su persecución penal. Para la comprobación de la presente hipótesis se plantea utilizar los métodos de investigación analítico, sintético, inductivo y deductivo.



COMPROBACIÓN DE LA HIPÓTESIS

La hipótesis planteada fue comprobada al evidenciar que, la creación de un perfil psicológico para identificar a una persona que comete conducta delictiva por medios informáticos o bien delitos informáticos, se puede perseguir de una manera efectiva, ya que con ello se determinan las conductas delictivas por medios informáticos más comunes; lo que hace una asociación de patrones de personalidad que permiten establecer las diferencias entre los tipos de delincuentes informáticos.

El presente trabajo de investigación utilizó para la comprobación de la hipótesis el método de investigación analítico, sintético, lógico para determinar las variantes de investigación científica, asimismo el método de investigación inductivo y deductivo para generar las conclusiones.



ÍNDICE

	Pág.
Introducción	i

CAPÍTULO I

1. El derecho penal	1
1.1. Definición del derecho penal.....	3
1.2. Naturaleza jurídica del derecho penal.....	5
1.3. Principios del derecho penal.....	7
1.4. Características del derecho penal.....	10
1.5. Formas y especies de la ley penal.....	14
1.6. Fuentes del derecho penal	16

CAPÍTULO II

2. El derecho informático.....	19
2.1. Definición de derecho informático	19
2.2. Diferencia entre el derecho informático y la informática jurídica	21
2.3. Antecedentes del derecho informático	23
2.4. Seguridad en el derecho informático.....	25
2.5. Incidentes de seguridad informática.....	26
2.6. La protección de datos personales	30

CAPÍTULO III

3. Los delitos informáticos	35
3.1. Definición	36
3.2. Antecedentes	38



3.3. Sujetos que involucran los delitos informáticos.....	43
3.4. Regulación legal de los delitos informáticos.....	45

CAPÍTULO IV

4. Creación del perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala .	49
4.1. Utilización de la criminología.....	49
4.2. El perfil psicológico.....	53
4.3. Herramientas para determinar perfiles psicológicos	58
4.4. Creación de perfiles psicológicos para delincuentes informáticos	61
CONCLUSIÓN DISCURSIVA	63
BIBLIOGRAFÍA.....	65



INTRODUCCIÓN

El presente trabajo de investigación se planteó la temática referente a la creación de un perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala, ya que no hay una persecución penal efectiva en cuanto a los delitos informáticos se refiere por la falta de identidad de los delincuentes informáticos.

Con base a la problemática establecida mediante los métodos de investigación analítico, analítico, sintético, inductivo y deductivo cómo la creación de un perfil psicológico no solo es beneficioso para la identificación de un delincuente informático si no también para generar una asociación en los patrones de personalidad de los mismos que permiten establecer las diferencias entre los tipos de delincuentes informáticos.

El objetivo general de la investigación planteó demostrar que la creación de un perfil psicológico para la identificación de una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala, ayudará al Estado a combatir los delitos informáticos por personas anónimas.

El sujeto del presente trabajo de investigación fue la persona que comete una conducta delictiva por medios informáticos, a quien se pretende identificar por medio de la creación de un perfil psicológico para facilitar su persecución penal, es decir el delincuente informático.

La investigación quedó contenida en cuatro capítulos, el primero desarrolla al Derecho Penal por ser la ciencia del derecho que regula los delitos informáticos, estableciendo



para el efecto su definición, naturaleza jurídica, sus principios, características, las formas y especies de la ley penal y las fuentes del Derecho Penal.

En el segundo capítulo se abordó lo referente al Derecho Informático por ser base de la temática que involucra el trabajo de tesis, por lo que, se verificó su definición, su diferencia con la informática jurídica, sus antecedentes, la seguridad que aplica, los incidentes de seguridad y la protección de datos personales.

Asimismo, en el tercer capítulo se desarrolló lo referente a los delitos informáticos, estableciendo para el efecto su definición, antecedentes, los sujetos que involucran los delitos informáticos y su regulación legal en Guatemala.

Para concluir con el capítulo final, se abordó la temática central del trabajo de investigación de tesis desarrollando el tema de la creación del perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala, desarrollando como subtemas para la comprobación de la temática, el planteamiento para utilizar la criminología, la creación de un perfil psicológico y sus atribuciones, las herramientas para determinar perfiles psicológicos y la creación de perfiles psicológicos para delincuentes informáticos

Comprobando con los capítulos anteriores, mediante el análisis jurídico y doctrinal la hipótesis planteada.



CAPÍTULO I

1. El derecho penal

La presente investigación utiliza como base fundamental al derecho penal, por ser la ciencia que establece la regulación de normas jurídicas de protección al derecho informático. Dentro del desarrollo de la sociedad en cuanto a los medios y utilización de la tecnología, surge la informática, herramienta por la cual facilita la realización de varias labores, ya sea en el ámbito estatal, de las empresas privadas, de la familia o a nivel personal. Desafortunadamente junto al avance de la tecnología y su utilización, existen nuevas formas de delinquir, lo cual genera un grave daño, tal es el caso del delito informático, que en la actualidad ha cobrado auge, es por ello que la presente investigación inicia su análisis doctrinal desarrollando al derecho penal.

El derecho penal como ciencia del derecho determina el listado de las conductas que son consideradas como delitos por el Estado y la pena que corresponde a cada delito, esto con el objeto de brindar la protección contra la delincuencia en la sociedad.

Asimismo, la existencia de medidas y sanciones sirven para aislar al delincuente en los centros penitenciarios que se crean, para que posteriormente el mismo sea reincorporado por medio programas de rehabilitación, lo cual no ocurre en Guatemala, ya que la mayor parte de delincuentes que cumplen su condena por algún delito, en su mayoría son reincidentes.



La doctrina del derecho penal y los juristas especializados en esa rama del derecho han preocupado, de la naturaleza y características que presenta la potestad de la administración del Estado, del poder ejecutivo para imponer sanciones a las personas; y de los requisitos que se tienen que cumplir. La historia del derecho penal es bastante extensa. El surgimiento del derecho penal obedece a la necesidad de regular el comportamiento del hombre en la sociedad.

El derecho penal especial, describe los actos delictuosos e indica la pena que tiene que imponerse al responsable. El estudio de la parte general está muy desarrollado y la teoría del delito constituye un ejemplo del refinamiento dogmático alcanzado.

En cuanto al derecho penal especial es de lamentar la falta de análisis sistemático orientado a nociones básicas de derecho penal para integrar o completar los tipos legales mediante la elaboración de principios o de criterios generales.

Por razones esencialmente prácticas y de técnica legislativa se justifica la distinción anotada, es de señalar que las disposiciones de la parte general y de la parte especial de los códigos se encuentran estrechamente relacionadas; tanto en el plano teórico como en su aplicación concreta. Este vínculo puede ser mostrando los delitos dolosos y culposos, respectivamente.

De manera que, el derecho penal forma parte de los mecanismos sociales, que tienen por objeto la obtención de determinados comportamientos individuales en vida de la

sociedad. Asimismo, procura alcanzar sus fines declarando ciertos comportamientos como delitos y amenazando su relación con sanciones que pueden generar el encarcelamiento por muchos años de acuerdo con el delito cometido.

Para entender de un mejor forma al derecho penal es necesario establecer su definición desde distintos puntos de vista, ya que es una ciencia muy compleja que ha sido estudiada a lo largo de los siglos por distintos doctos y tratadistas del derecho.

1.1. Definición del derecho penal

Para entender el significado concreto de su definición, primeramente, es necesario mencionar las definiciones que establece al derecho penal como ciencia, dentro de las cuales se encuentran.

La definición que establece que el derecho penal es: “una rama del saber jurídico, que mediante la interpretación de leyes penales propone a los jueces un sistema orientador de decisiones, que contiene y reduce el poder punitivo; para impulsar el progreso del Estado Constitucional de derecho”.¹

Otra definición establece al derecho penal como: “el conjunto de normas jurídicas que regulan la potestad punitiva del Estado, asociando a hechos, estrictamente determinados por la ley, como presupuesto, una pena o medida de seguridad o corrección como consecuencia, con el objetivo de asegurar los valores elementales

¹ Bustos Ramírez, Juan. **Manual de derecho penal parte general**. Pág. 38.



sobre los cuales descansa la convivencia humana pacífica”.²

También se puede definir al derecho penal desde el punto de vista subjetivo la cual establece que: “El derecho penal subjetivo consiste en la facultad de aplicar normas jurídicas que se encarguen de regular el poder punitivo del Estado, asociando los hechos determinados legalmente, como presupuestos y penas o medidas de seguridad como las consecuencias jurídicas”.³

En cambio, la definición objetiva establece que: “es aquel que se refiere a las normas jurídico penales en sí, es el conjunto de leyes que determinan los delitos y las penas que el poder social impone al delinciente”.⁴ Cuando se habla del derecho penal objetivo o *jus peonale*, se debe hacer referencia al conjunto de normas jurídicas establecidas por el Estado que determinan los delitos y las penas y que, de esa manera, regulan el poder estatal de penar.

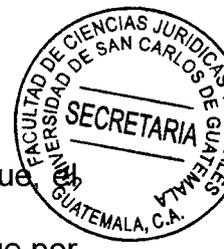
Otro reconocido tratadista define al derecho penal como: “el conjunto de normas jurídico-penales y, o, al sistema de interpretación de esa agrupación dispositiva; el primero de ellos es el derecho penal propiamente dicho y, el segundo es la ciencia del derecho penal; el cual es el sistema de comprensión de la legislación penal y le asigna un carácter interpretativo, como lo tiene cualquier ciencia”.⁵

² **Ibíd.** Pág. 39.

³ **Ibíd.** Pág. 40.

⁴ Cuello Calón, Eugenio. **Derecho penal.** Pág. 25.

⁵ Zaffaroni, Eugenio Raúl. **Tratado de derecho penal.** Pág. 69.



De las definiciones anteriores, la mayoría de los autores coinciden en cuanto a que el derecho penal, es un conjunto o sistema de disposiciones jurídicas que se distingue por los fines que se persiguen a través de él y por la particularidad de sus sanciones. Por lo tanto, puede decirse que el derecho penal desde el punto de vista objetivo o derecho penal material es el conjunto de normas jurídico-penales que regulan los delitos y las faltas, y establecen las correspondientes penas y medidas de seguridad que se deben imponer a los delincuentes.

En cuanto a la definición del derecho penal a criterio del autor del presente trabajo de investigación de tesis, es posible determinar que el derecho penal es un conjunto de normas jurídico-penales que sancionan las conductas determinadas como delitos y penas para la persona que cometa los mismos.

1.2. Naturaleza jurídica del derecho penal

El derecho penal ha sido asignado para defender tanto intereses públicos como también privados, ya que, el derecho privado se encarga de regular las relaciones entre los particulares. Dentro de las ramas del derecho que pertenecen al derecho privado se encuentran tanto el derecho civil y el derecho mercantil, el derecho público se encarga de regular las relaciones jurídicas relativas al Estado: la organización de la Administración y de los servicios públicos, las relaciones de trabajo de los funcionarios o la recaudación de impuestos, verbigracia.

El derecho penal es derecho público, debido que: “de un lado, porque el objetivo de la tutela del derecho penal (los bienes jurídicos) tiene carácter directamente comunitario, afectando a la colectividad organizada en Estado. Cuando un sujeto comete un delito no está solo lesionando el bien de la víctima, sino el interés general de la sociedad en la preservación de ciertos bienes y valores. A todos nos interesa que se castigue al homicida, y no solo a la familia de la víctima. El derecho penal, más que una relación entre dos particulares, sujeto activo y sujeto pasivo del delito disciplina una relación entre el Estado y el autor del delito”.⁶

Es por ello por lo que se ha dicho en la doctrina que el derecho penal cumple con la naturaleza jurídica mixta, sin embargo, debido al *ius puniendi*, que se refiere a la facultad del Estado para imponer un castigo es que se ha establecido su naturaleza dentro del derecho público.

Esto también es demostrable por el actuar de oficio que realiza el Ministerio Público, ya que es el ente que tiene mandato legal para perseguir penalmente a toda persona que cometa conductas delictivas, cualquiera puede solicitar de los Tribunales la persecución de un delito, hacerlo incluso contra la opinión de la víctima, y hacerlo hasta el punto de constituirse en parte en el proceso, sosteniendo la acusación, salvo excepciones.

Por lo cual, no solo sucede que el delito no es un mero conflicto entre particulares, también que la resolución del conflicto pasa necesariamente por el Estado, que es el

⁶ Sánchez Lascuarín, Juan Antonio, Cancio Meliá, Manuel, Basso J. Gonzalo. **Manual de introducción al Derecho Penal**. Pág. 37

que impone la pena. Es por ello que, la sanción penal solo pueden aplicarla órganos jurisdiccionales que actúan investidos de ius imperium, en el ejercicio de la soberanía del Estado.

1.3. Principios del derecho penal

El derecho penal, se encuentra conformado por diversos principios que, rigen esta disciplina jurídica y establece los lineamientos que se deben seguir para aplicar correctamente la Ley penal.

Los principios son: “normas básicas del ordenamiento jurídico que se inspiran en los valores y que los encauzan hacia las concretas reglas del mismo. Nos indican por ello si es valiosa una norma desde la perspectiva de un determinado valor, o cuán valiosa es o, en su caso, si es intolerablemente disvaliosa”.⁷

- El principio de legalidad: en la doctrina se establece que este principio: “genera el mandato de precisión o determinación de las normas penales, que es un postulado derivado del principio de legalidad que apela a la redacción precisa y concreta de los enunciados penales”.⁸ En la Constitución Política de la República de Guatemala, el principio de legalidad se encuentra contenido, esencialmente, en dos artículos. El Artículo 152, que establece que el poder proviene del pueblo y que *su ejercicio está* sujeto a las limitaciones señaladas por la Constitución y la ley. Y el Artículo 154, el

⁷ Zaffaroni, Eugenio Raúl. **Ob. Cit.** Pág. 75.

⁸ **Ibíd.** Pág. 78.



cual señala que los funcionarios son depositarios de la autoridad, responsables legalmente por su conducta oficial, sujetos a la ley y jamás superiores a ella; asimismo, el Código Penal, Decreto Número 17-73, del Congreso de la República en su Artículo uno establece: “Nadie podrá ser penado por hechos que no estén expresamente calificados, como delitos o faltas, por ley anterior a su perpetración; ni se impondrán otras penas que no sean las previamente establecidas en la ley”.

- El principio de extractividad: este principio demuestra la temporalidad del delito de acuerdo con el momento de su ejecución, y a su vez beneficia al reo; el Artículo dos del Código Penal lo establece al preceptuar: “Si la ley vigente al tiempo en que fue cometido el delito fuere distinta de cualquier ley posterior, se aplicará aquélla cuyas disposiciones sean favorables al reo, aun cuando haya recaído sentencia firme y aquél se halle cumpliendo su condena”.
- El principio de territorialidad de la Ley Penal: este principio determina la aplicación de la Ley penal a toda persona que cometa un delito o falta en el territorio de la República; el mismo se encuentra preceptuado en el Artículo 4 del Código Penal.
- El principio de exclusión por analogía: este principio se encuentra contenido en el Artículo 7 del Código Penal. En doctrina se le da el nombre simplemente de juzgamiento por analogía. Es decir, que por analogía los jueces no podrán crear figuras delictivas ni aplicar sanciones. Como queda claro, el principio es una manifestación del carácter garantista del derecho penal por esta ley.

- Principio de taxatividad: este principio consta de la forma en que se puede establecer la seguridad jurídica de que únicamente el Estado, por medio de su congreso u órgano legislativo tiene la facultad de considerar una conducta determinada como punible o no.

- Principio de proporcionalidad: este principio establece que: “La proporcionalidad que debe prevalecer en el momento de aplicar la pena, según la cual, debe existir un “equilibrio” entre sanción y el fin que persigue la pena”.⁹ En este sentido las teorías preventivas resultan bastante contestes con la enunciación, sin embargo, es aún mayor la consecuencia que significa para la proporcionalidad que debe existir entre la determinación de la pena y los bienes jurídicos tutelados. Y en tal dirección debe apuntar así mismo, la discusión que se tendrá en adelante con respecto a la proporcionalidad que establece actualmente la política delincencial que en materia de narcoactividad se refiere.

- Principio del debido proceso: este principio puede significar dos cosas, primeramente, que para el juzgamiento de todo delito debe haber un juicio previo, asimismo, que se deben respetar todas las etapas y derecho que la Ley concede a las partes del proceso penal.

- Principio de inocencia: en la Constitución Política de la República de Guatemala, en el Artículo catorce: “Toda persona es inocente, mientras no se haya declarado responsable judicialmente en sentencia debidamente ejecutoriada”. El ser tratado

⁹ **Ibíd.** Pág. 88.

como inocente no solo está incluido en la garantía de presunción de inocencia, sino que sus alcances son más limitados que ésta. Es alrededor de esa presunción que gira todo el proceso penal moderno y las demás garantías judiciales. El grado de prueba más allá de la duda razonable es un corolario de este principio.

1.4. Características del derecho penal

El derecho penal posee características únicas que lo diferencian de las demás ramas del derecho, dentro de las cuales se estudian en este subtema, para lograr una mejor comprensión de la temática del derecho penal.

Se ha afirmado en la doctrina que el derecho penal tiene las siguientes características, es una ciencia cultural, es normativo, es positivo, es valorativo, es finalista, es sancionador, es preventivo y es rehabilitador.

Es una ciencia cultural: “atendiendo a que el campo del conocimiento científico aparece dividido en dos clases de ciencias; las ciencias naturales por un lado y las ciencias sociales o culturales por el otro, se hace necesario ubicar a la disciplina en ambos campos, ya que es aplicable a los dos”.¹⁰

Es normativo ya que se integra por normas penales y jurídicas que son ordenanzas que contienen mandatos o prohibiciones para regular la conducta del ser humano, y con ello normar el correcto actuar de las personas dentro de una sociedad que tiene amparo del

¹⁰ De León Velasco, De Mata Vela José Francisco. **Derecho penal guatemalteco**. Pág. 6.



Estado de derecho.

Es positivo porque por ser parte de la normativa jurídica mundial sus normas deben cumplirse en todo momento ya que se encuentran vigentes por la imposición del Estado.

Pertenece al derecho público por que, siendo el Estado único titular del derecho penal, solamente el establece la facultad de establecer los delitos y las penas o medidas de seguridad correspondientes. El derecho penal es indiscutiblemente derecho público interno, puesto que el establecimiento de sus normas y su aplicación está establecido en forma exclusiva al Estado, investido del poder público.

Es valorativo en virtud que toda norma supone una valoración, en cuanto al derecho penal está subordinado, a un orden calificativo, en cuanto que examina los actos humanos con arreglo a una valoración la cual refiere evaluar la conducta de los hombres.

Es finalista, debido que, siendo una ciencia teleológica, su fin primordial es resguardar el orden jurídicamente establecido, a través de la protección contra el crimen.

Es fundamentalmente sancionador: “debido que se ha caracterizado para castigar, reprimir, imponer una pena con carácter retributivo a la Comisión de un delito, de esta manera se manifiesta su naturaleza sancionadora, en base a que la pena es la única

consecuencia del delito”.¹¹

También se dice que es preventivo ya que desde hace algún tiempo en su estudio se evidenció que dejó de ser únicamente sancionador, por lo que, dejó de ser una simple operación lógica jurídica que implicaba una retribución penal, muchas veces desproporcionada, a los sujetos que causaran un daño a la sociedad predeterminado por la ley, el delito. Se ha dicho que con el apareamiento de las medidas de seguridad que el derecho penal toma la característica de ser preventivo.

Dentro del inacabable proceso de búsqueda de sus fines, como el sistema de control social que es, el derecho penal actualmente también pretende evitar el delito y es que, con toda razón, es válido afirmar que un sistema que busca mantener la paz y el orden social, o que estos se alteren lo menos posible, es mucho más eficaz si se anticipa a evitar y resolver las causas que puedan alterarlos, que si solo intenta mantenerlos con la amenaza general de un mal a las conductas antisociales contra ese orden jurídico establecido y con la aplicación particular de un mal, una pena, a quien realice esas conductas, pues históricamente solo con estas medidas no se ha logrado la consecución de los fines del derecho penal.

De manera que, como última característica se establece al derecho penal como rehabilitador, esto de acuerdo a lo preceptuado en el Artículo 19 de la Constitución Política de la República de Guatemala, la cual establece que: “El sistema penitenciario debe tender a la readaptación social y a la reeducación de los reclusos y cumplir en el

¹¹ *Ibíd.* Pág. 9.

tratamiento de los mismos, con las siguientes normas mínimas:

- a. Deben ser tratados como seres humanos; no deben ser discriminados por motivo alguno, ni podrán infligírseles tratos crueles, torturas físicas, morales, psíquicas, coacciones o molestias, trabajos incompatibles con su estado físico, acciones denigrante s a su dignidad, o hacerles víctimas de exacciones, ni ser sometidos a experimentos científicos;
- b. Deben cumplir las penas en los lugares destinados para el efecto. Los centros penales son de carácter civil y con personal especializado; y
- c. Tienen derecho a comunicarse, cuando lo soliciten, con sus familiares, abogado defensor, asistente religioso o médico, y en su caso, con el representante diplomático o consular de su nacionalidad. La infracción de cualquiera de las normas establecidas en este artículo, da derecho al detenido a reclamar del Estado la indemnización por los daños ocasionados y la Corte Suprema de Justicia ordenará su protección inmediata. El Estado deberá crear y fomentar las condiciones para el exacto cumplimiento de lo preceptuado en este artículo”.

La rehabilitación es la reeducación del sujeto para su incorporación a la vida social, suprimiendo los factores negativos de su personalidad y potenciando los positivos, hasta conseguir una adaptación definitiva del sujeto peligroso o delincuente a una vida en comunidad, respetando las normas y al resto de sujetos que conviven con él.

1.5. Formas y especies de la ley penal

La Ley Penal es aquella disposición por virtud de la cual el Estado crea derecho con carácter de generalidad estableciendo las penas correspondientes a los delitos que define. En su *strictu sensu* es una norma de carácter general que asocia una sanción a una conducta prohibida por ella.

Por su especialización, estas se dividen en: “leyes penales codificadas y en leyes penales especiales, comprendiendo bajo esta amplia denominación, no sólo las que particularmente definen delitos y establecen penas, sino las de índole civil, política y administrativa que encierran infracciones y señalan una sanción penal”. Por la naturaleza de determinar las penas, se clasifican en determinadas, indeterminadas y relativamente indeterminadas”.¹²

Asimismo, la Ley penal tiene distintas especies dentro de las cuales se encuentran:

- “a) Ley penal *stricto sensu*: Tema tratado en la definición de ley penal, específicamente en cuanto a que ésta define los delitos y las faltas, determina las responsabilidades o las exenciones y especifica las penas o medidas de seguridad que a las distintas figuras delictivas o de peligro social corresponden.

- b) Convenios internacionales: El tratado internacional sólo es obligatorio para los súbditos de un país cuando una ley interna lo ha convertido en legislación del

¹² Jiménez de Asúa, Luis. **Lecciones de Derecho Penal**. Pág. 56.

Estado. Mientras ello no sucede, el convenio autoriza a cada una de las altas partes contratantes para que pida la aprobación del convenio y se convierta así en derecho de cada uno de los países que lo suscribieron. De tal forma, los tratados internacionales no son más que las leyes estricto sensu que tendrán los mismos efectos que las leyes auténticas.

- c) Plenos poderes: En tiempo de guerra, en caso de catástrofe, cuando una revolución ha triunfado o cuando otra se toma, pueden asumir los gobernantes, con el jefe del Estado a la cabeza, plenitud de poder.
- d) Leyes delegadas: Aunque en las Constituciones no se hable de ellas, son posibles, cuando no estén prohibidas, porque facilitan la aprobación parlamentaria de los códigos técnicos, tales como el civil, penal y el de comercio, las cuales se podrían aplicar de manera supletoria en un determinado momento dependiendo del origen que dio al nacimiento de la infracción jurídica tutelada etc.
- e) Decretos-leyes: Todas las dictaduras han acudido a decretos-leyes para disciplinar aquellas materias que no pueden ser objeto de decreto estricto sensu”.¹³
- f) Decretos, órdenes, reglamentos, ordenanzas: No es posible crear por decreto del Presidente, ni por orden ministerial, disposiciones penales estricto sensu. Si puede por el poder ejecutivo, reglamentar las leyes, incluso las de carácter penal.

¹³ *Ibíd.* Pág. 98.

1.6. Fuentes del derecho penal

El estudio del derecho penal conlleva analizar de donde surgió es decir sus fuentes, por lo que, algunos autores y estudiosos del derecho penal han abordado el tema de las fuentes del derecho penal estudiando únicamente la ley, lo cual ha sucedido probablemente porque, como se podrá observar en el transcurso de este trabajo, es generalmente aceptado que la ley penal es la única fuente directa del derecho penal.

La palabra fuente, indica en sí, el lugar por donde fluye o emana algo. Cuando el jurista toma esa expresión para llenarla de contenido se le atribuye un doble significado, siendo estos: “la fuente de producción, que es la voluntad que dicta la normas jurídicas en el derecho penal por medio del Estado y la fuente de conocimiento, la cual es la forma en que ese derecho objetivo asume en la vida social”.¹⁴ Para comprender mejor el monopolio que la ley ejerce en cuanto a la producción de derecho penal es necesario dirigirse a los enunciados *Nullum Crimen, Nulla Pena sine lege*, pero para que la pena produzca su función de coaccionar psicológicamente ha de haber una definición exacta de cada delito y la pena que corresponde a cada uno en la ley penal, ya que para producir una amenaza con efecto intimidante el amenazado por la norma debe saber que, se le está conminando a obedecer la ley. Dejando establecido lo anterior se afirma que solo la ley es fuente del derecho penal, pero dejando también sentada la importancia de las fuentes en toda disciplina y particularmente en el derecho.

¹⁴ <https://www.repositorio.pucp.edu.pe/index/bitstream/handle/lasfuentesdelderechopenal.pdf> (Guatemala, 18 de diciembre de 2016).

Es por ello que, el derecho penal, describe que hechos son delitos. Es excluyente, permite que otras disciplinas se introduzcan en su campo. Es una garantía, ya que aplica una sanción solo a delito establecido por ley penal. La Ley Penal surge del *ius puniendi* del Estado. “La ley penal es la manifestación de voluntad soberana del Estado, imperativa y obligatoria, que describe una conducta humana omisiva o activa como delito al cual se le impone una pena”.¹⁵

Otra clasificación establece que las fuentes del derecho penal se clasifican de la siguiente forma.

- a) Fuentes Reales o Materiales: “tienen su fundamento en la realidad de los hombres y por ende de los pueblos son las expresiones humanas, los hechos naturales o los actos sociales que determinan el contenido de la norma jurídico penal, es decir son las expresiones y manifestaciones socio naturales previas a la formalización de una ley penal”.¹⁶
- b) Fuentes Formales: se refiere al proceso de creación jurídica de las normas penales y a los órganos donde se realiza el mencionado proceso legislativo que en Guatemala corresponde al Congreso de la República.
- c) Fuentes Directas: son aquellas que por sí mismas tienen la virtud suficiente para crear normas jurídicas con carácter obligatorio, de donde se emana directamente el

¹⁵ <https://www.oocities.org/penaluno/fuentesdelderechopenal.htm> (Guatemala, 19 de diciembre de 2021).

¹⁶ De Mata Vela. **Ob. Cit.** Pág. 105.

derecho penal: “La Ley es la única fuente directa del derecho penal, por cuanto sólo esta puede tener el privilegio y la virtud necesaria para crear figuras delictivas y las penas o medidas de seguridad correspondientes”.¹⁷

- d) Las fuentes directas se dividen en fuentes de producción y fuentes de cognición. Fuentes directas de producción: Son las integradas por la autoridad que declara el derecho, el poder que dicta las normas jurídicas que no es más que el Estado, a través del Órgano Legislativo; fuentes directas de cognición: Son las manifestaciones de la voluntad estatal. La expresión de la voluntad del legislador, es decir la fuente de conocimiento que es precisamente el Código Penal y las Leyes Penales especiales.
- e) Fuentes Indirectas: Son aquellas que solo en forma indirecta pueden coadyuvar en la proyección de nuevas normas jurídico-penales, e incluso pueden ser útiles tanto en la interpretación como en la sanción de la ley penal, pero no pueden ser fuente de derecho penal, ya que por sí solas carecen de eficacia para obligar. Por lo cual, estas son las fuentes que reconoce la doctrina en Guatemala, siendo la Ley la única fuente directa del derecho penal, por conformarse de acuerdo con las normas.

¹⁷ **Ibíd.** Pág. 125.



CAPÍTULO II

2. El derecho informático

El derecho informático desarrolla parte del tema central del presente trabajo de investigación, es por ello que es preciso analizar a esta ciencia. En los últimos treinta años se han diversos problemas que relacionan el derecho con las tecnologías de información, pero aún no se ha logrado obtener un nivel teórico satisfactorio que permita dilucidar con exactitud los problemas principales que se generan a nivel informático.

Una primera forma de entender al derecho informático en su relación con el derecho, y las tecnologías de información es interpretada como la aplicación de instrumentos tecnológicos a las operaciones que realizan quienes actúan en el ámbito del derecho.

2.1. Definición de derecho informático

Es preciso establecer la definición de esta ciencia para una mejor comprensión, esta ciencia es de reciente estudio por parte de tratadistas y estudiosos del derecho.

La mayoría de los autores consideran que el derecho informático es la rama del derecho que consiste en: “el conjunto de normas, aplicaciones, procesos, y relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la Informática



jurídica, así como la evolución del derecho en general. Tiene como objetivo regular la actividad jurídica, utilizándola como instrumento que simplifique al profesional del derecho el ejercicio de su profesión”.¹⁸

Otra definición indica que el derecho informático es: “es el marco jurídico que actúa para regular todo lo relacionado con los datos y la información electrónica de cualquier tipo”.¹⁹

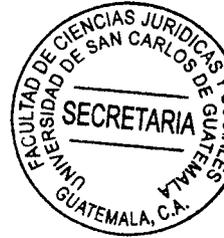
Entender qué es el derecho informático implica aceptar que el mundo se está transformando al ritmo en que aparecen nuevos e importantes avances tecnológicos en una variedad de campos, como la tecnología de las comunicaciones de información, la inteligencia artificial, la nanotecnología, la tecnología espacial, la biotecnología o la computación cuántica, entre otros.

Se trata de innovaciones altamente disruptivas y capaces de producir cambios transformadores importantes en el funcionamiento de las sociedades. Avances muy diferentes, pero con un elemento común: que se centran en la recopilación, el procesamiento y el análisis de enormes cantidades de datos, dando origen a lo que conocemos como justicia digital.

Otra definición puede ser: derecho informático es: “el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad

¹⁸ Téllez Valdés, Julio. **Derecho informático**. Pág. 14.

¹⁹ Sierra, Yhorman. <https://www.blog.lemontech.com/derecho-informatico/> (Guatemala 17 de agosto de 2016).



informática”.²⁰

De manera que en conclusión el derecho informático es aquella ciencia que estudia el tratamiento automatizado de la información desde una perspectiva jurídica, capaz de ordenar la actividad, situaciones y relaciones jurídico-informáticas emergentes, al servicio del derecho a la información.

2.2. Diferencia entre el derecho informático y la informática jurídica

Es importante para una mejor comprensión de la temática actual, establecer la diferencia que existe entre el derecho informático y la informática jurídica, ya que muchas veces causa confusión por su similitud.

Como ya se hizo mención el derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el derecho y la informática. También se le considera como una rama del derecho especializada en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales.

Es por ello que, el derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos que devienen de la relación entre derecho y la informática, o una rama especializada del derecho relacionada con la informática, aplicaciones e implicaciones legales.

²⁰ Téllez Valdés, Julio. **Ob. Cit.** Pág. 15.



En cambio, por informática jurídica se entiende a: “la técnica interdisciplinaria que tiene por propósito la aplicación de la informática, para la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de dicha información necesarios para la toma de decisión con repercusiones jurídicas”.²¹

Asimismo, la informática jurídica surge cuando se aplican los instrumentos informáticos a los fenómenos del derecho, se refiere a la informática como avanzado medio técnico que proporciona auxilio y servicio a las diversas actividades relacionadas con el derecho.

En sentido coincidente puede ser definida como: “el ámbito de la informática al servicio del derecho, es decir como instrumento que en el ámbito del derecho permite optimizar la labor del abogado, el jurista y el juez”.²²

Una definición simple establece que es: “la técnica multidisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”.²³

Otra definición establece que la informática jurídica es: “la ciencia que estudia la

²¹ **Ibíd.** Pág. 18.

²² **Ibíd.** Pág. 19.

²³ **Ibíd.** Pág. 22.



utilización de los recursos informáticos (hardware y software) para la mejora de los procesos (análisis, investigación y gestión) en el ámbito jurídico”.²⁴ Esta aplicación concreta de la informática al derecho se traduce en distintas formas de captar su utilidad, lo que ha dado lugar a la subdivisión en distintas especialidades; informática jurídica documental, informática jurídica de gestión, informática jurídica decisional y ofimática.

La informática jurídica, que implica las ciencias de la informática aplicadas al campo de lo jurídico, disciplina que se encarga de la aplicación de las tecnologías derivadas de la Ciencia de la Computación al conocimiento jurídico, para optimizar y facilitar el desempeño del Abogado, Jurista, Administración Pública y Administración de Justicia. Son muchos los campos de aplicación de esta disciplina al campo jurídico, como lo son sistemas de documentación legislativa y jurisprudencial, de conocimiento científico jurídico, automatización del funcionamiento de los Juzgados y Tribunales, entre otras.

2.3. Antecedentes del derecho informático

Su primera denominación se remonta a: “1949 con la obra de Norbert Wiener, donde expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.

Además añade que en ese mismo año, el Juez de origen estadounidense Lee Loevinger publicó un artículo en la revista Minnesota Law Review, de título The Next

²⁴ Aguilar, Alfonso Pablo. **¿Derecho informático o informática jurídica?**. Pág. 12.



Step Forward, en donde afirma que el próximo paso adelante en el largo camino del progreso del hombre debe ser el de la transición de la teoría general del derecho hacia la jurimetría. Este término implica la sustitución del Juez por la computadora”.²⁵

De manera que, es surgimiento se manifiesta en tiempos modernos donde predominan las tecnologías de la información y comunicación, necesarios para satisfacer la demanda de servicios acorde al contexto de la sociedad, la evolución de la Ciencia de la Computación ha incursionado en el derecho como facilitador de las labores de Abogados, Juristas, Servidores Públicos de la Administración de Justicia y público en general.

En este sentido, esta ciencia del derecho conforma una parte fundamental del derecho como regulador de los fenómenos jurídicos derivados de la actividad del hombre en cualquier área, tuvo que ocuparse de los mismos en consecuencia por la utilización de la informática en la vida diaria.

De esta forma a finales de los años sesenta y luego de cerca de diez años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático, demostrando con ello que se requería un trato especial y una regulación específica para un mejor control.

²⁵ **Ibíd.** Pág. 25.

2.4. Seguridad en el derecho informático

La seguridad informática y la seguridad de la información suelen considerarse como sinónimos cuando en realidad son conceptos distintos, aunque se encuentran relacionados.

La seguridad informática se refiere a: “las diversas técnicas, aplicaciones y dispositivos encargados de asegurar la confidencialidad, integridad, privacidad y disponibilidad de la información de un sistema informático y por consiguiente de sus usuarios”.²⁶

La palabra seguridad toma forma de propuestas para dar una mayor prioridad a temas como son los derechos humanos, la economía, el medio ambiente, el tráfico de drogas, las epidemias, los crímenes, la injusticia social además de los hechos tradicionales en relación a la seguridad de amenazas militares externas.

Asimismo, la seguridad de la información se relaciona con la ausencia de riesgos sobre específicamente los datos que ya han sido procesados, y que sirven para construir un mensaje y que de acuerdo a las normas jurídicas esta seguridad de la información se encuentra a cargo de encargados de la información y responsables de la misma.

Por lo anterior, la seguridad informática consiste en asegurar la ausencia de riesgos en cualquiera de los componentes de un sistema hardware, software, personal informático, redes, usuarios, datos y procedimientos, impidiendo que cualquier persona sin

²⁶ Gómez Vieites, Alvaro. **Seguridad Informática**. Pág. 3.

autorización pueda tener acceso a la información contenida en el sistema y por lo tanto no pueda modificarla, dañarla, alterarla, eliminarla o darle cualquier tratamiento que no esté autorizado.

2.5. Incidentes de seguridad informática

Los incidentes de seguridad informática tienen su origen debido a fallas de algún componente del sistema mismo, mal funcionamiento del equipo como descargas eléctricas, problemas en con el hardware y software que se utilizan, etcétera, por su tipo amenazas internas o externas, de alto riesgo, de mantenimiento, errores de utilización, omisiones, terremotos, erupciones volcánicas, inundaciones, incendios, etcétera o bien por alguna motivación robo, terrorismo, fraude, hackeos, alteración de datos, denegaciones de servicio, virus informáticos, worms, troyanos, atentados, etcétera.

De manera que, son los incidentes que causan riesgos y peligros los cuales ponen en riesgo la seguridad informática por alguna motivación ya que a diferencia de las amenazas de origen.

que cuentan con las normas específicas que van desde los derechos de consumidor que podemos ejercer al hacer efectiva una garantía por mal funcionamiento de un equipo que hemos adquirido o bien solicitar la intervención de una aseguradora por la pérdida de determinados equipos que fueron asegurados y hubieran sido dañados por alguna descarga o bien por eventos externos como pudieran ser fenómenos de la

naturaleza como un huracán o un sismo.

Los incidentes de seguridad informática por alguna motivación, en cambio, pueden accionar normas como las penales en caso de estar como se dijo ante un robo o bien una amenaza terrorista o una extorsión. Es por esto que hablar de seguridad informática y un solo derecho que le asista o resuelva resulta casi un imposible.

Es común escuchar la solicitud de los encargados de la seguridad informática solicitar al encargado del despacho jurídico que le explique cuáles son las leyes que deben de cumplirse para poder cumplir con las obligaciones de una adecuada seguridad informática.

La realidad es que el derecho no pretende regular la tecnología y que los riesgos son inherentes al mismo sistema informático, es decir existen vulnerabilidades y riesgos derivado de ellas tanto en el aspecto del hardware, el software y el del personal que los utiliza lo que puede traducirse en una vulnerabilidad como el robo o acceso no autorizado a bases de datos por ejemplo de clientes de un banco.

En este caso se estaría frente a un tema de seguridad informática que vulnera también el derecho a la protección de datos. Todo un cuerpo normativo que regula esta temática. La seguridad informática, no hay duda, requiere de la identificación de riesgos, es decir de las posibilidades de que un evento crítico aparezca y su evaluación permite poder tener acciones específicas para reducir la amenaza. En este caso las

vulnerabilidades que nos interesan son las derivadas de las amenazas por motivación relacionadas con los aspectos legales.

Algunos casos en los que la presencia de este tipo de amenazas y acciones perpetradas en contra de la seguridad informática y de la información ha hecho que las partes involucradas acudan ante autoridades correspondientes e incluso tribunales internacionales para dirimir las consecuencias derivadas. Es importante señalar que las normas jurídicas han tenido que ir evolucionando ante el avance científico y tecnológico pues una de las características del derecho es que no es apriorístico por lo que no puede encontrarse a la par del surgimiento de los nuevos descubrimientos.

Es relevante considerar que gran parte de los casos sobre incidentes de seguridad informática se centran en cómo las empresas y gobiernos se ocupan de las infracciones de datos o problemas de privacidad, como puede ser: “el caso del hackeo que puso en riesgo los números de tarjetas de crédito y débito de 4.2 millones de usuarios por medio de la cadena de supermercado Hannaford Bros., en la costa este de los Estados Unidos que registró 1,800 casos de fraude y cuya vulnerabilidad si bien se identificó en febrero de 2008, en realidad se había venido realizando desde diciembre del año anterior”.²⁷

De este caso se desprende que ante una situación que atenta contra la seguridad informática que pone en riesgo la información, se debe de comunicar a los involucrados sobre la situación y hacer de su conocimiento los posibles riesgos.

²⁷ <http://www.alliedacademies.org/articles/jiacsvol16si12010.pdf#page=133>. (Guatemala, 26 de noviembre de 2016).



Si la situación se deriva del incumplimiento que obliga a los participantes, es menester dar una respuesta y señalar cuál es la estrategia para seguir ante tal situación ya que negarla o tratar de ocultarla puede complicar la situación misma y agravar la responsabilidad. Evidentemente siempre es imprescindible conocer las normas que regulan cada una de las situaciones particulares.

Asimismo, la pérdida de datos dentro de una empresa puede, por supuesto, ser causada por varios factores, el principal es el mal funcionamiento del hardware. Otras causas principales de estas pérdidas son el desconocimiento de los empleados al usar incorrectamente las herramientas de almacenamiento o por la corrupción de software, virus, desastres naturales y la piratería.

Un gran porcentaje de pérdida de la información se debe al extravío de equipos portátiles, sean computadoras, celulares, agendas electrónicas, discos compactos, memorias USB.

En otros casos estamos ante fugas de información en donde los empleados son los que venden la información confidencial a otras empresas, o un empleado pierde los documentos como se había señalado anteriormente como amenaza por motivación.

Así por un lado habrá que enfrentar en materia de seguridad informática amenazas por motivación de tipo internas derivados por: la falta de integridad de los empleados, el robo de propiedad intelectual, la fuga de información, el espionaje industrial, la



interrupción operacional, algún conflicto entre empelados, el crimen corporativo, conducción de un negocio personal para el cual se extrae la información necesaria o bien por el bajo desempeño del empleado y por otro lado las amenazas por motivación tanto internas como externas de los equipos como es el hackeo y el crimen organizado, los virus, troyanos, worms, exploits, incluso las políticas de seguridad interna.

Es por ello por lo que, el derecho es un componente necesario al momento de hacer frente a las actividades ilícitas que se despliegan en contra tanto de los sistemas informáticos como de la información almacenada en los mismos, sin embargo, aún hoy en día no hay barrera que pueda evitar que la seguridad informática se vea vulnerada sea por amenazas por motivación o bien por amenazas externas como pueden ser los fenómenos naturales.

2.6. La protección de datos personales

Adicional a la seguridad informática, es importante desarrollar la protección de los datos personales, debido que, es un tema relacionado al derecho informático, ya que es de gran trascendencia para la sociedad actual.

Es importante mencionar que: “el reconocimiento de la libertad personal. En este contexto se incorporó el derecho a la intimidad de la persona como una prerrogativa objeto de tutela, ya no sólo en los instrumentos internacionales, sino, además, en sede constitucional”.²⁸

²⁸ González García, Aristeo. **La protección de datos personales: derecho fundamental del siglo XXI.**

Sin embargo, en la situación actual este derecho ha ido variando considerablemente, virtud de que el desarrollo tecnológico ha redimensionado las relaciones del hombre con sus semejantes, así como su marco de convivencia. Hoy, no podemos negarlo, la informática se ha convertido en el símbolo emblemático de la cultura contemporánea.

Por ello, el reconocimiento del derecho a la intimidad en sus diversas manifestaciones luego de lograr su consolidación como un derecho fundamental, ha ido alcanzando nuevos matices.

Ahora, con el tratamiento, la recolección, el almacenamiento de informaciones que antes sólo podía formar parte de la vida íntima de cada ser humano o bien, era conocido por un mínimo sector, ha ido variando paulatinamente su entorno y estructura.

Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados.

Es por ello que el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso de sus informaciones, es decir, de toda aquella información relativa a su persona.

Por tal motivo, el uso y control sobre los datos concernientes a cada persona, debe serle reconocido ya no sólo como una mera prerrogativa, sino además como un derecho fundamentalmente protegido y garantizado por mecanismos de protección idóneos.

El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano entendiéndose por propio y oculto la información que mantiene para sí mismo. Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad el ser humano.

Un derecho tal como ha sido reconocido por las normas puede justificarse por su capacidad de promover ciertos bienes básicos para los ciudadanos: “como es la libertad, la igualdad, la seguridad y otros semejantes. Por lo que desde esta perspectiva puede justificarse la intimidad como un medio para promover la libertad individual”.²⁹

Consecuentemente, frente a una actual sociedad de la información, resulta insuficiente hoy concebir a la intimidad como un derecho garantista estatus negativo de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control sobre el flujo de informaciones que afectan a cada sujeto. Este derecho, en conclusión es consecuencia del desarrollo tecnológico y el creciente almacenamiento de información relativa a la persona, así como la inmersión

²⁹ Peso Navarro, Emilio. **Servicios de la sociedad de la información**. Pág. 52.



cada vez mayor de la misma y de la propia sociedad ha tenido que ir ampliando directrices, ya no sólo dentro de su contexto de los sentimientos, emociones, del hogar, de los papeles, la correspondencia, las comunicaciones telefónicas, video vigilancia, etcétera, sino que además, hoy, es necesario su reconocimiento, y más aún, el establecimiento de mecanismos de protección que puedan hacer frente a su uso y manejo.

Por lo que, la propia noción de intimidad o privacidad es una categoría cultural, social e histórica. Por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica, puesto que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona. Es por ello que al tratarse de un derecho con un carácter abierto y dinámico que está frente a una sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual, se señala acertadamente que el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro de crédito, así como de las reservas de viajes, representan muestras conocidas de la omnipresente vigilancia informática de la existencia habitual de la persona.

En consecuencia, si un derecho a la intimidad en la vida del ser humano ha sido viable; un tratamiento y almacenamiento tecnológico de sus datos, también lo puede ser. Por ende, un derecho a la protección de sus datos personales en pleno siglo XXI, también debe implicar el reconocimiento de este último derecho como fundamental. Por lo que el fenómeno de la intimidad aparece en todas las sociedades humanas. Dado que, las



nuevas tecnologías, al posibilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas y de recopilación de datos, se presentan como una exigencia inaplazable de regulación, que cualquier Estado debe tener en cuenta. Asimismo, cabe señalar que los datos de toda persona deben ser objeto de protección para que éstos puedan ser tratados o elaborados, y finalmente ser convertidos en información, y en consecuencia, sólo ser utilizados para los fines y por las personas autorizadas.

Con base en lo anterior, conviene iniciar el estudio de la protección de datos, desde el primer desafío de las nuevas tecnologías de la información con respecto a la recolección, procesamiento y transmisión de datos personales. Dentro de esta base, el concepto de la intimidad, en el contexto de la sociedad computarizada, concede derechos a los individuos respecto de sus datos personales que son objeto de tratamiento automatizado, e impone obligaciones y deberes de aquellos que controlan y tienen acceso a los ficheros. Para lo cual, atendiendo al interés de proteger la veracidad de los datos y el uso que de ellos se hace, no está relacionado necesariamente con la protección a la intimidad. Sin embargo, el derecho a la protección de datos refleja más que una idea individualista de protección a la intimidad, puesto que engloba los intereses de grupo contra el procesamiento, almacenamiento de información.



CAPÍTULO III

3. Los delitos informáticos

Para generar un mayor conocimiento en cuanto al tema central del presente trabajo de investigación de tesis, es preciso desarrollar a los delitos informáticos que existen y han sido reconocidos.

Debido que, la informática, es una de las ciencias más jóvenes en el contexto de las ramas del conocimiento humano; pero constituye una materia, cuyos avances y desarrollo constantes parecen no tener límites. La informática tiene singular importancia en la época actual, marcada por los adelantos en materia tecnológica y sobre todo en la expansión de las economías a nivel mundial, que poco a poco han ido convirtiendo al mundo en una aldea global, con el presente proceso globalizador que permite la eliminación de las fronteras de tipo social, cultural, arancelarias, económicas y en algunos países, especialmente en los europeos, política; para la plena integración de las culturas de las naciones de los países parte de la globalización .

Sin embargo, en Guatemala no existe un marco legal para la tipificación del ciberdelito, lo que complejiza su abordaje y medición en el país. Es decir, no existe una Ley específica que regule y desarrolle esta materia como tal, únicamente algunos delitos que se encuentran relacionados con la materia informática pero que son generalizados. Asimismo, han sido muy pobres las estrategias que el Estado de Guatemala, ha

formulado para combatir a los delitos que se cometen por medios informáticos.

Esto es importante debido que se debe tomar en cuenta que hoy en día también no se puede solamente utilizar una computadora para cometer esta clase de delitos, ya que con aplicaciones móviles también se han desarrollado diferentes tipos de amenazas para vulnerar la seguridad de diferentes dispositivos y también cometer delitos, como lo son los teléfonos móviles o celulares.

Tomando en cuenta que más de la mitad de los guatemaltecos tienen un celular con posible acceso a internet es importante empezar a dimensionar todos los actos ilegales que se puedan estar cometiendo por el medio tecnológico y de las telecomunicaciones. Derivado a la falta de un marco legal definido la información disponible es limitada, sin embargo, se ha podido recolectar información que da indicios de la problemática.

3.1. Definición

Es importante desarrollar la definición que corresponde conforme a la doctrina de un delito informático, ya que por ser un fenómeno jurídico que se relaciona o deriva de conductas antijurídicas el Estado ha creado diversos medios de protección regulando estas conductas como delitos.

Primeramente, se ha establecido que la conducta delictiva de una persona por medios informáticos ha sido denominada de formas distintas por cada país en su legislación; comprendiendo en la mayor parte de legislaciones que: “la denominación de delito



informático, cibercrimen o delito telemático, se encuadran los hechos que de alguna forma tienen dos componentes básicos siendo estos la existencia de delito y uso de la informática”.³⁰

La primera definición que es preciso mencionar es la que establece que un delito informático es: “el acto delictivo en el que se hace uso de la informática para su comisión bien sea como medio o como fin de este”.³¹

Otra definición lo establece como: “el acto ilícito en el que se usan como medio o como fin para realizarlos, las Tecnologías de la Información y la Comunicación, tales como recursos informáticos, electrónicos, tecnológicos, Internet, entre otros. Es decir, en la comisión de estos delitos se usan las computadoras, los teléfonos inteligentes, software, etcétera, como por ejemplo la falsificación de documentos a través de una computadora o destrucción de información contenida en una computadora”.³²

De manera que, el delito informático es entendido en sus diferentes denominaciones como delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora o delincuencia relacionada con el ordenador.

Algunos códigos penales como el de Perú definen al delito informático como: “el delito que comete una persona que utiliza o ingresa indebidamente a una base de datos,

³⁰ <https://www.ertzaingia.euskadi.eus/lfr/web/ertzaingia/que-es-el-delito-informatico> (Guatemala, 15 de enero de 2017).

³¹ *Ibíd.*

³² <https://www.mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/#q2> (Guatemala, 16 de enero de 2017).

sistema por red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas”.³³

De manera que, la tipificación de un delito tiene que ver con la descripción de actos ilegales que puede ser por acción u omisión, que son considerados como delitos. Suele afirmarse que un acto es típico cuando se puede encuadrar o encajar en un tipo penal, en virtud del principio de legalidad, si un acto encaja en lo tipificado como delito, se considerar como tal.

En ese sentido la tipificación de los delitos informáticos es necesaria, toda vez que se ha evidenciado que, si estas conductas no están establecidas dentro del marco normativo, sea dentro del Código Penal o en una ley especial, las conductas ilegales no podrán ser objeto de sanción, conforme a la vigencia del principio de legalidad.

3.2. Antecedentes

Los delitos informáticos tienen origen generalizado en la sociedad, desde la creación de nuevas tecnologías que intermedian en la comunicación entre las personas trae aparejado nuevas posibilidades para su aprovechamiento indebido e ilícito.

³³ Dávila Laguna. Resultado Legal. <http://www.resultadolegal.com/BFdelitos-informaticos-peru.html> (Guatemala, 25 de enero de 2017).

Eso sucedió desde la creación del telégrafo y también posterior incorporación del teléfono a la vida cotidiana de las personas. Con la irrupción de la computadora personal y la posterior expansión de Internet y la World Wide Web, de modo que: “la capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo de características globales amplió las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales “amigables” y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto así como las posibilidades de anonimato en las comunicaciones”.³⁴

Los orígenes de los delitos informáticos pueden rastrearse a partir de: “los años 60s por el temor infundido por la literatura de la época en relación a la recolección y almacenamiento de datos personales en computadoras. Este tiene como referencia la obra “1984” de George Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías. Tras la publicación de artículos periodísticos sobre algunos de los casos apareció por primera vez del término delitos informáticos o delincuencia relacionada con computadoras, retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como cyberpunk.”³⁵ Durante los años sesenta en pleno, diferentes programadores o especialistas en informática intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio telefónico.

³⁴ Saín, Gustavo. **Evolución Histórica de los delitos informáticos.** <https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina> (Guatemala, 15 de febrero de 2017.)

³⁵ **Ibíd.**



Con el correr del tiempo, estas técnicas de hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales.

Ya durante la década de 1970 se comienzan a registrar una serie de casos que arrojan pérdidas cuantiosas para los sectores privados. A partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión.

En relación con el espionaje, estos se llevaban a cabo mediante la copia directa desde los dispositivos informáticos, el robo directo de los mismos para la extracción de información discos duros, diskettes, y la absorción de emisiones electromagnéticas para la captación de datos.

Los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco espionaje industrial.

Para los casos de sabotaje y extorsión informática, estos eran los delitos que más



preocupaban a las administraciones gubernamentales y empresas ante la concentración de datos almacenados electrónicos.

Los objetivos eran tanto bienes tangibles dispositivos físicos como intangibles datos e información afectando tanto hardware como de software de los dispositivos. En relación a los daños físicos, durante los años setenta se registraron casos de uso de bombas caseras en instalaciones y dispositivos informáticos de empresas por distintos problemas laborales.

En relación con los fraudes financieros producidos a partir del uso de nuevas tecnologías, los primeros casos se empezaron a producir en Estados Unidos a finales de la década de 1970 a partir de los fallos en los sistemas de seguridad de las redes y la inexperiencia de los administradores de dichos sistemas.

A partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas.

Esto motivó la utilización por parte de las empresas emisoras de la adopción de chips en los plásticos como medida de seguridad. Fue justamente durante esta época donde



comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

A fines de esa década comenzaron a aparecer: “contenidos ilícitos y nocivos en las redes tales como amenazas contra las personas, incitación al odio y el intercambio de material de pornografía infantil, tanto, así como actos de violencia y discriminación racista por parte de grupos extremistas. Nuevas técnicas de hacking manipulaban sistemas de vuelo o sistemas hospitalarios y de salud, definidos como ataques contra la vida”.³⁶

Con la apertura global de Internet a mediados de los 90s por parte de la administración norteamericana y el posterior desembarco de las empresas y bancos a la red para el desarrollo del comercio electrónico, la preocupación central pasaba por el desarrollo de estándares de encriptación seguros para el desarrollo de operaciones financieras y la compraventa de productos en línea.

La difusión de imágenes y ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad se empezaron a debatir mediante el uso de nuevas

³⁶ *Ibíd.*



tecnologías.

3.3. Sujetos que involucran los delitos informáticos

En el delito informático una persona participa en la ejecución de una conducta punible, la cual en muchas ocasiones genera el involucramiento de dos personas, un sujeto activo y otro pasivo.

Estos, a su vez, pueden ser: “una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo”.³⁷

Lo anterior es determinable debido que, en el derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.

³⁷ Pérez Luño, Antonio Enrique. **Manual de informática y derecho**. Pág. 36.



El sujeto activo es: “la persona que realiza toda o una parte de la acción descrita tipo penal”.³⁸

De manera que, las personas que cometen los delitos Informáticos son aquellas que: “poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos”.³⁹

En cuanto al sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. Por lo que, se debe distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

Mediante el reconocimiento del sujeto pasivo se pueden conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por

³⁸ Garrido Montt, Mario. **Nociones Fundamentales de la teoría del delito**. Pág. 59.

³⁹ Pérez Luño, Antonio Enrique. **Ob. Cit.** Pág. 41.



el desconocimiento del modus operandi de los sujetos activos.

Esto debido que, la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos.

Asimismo, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas mantengan sin un análisis extensivo.

3.4. Regulación legal de los delitos informáticos

El reconocimiento de las conductas que se han evidenciado en Guatemala ha llevado al legislador a crear tipos penales que encuadren en estas conductas para la aplicación de una sanción por parte de Estado. Dentro del contexto de la regulación jurídica penal, se produce un gran vacío legal toda vez que, en lo concerniente al Código Penal, no se da en ninguno de sus títulos la regulación de los delitos informáticos, lo cual es perjudicial, toda vez que no se protege de manera efectiva a las personas tanto individuales, como a nivel de la industria, de las entidades estatales, y en general a todos aquellos que manipulen de alguna forma datos a nivel informático.



Por lo anterior, se evidencia que el avance del Estado para combatir conductas delictivas por medios informáticos se ha quedado rezagada en cuanto a la realidad que se vive a nivel de los sistemas operativos, toda vez que no se ha producido por parte de los legisladores una reforma estructural al Código Penal Decreto 17-73, a fin de regular de forma taxativa los distintos tipos penales relacionados con los delitos informáticos, pero no se crea un apartado específico para este tipo de delitos.

Si bien es cierto, la gama de delitos informáticos que existen es inmensa, regular de manera efectiva los que se producen en el país, representaría un gran avance en la aplicación de los diferentes tipos penales, toda vez que actuaría como elemento disuasivo entre los delincuentes informáticos, los cuales valiéndose de ciertos conocimientos actúan con total impunidad, escudados en la falta de tipos penales que sancionen este tipo de actuar. La única protección que se ha dado en Guatemala a través del Código Penal ha sido en relación contra el derecho de autor, la propiedad industrial así como en la tipificación de delitos contra la indemnidad sexual de las personas. Dentro de los delitos regulados es preciso mencionar el delito de destrucción de registros informáticos, que es regulado en el Artículo 274 "A", estableciendo que: "Será sancionado con prisión de seis meses a cuatro años y multa de dos mil a diez mil Quetzales, quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos. Si la acción contemplada en el párrafo anterior estuviere destinada a obstaculizar una investigación o procesamiento de carácter penal, el responsable será sancionado conforme al artículo 458 Bis del presente Código".



Asimismo, delito de alteración de programas, la reproducción instrucciones o programas de computación, según el Artículo 274 “C” preceptuado que: “Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación”.

En cuanto al registro de datos prohibidos también se encuentra preceptuado el delito de Registros Prohibidos, tipificado en el Artículo 274 “D”, estableciendo que: “se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas”.⁴⁰

Otros delitos relacionados en esta sección del Código Penal vigente, son el delito de manipulación de información el cual se regula en el Artículo 274 “E” estableciendo que: “Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica”.

En cuanto al uso de información sin autorización se creó el delito de uso de información y el delito de uso de programas destructivos.

40



En cuanto a la regulación del Código Penal para proteger la indemnidad sexual de las personas se tipificó el delito de violación a la intimidad sexual, preceptuado en el Artículo 190 el cual establece: “Quien, por cualquier medio sin el consentimiento de la persona, atentare contra su intimidad sexual y se apodere o capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general o imágenes de su cuerpo, para afectar su dignidad será sancionado con prisión de uno a tres años. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, acceda, utilice o modifique, en perjuicio de tercero, comunicaciones efectuadas por cualquier medio físico o electrónico o datos reservados con contenido sexual de carácter personal, familiar o de otro, que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, en perjuicio de la persona titular de los datos o de una tercera persona. Se impondrá prisión de dos a cuatro años a quien difunda, revele o ceda, a cualquier título, a terceros, los datos o hechos descubiertos o las imágenes captadas a que se refiere este artículo”.

CAPÍTULO IV

4. Creación del perfil psicológico para identificar a una persona que ha cometido una conducta delictiva por medios informáticos en Guatemala

El presente trabajo de investigación de tesis, tiene como finalidad principal, demostrar la importancia de la creación del perfil psicológico de los delincuentes que cometen delitos informáticos para poder identificar con más facilidad a las personas que han cometido estas conductas delictivas por medios informáticos en Guatemala, ya que con la legislación penal vigente y en ausencia de una Ley penal especial que regule los delitos informáticos es difícil para los investigadores que realizan la persecución penal, encontrar un medio eficaz que influya en la identificación de estas personas.

4.1. Utilización de la criminología

Primeramente, es preciso mencionar que en otros países se han utilizado distintos medios y métodos que involucran el estudio y la identificación de los delincuentes cibernéticos. Siendo uno de estos métodos la aplicación de la llamada Criminología plurifactorial se ha ocupado de las particularidades del ciberdelito. Se identifican, de este modo, los factores de riesgo de Internet que pueden derivar en la comisión de hechos delictivos.

Lo anterior debido que se han identificado distintos factores siendo estos los siguientes:

1. Alcance mundial de Internet: “permite a los perpetradores buscar las computadoras y a las víctimas más vulnerables, dondequiera que se encuentren en el mundo, sin tener que salir de sus espacios de seguridad”.⁴¹
2. Desterritorialización: la ciberdelincuencia es: “esencialmente internacional, con retos importantes en términos de jurisdicción y colaboración internacional”.⁴²
3. Subcultura criminal en el ciberespacio: el entorno digital permite la creación de redes flexibles y descentralizadas dentro de las cuales los delincuentes pueden organizarse para dividir el trabajo o compartir competencias, conocimientos o herramientas.
4. Anonimato a los delincuentes: utilizar instrumentos de anonimización. Por otra parte, los delincuentes menos competentes desde el punto de vista tecnológico son relativamente anónimos cuando llevan a cabo sus actividades a gran distancia, ocultos detrás de una dirección IP, un correo electrónico o una cuenta de Facebook fraudulenta, a menudo difíciles de conectar con un individuo específico.
5. La posibilidad de interacciones remotas entre los perpetradores y las víctimas elimina las barreras sociales potenciales con las que se encuentran los perpetradores en las relaciones cara a cara; por lo tanto, la ciberdelincuencia implica relaciones anónimas, ocultas y en red entre las víctimas y los perpetradores.

⁴¹ Arroyo Cámara, Sergio. **Estudios criminológicos contemporáneos: La Cibercriminología y el perfil del ciberdelincuente**. Pág. 480.

⁴² **Ibid.** Pág. 481.



6. El entorno virtual facilita la manipulabilidad de datos y programas a un costo mínimo porque se basa en: “una representación digital que permite copiar sin perder calidad y modificar sin dejar huellas, pero también porque Internet se construyó como una infraestructura abierta, con el fin de fomentar la innovación aportada por sus propios usuarios”.⁴³

7. El entorno online permite la automatización de los procesos y conductas criminales ya que: “un programa difundido por Internet puede lanzar y replicar un ataque millones de veces al mismo tiempo y durante largos períodos de tiempo, y en los que programas muy sencillos también pueden ser fácilmente adaptados por los famosos script kiddies para crear nuevos virus”.⁴⁴

8. Diferente escala criminal: “ya que la ciberdelincuencia puede multiplicar exponencialmente la escala de un delito, que sería mínima en un caso individual, pero que se convierte en un factor de daños importantes debido a su alcance mundial y masivo”.⁴⁵

9. Del mismo modo, la explosión de las escalas permite la acumulación de beneficios individuales no sustanciales gracias a los distintos métodos informáticos de acumulación de datos, en los cuales las transacciones financieras, se van tomando repetidamente de una cuenta y se transfieren a otra. Se trata de uno de los principales desafíos relacionados con la ciberdelincuencia, que reduce al mínimo la presentación

⁴³ **Ibid.** Pág. 482.

⁴⁴ **Ibid.**

⁴⁵ **Ibid.** Pág. 483.

de denuncias, pero también las causas de la investigación y el enjuiciamiento de delincuentes.

10. La información se convierte en un bien valioso en el ciberespacio, en los mercados legales e ilegales.
11. El ciberespacio tiene características estructurales que limitan la posibilidad de controles que sirven, en el mundo real, como barreras sociales y técnicas a la comisión de delitos.
12. El ciclo de innovación en el ciberespacio es particularmente rápido, lo cual permite el desarrollo de nuevas técnicas e instrumentos en plazos muy breves, lo que facilita saltarse las medidas de seguridad y la creación de nuevos vectores y actividades delictivas.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

4.2. El perfil psicológico

La identificación de una persona que ha cometido una conducta delictiva es importante debido que, en la mayoría de las ocasiones el infractor no necesita estar en el lugar físico del delito, pudiendo realizarlo desde otro lugar o país.

También es importante mencionar la velocidad con la que se cometen este tipo de conductas delictivas por medios informáticos. A diferencia del delito común las herramientas son diferentes, dado que el delincuente informático utiliza computadoras, en la mayoría de las ocasiones es difícil encontrar pruebas.

De manera que: “La principal característica que los hace diferentes es que los delitos informáticos requieren alto grado de especialización, se trata de conductas criminales de cuello blanco, ya que son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada por el ámbito tecnológico, refiriéndose principalmente a las vulnerabilidades de cualquier sistema de información”.⁴⁶

El uso de la Psicología para generar un perfil del criminal es beneficioso para la identificación de los criminales debido que la Psicología es: “la ciencia que estudia la conducta y los procesos mentales. Trata de describir y explicar todos los aspectos del pensamiento, de los sentimientos, de las percepciones y de las acciones humanas. Por ser una ciencia, la Psicología se basa en el método científico para encontrar

⁴⁶ Kerlinger Fred y Lee, Howard. **Investigación del comportamiento**. Pág. 254.



respuestas”.⁴⁷

Etimológicamente, es preciso determinar que el término: “Psicología proviene del griego psique: alma y logos: tratado. Literalmente significaría ciencia del alma”.⁴⁸ Sin embargo, se le conceptualiza a la Psicología como una parte de las Ciencias Humanas o Sociales que estudia:

“a) El comportamiento de los organismos individuales en interacción con su ambiente.

b) Los procesos mentales de los individuos.

c) Los procesos de comunicación desde lo individual a lo micro social”.⁴⁹

Lo anterior es importante tomar en cuenta en virtud que el presente trabajo de investigación de tesis busca demostrar la importancia de la creación de perfiles psicológicos de delincuente informáticos.

Para concretar lo anterior es preciso comprender lo que comprende la creación de un perfil psicológico, como antecedentes: “se sabe que durante todo el siglo XX los psicólogos se preocuparon por extender las concepciones ya existentes de psicología, especialmente en medicina, sobre los tipos de contextura física y sus relaciones con

⁴⁷ **Ibíd.** Pág. 256.

⁴⁸ Labake, Julio Cesar. **Introducción a la psicología.** Pág. 10.

⁴⁹ **Ibíd.** Pág. 12.



disposiciones de tipo comporta mental”.⁵⁰

A partir de este conocimiento se diseñaron varios modelos de factores de la personalidad y pruebas para determinar el conjunto de rasgos que caracterizaban a una persona.

La personalidad se entiende como un conjunto organizado de rasgos, es decir comportamientos relativamente permanentes y estables en el tiempo, que caracterizan a un individuo: “Los perfiles psicológicos son también conocidos como perfiles de personalidad. Por lo que, el estudio de la personalidad responde a las preguntas acerca de que tan diferentes son dos personas, que motiva a las personas a actuar de cierta forma e inclusive cual ha sido el desarrollo de cierto individuo en la niñez. Por lo que personalidad puede definirse como las conductas internas que subyacen al comportamiento individual y a la experiencia de la persona”.⁵¹

El perfil psicológico ha sido definido como: “como el conjunto de características y rasgos que deben tener los nuevos empleados que se contraten para desempeñar bien un cargo. Este perfil psicológico se construye tomando en consideración varios factores, comenzando en primer lugar por la descripción de cargo. Cada empresa define las características que deben tener las personas para ocuparan cierto cargo. Y estas características no solamente son técnicas, como el nivel de estudios o la especialización, sino más sutiles, como el tipo de personalidad y el carácter, el nivel

⁵⁰ **Ibíd.** Pág. 16.

⁵¹ Cloninger, Susan. **Teorías de la personalidad.** Pág. 57.

intelectual, etc”.⁵²

Es por ello que, el estudio de la personalidad continúa siendo un tema importante y se configura alrededor de tres modelos vigentes: “el clínico, el correlacional y el experimental. El modelo clínico da prioridad al estudio a profundidad de los individuos. El modelo correlacional busca explorar diferencias individuales mediante estudios de tipo encuesta en grandes muestras de población.

El modelo experimental busca establecer relaciones causa-efecto a partir de la manipulación de variables. Si bien existen diferentes posiciones respecto al nivel de tecnicidad de cada modelo, en la actualidad cada uno de ellos agrupa un conjunto de teorías de gran utilidad para el trabajo aplicado del psicólogo”.⁵³

Por otro lado, considerado desde una perspectiva de criminalística el perfil psicológico es mejor conocido por la práctica que por su nombre mismo, debido a que la determinación del perfil involucra la investigación del comportamiento del delincuente y los motivos que lo llevaron a realizarlo, siendo el perfil psicológico una de las herramientas más importantes para la investigación en un intento por orientar la investigación.

El análisis de los hábitos y rituales del criminal permite a los investigadores localizar las similitudes con los crímenes anteriores, para realizar esto los investigadores utilizan

⁵² **Ibíd.** Pág. 61.

⁵³ **Ibíd.** Pág. 62.

tanto enfoques inductivos como deductivos. En el enfoque deductivo se asume que cuando una persona realiza un delito, dicha persona tendrá razones similares, sino es que razones iguales para cometer dicho delito.

Sin embargo, estas asunciones han sido fuertemente cuestionadas. El enfoque deductivo representa un proceso que evita la generalización y los promedios, este método implica un estudio exhaustivo de los sospechosos.

Desde un punto de vista puramente psicológico, el perfil se define como: “un informe en forma de diagrama de varias puntuaciones de una persona en escalas presumiblemente comparables donde se han utilizado técnicas proyectivas. O una serie de puntuaciones que pueden ser puestos en forma de diagramas.

Una prueba psicológico constituye esencialmente una medida objetiva tipificada de una muestra de conducta. Un test es una técnica sistemática que compara la conducta de dos o más personas”.⁵⁴

Con base en la definición anterior, se puede enunciar que el perfil psicológico se determina en base al patrón de puntuaciones de una persona en varias partes de un test de personalidad.

⁵⁴ **Ibíd.** Pág. 65.

4.3. Herramientas para determinar perfiles psicológicos

El uso de herramientas para determinar perfiles psicológicos ha sido un método eficaz en otros países que utilizan los mismos para identificar de una manera más rápida a los presuntos delincuentes informáticos que cometen delitos informáticos en la sociedad.

Existen varias herramientas que son utilizadas como ayuda para identificar diversos tipos de perfiles psicológicos y así saber si es conveniente o no integrar al candidato al grupo de trabajo. Es tan amplio el tema de psicología, que para poder identificar los perfiles psicológicos se necesitan aplicar muchos instrumentos, tales como test, cuestionarios o encuestas, y a su vez cada uno sirve para determinar solo un aspecto del aspirante.

Por ello existen distintos tipos de test o herramientas para definir la personalidad, inteligencia o coeficiente intelectual de una persona, asimismo, la determinación de perfiles psicológicos exige evaluar diversos aspectos como la personalidad del individuo, a continuación, se describirán algunas de estas herramientas:

a) MMPI: “Este test consiste en 550 afirmaciones que el sujeto debe clasificar como Verdaderas o Falsas, si es que son aplicables o no a sí mismo, los resultados obtenidos corresponden a su puntaje en cuatro escalas de validez, que tienen como propósito detectar actitudes desviadas al responder al test y que permiten evaluar lo



confiables que son las respuestas de la persona evaluada”.⁵⁵

Este test se puede aplicar en forma individual o colectiva y tiene tres formas de aplicación: “cuadernillo de tapas blandas o duras, el cual consiste en un cuadernillo que contiene impresas en la primera página las instrucciones y en las siguientes las 550 afirmaciones que forman el test; se le entrega además a la persona a evaluar una hoja de respuestas donde debe marcar si la afirmación es Verdadera o Falsa al ser aplicada a él”.⁵⁶

Otra forma de aplicación es mediante el uso de tarjetas las que encuentran ordenadas en una caja: “que incluye las instrucciones en su tapa. Además, esta caja contiene tres tarjetas más grandes con las etiquetas, falso, verdadero y no sé”.⁵⁷

La última forma de aplicación de este test, es mediante la utilización de formas abreviadas. La forma abreviada que más es aceptada consiste: “en aplicar sólo aquellos enunciados que forman parte de las Escalas de validez y de las Escalas clínicas básicas. Para este caso, en la forma colectiva se instruye al sujeto para que responda las primeras 366 afirmaciones y 33 aseveraciones adicionales que están dispersos en el cuadernillo. Obviamente un procedimiento de este tipo implica dificultades para el sujeto que puede confundirse y para el examinador, ya que si agrupa juntos los enunciados que el sujeto debe responder, debe cambiar algunas

⁵⁵ Labake, Julio Cesar. **Ob. Cit.** Pág. 35.

⁵⁶ **Ibíd.** Pág. 38.

⁵⁷ **Ibíd.** Pág. 39.

plantillas de corrección”.⁵⁸

b) Test de Cleaver: este proporciona una descripción completa de la personalidad del individuo, haciendo énfasis en sus aptitudes para realizar diferentes labores sociales, su capacidad para desenvolverse con otras personas y relacionarse con ellas. Para ello se realiza un pronóstico de la forma en que este individuo reacciona ante determinadas circunstancias y también de sus reacciones y actitudes típicas bajo situaciones de presión; se sugiere que tipo de actividad realizaría con más eficiencia y qué cosas motivan al individuo, orientando sus necesidades y preferencias. Finalmente, se describen las tendencias de la actitud de este individuo en situaciones bajo presión y se enumeran sus preferencias y necesidades.

En general esta descripción completa que brinda este test sobre una persona permite evaluar su capacidad para desempeñar determinada labor social y proporciona a sus superiores una visión general de lo que puede esperarse de ella y de las condiciones que deben rodear a este individuo para que pueda obtener los mejores resultados en su trabajo.

Estos test son aplicables para descifrar el perfil psicológico, sin embargo, se sabe que las características de un delincuente informático son completamente diferentes a las características de un delincuente común, siendo su valía tecnológica una de las principales diferencias con los delincuentes comunes, el establecimiento de características varía con relación al tipo de delito que se comete.

⁵⁸ **Ibíd.** Pág. 42.

El objetivo del uso de estos test para la creación del perfil psicológico tiene que ver con la sugerencia de los patrones de comportamiento y características más significativas para cada tipo de delincuente informático. Adicionalmente, se ha propuesto una herramienta que apoye en la determinación de una posible tendencia asociada a un delincuente informático. A pesar de que la delincuencia informática se considera como un tipo de delincuencia de cuello blanco, donde es difícil encontrar y juzgar al culpable debido a la complejidad de los sistemas de información para ofrecer evidencias palpables, algunos culpables han sido condenados y durante su condena han sido observados.

4.4. Creación de perfiles psicológicos para delincuentes informáticos

Para culminar con el análisis referente a la creación de perfiles psicológicos para la identificación de delincuentes informáticos, se ha comprobado que, en la mayoría de las ocasiones, los delincuentes informáticos son personas que están involucradas con otras personas, organizaciones o estructuras criminales. El estudio de métodos y mejores prácticas para prevenirla ha sido una constante para los expertos en seguridad. Pero es indispensable ampliar el campo de investigación.

La determinación de los perfiles psicológicos de delincuentes informáticos ofrece una gran oportunidad para el Estado y para la investigación criminal del flagelo de los delitos informáticos, ya que con ello es posible identificar a una persona que genere conductas con posible tendencia a ser un delincuente informático, la prevención ha sido el mejor



aliado en la lucha de la delincuencia informática. De manera que, en el presente trabajo de investigación queda demostrada la importancia de la aplicación de estos perfiles informáticos para la aplicación de una justicia pronta en contra de las personas que practican este tipo de conductas delictivas por medios informáticos.



CONCLUSIÓN DISCURSIVA

En el presente trabajo de investigación se buscó establecer que la creación de un perfil psicológico es fundamental para la identificación de una persona que ha cometido una conducta delictiva por medios informáticos.

Por lo que, el presente trabajo de investigación utilizó como base de la misma al derecho penal y al derecho informático, demostrando con ello que su aplicación en Guatemala no es fundamentada por una Ley penal especial. Esta conclusión se evidenció con el análisis de la regulación legal actual y pobre que establece algunos delitos informáticos en el Código Penal, los cuales no fueron creados de forma independiente para atacar las conductas delictivas por medios informáticos, evidenciando con ello una debilidad en la normativa penal vigente.

Con base a esta debilidad, se plantea la creación de perfiles psicológicos para identificar de una mejor forma a las personas que ejecutan mediante medios informáticos hechos delictivos que conlleva el daño tanto a una persona, grupos de personas o al mismo Estado.

Para la comprobación de la hipótesis se utilizaron los métodos de investigación analítico, sintético, lógico para determinar las variantes de investigación científica, asimismo el método de investigación inductivo y deductivo para generar las conclusiones, por lo que, se concluye que la creación de perfiles psicológicos puede ayudar a lograr una asociación de los patrones de personalidad que permiten establecer las diferencias entre los tipos de delincuentes informáticos para su identidad.





BIBLIOGRAFÍA

AGUILAR, Alfonso Pablo. **¿Derecho informático o informática jurídica?** México: Ed. Universidad Nacional Autónoma de México –UNAM–, 2015.

ARROYO CÁMARA, Sergio. **Estudios criminológicos contemporáneos: La Ciber criminología y el perfil del ciberdelincuente.** España: UNED, 2017.

BUSTOS RAMÍREZ, Juan. **Manual de derecho penal.** Barcelona, España: Ed. Ariel, 1989.

CLONINGER, Susan. **Teorías de la personalidad.** México: Ed. Prentice Hall México, 2003.

CUELLO CALÓN, Eugenio. **Derecho penal.** Barcelona, España: Ed. Bosch, 1988.

DÁVILA LAGUNA. Resultado Legal. <http://www.resultadolegal.com/BFdelitos-informaticos-peru.html> (Guatemala, 25 de enero de 2017).

DE LEÓN VELASCO, Héctor Aníbal, DE MATA VELA, José Francisco. **Derecho penal guatemalteco.** Guatemala: Ed. Magna Terra, 2015.

GARRIDO MONTT, Mario. **Nociones Fundamentales de la teoría del delito.** Chile: Ed. Jurídica de Chile, 1992.



GÓMEZ VIEITES, Alvaro. **Seguridad Informática**. Madrid, España: Ed. Ra-Ma, 2011.

GONZÁLEZ GARCÍA, Aristeo. **La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado**.
<https://www.scielo.org.mx/scielo.php?script=sci>. (Guatemala, 30 de noviembre de 2016.)

<http://www.alliedacademies.org/articles/jiacsvol16si12010.pdf#page=133>. (Guatemala, 26 de noviembre de 2016).

<https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza/que-es-el-delito-informatico>
(Guatemala, 15 de enero de 2017).

<https://www.mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/#q2> (Guatemala, 16 de enero de 2017).

<https://www.repositorio.pucp.edu.pe/index/bitstream/handle/lasfuentesdelderechopena1.pdf> (Guatemala, 18 de diciembre de 2016).

JIMÉNEZ de Asúa, Luis. **Lecciones de derecho penal**. México: Ed. Mexicana, 1997.

KERLINGER Fred y LEE, Howard. **Investigación del comportamiento**. México: Ed. Mc. Graw Hill, 2002.

LABAKE, Julio Cesar. **Introducción a la psicología**. Argentina: Ed. Bonum, 2004.

PÉREZ LUÑO, Antonio Enrique. **Manual de informática y derecho**. Barcelona, España: Ed. Ariel, S. A., 1996.



PESO NAVARRO, Emilio. **Servicios de la sociedad de la información.** Madrid España: Ed. Diez de Santos, 2011.

SAÍN, Gustavo. **Evolución Histórica de los delitos informáticos.** <https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina> (Guatemala, 15 de febrero de 2017.)

SÁNCHEZ LASCUARÍN, Juan Antonio, CANCIO MELIÁ, Manuel, BASSO J. Gonzalo. **Manual de introducción al derecho penal.** Madrid, España: Ed. Agencia Estatal Boletín Oficial del Estado, 2012.

SIERRA, YHORMAN. <https://www.blog.lemontechjurisprudencialatam.com/derecho-informatico/> (Guatemala 17 de agosto de 2016).

TÉLLEZ VALDÉS, Julio. **Derecho informático.** México: Ed. McGraw-Hill, 2004.

ZAFFARONI, Eugenio Raúl. **Tratado de derecho penal.** México: Ed. Cárdenas, 1998.

Legislación:

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

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