

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



**IMPLEMENTACIÓN DE UNA FISCALÍA ESPECIALIZADA CONTRA EL
CIBERCRIMEN EN EL MINISTERIO PÚBLICO EN LA REPÚBLICA DE
GUATEMALA**

ANDREA EB'ECH CH'EW MENDOZA MENDOZA

GUATEMALA, JULIO DE 2024

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

**IMPLEMENTACIÓN DE UNA FISCALÍA ESPECIALIZADA CONTRA EL
CIBERCRIMEN EN EL MINISTERIO PÚBLICO EN LA REPÚBLICA DE
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

ANDREA EB'ECH CH'EW MENDOZA MENDOZA

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, julio de 2024

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

DECANO: M.Sc. Henry Manuel Arriaga Contreras

VOCAL I: Vacante .

VOCAL II: Lic. Rodolfo Barahona Jácome

VOCAL III: Lic. Helmer Rolando Reyes García

VOCAL IV: Lic. Javier Eduardo Sarmiento Cabrera

VOCAL V: Br. Gustavo Adolfo Oroxom Aguilar

SECRETARIO: Licda. Wilfredo Eliú Ramos Leonor

**TRIBUNAL QUE PRACTICÓ EL EXAMEN
TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lic. Marco Vinicio Villatoro.

Vocal: Licda. Aura Marina Donis Molina.

Secretario: Lic. Enrique Rolando Huitz Enríquez.

Segunda Fase:

Presidente: Licda. Yina Ardón.

Vocal: Lic. Edson Waldemar Bautista.

Secretario: Lic. José Luis de León Melgar.

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



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala



Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,
quince de junio de dos mil veintiuno.

Atentamente pase al (a) Profesional, WILBER JOEL NAVARRO VÁSQUEZ
_____, para que proceda a asesorar el trabajo de tesis del (a) estudiante
ANDREA EB'ECH CH'EW MENDOZA MENDOZA, con carné 201014582,
intitulado IMPLEMENTACIÓN EN EL MINISTERIO PÚBLICO DE UNA FISCALÍA ESPECIALIZADA CONTRA EL
CIBERCRIMEN EN LA REPÚBLICA DE 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.

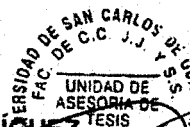
El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de
concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y
técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros
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.



ASTRID JEANNETTE LEMUS RODRIGUEZ
Vocal I en sustitución del Decano.

Fecha de recepción 17/09/2021

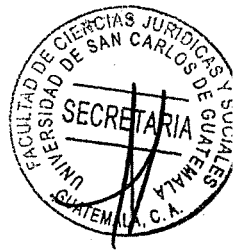


Abogado y Notario

Asesor(a)
(Firma y Sello)



LIC. WILBER JOEL NAVARRO VÁSQUEZ
ABOGADO Y NOTARIO
6 av. 3-11 Zona 4
Ciudad de Guatemala
Tel. 24730685- 532121203



Guatemala 28 de febrero de 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
Su despacho.



Respetable Doctor Carlos Herrera

En atención a la providencia emitida por esta unidad con fecha quince de junio del año dos mil veintiuno, en el cual se me nombra **asesor** de tesis de la bachiller **ANDREA EB'ECH CH'EW MENDOZA MENDOZA**, quien se identifica con el número de Carné 201014582. Declaro que no tengo ningún impedimento legal ni moral para desempeñar el cargo de asesor, no soy pariente de la estudiante ni ella tiene relación de dependencia con el suscrito. Se le brindó la asesoría de su trabajo de tesis INTITULADA **"IMPLEMENTACIÓN EN EL MINISTERIO PÚBLICO DE UNA FISCALÍA ESPECIALIZADA CONTRA EL CIBERCRIMEN EN LA REPÚBLICA DE GUATEMALA."** Luego de varias sesiones de trabajo se obtuvo la versión final de la investigación y en su oportunidad sugerí algunas correcciones de tipo gramatical y de redacción; que consideré que en su momento fue necesario para mejor comprensión del tema que se desarrolla; asimismo fue oportuno cambiar el título de esta; quedando de la siguiente manera: **"IMPLEMENTACIÓN DE UNA FISCALÍA ESPECIALIZADA CONTRA EL CIBERCRIMEN EN EL MINISTERIO PÚBLICO EN LA REPÚBLICA DE GUATEMALA."**

Hago constar que se realizó un análisis documental y jurídico en materia de derecho informático, penal y constitucional, en el lapso de la asesoría, así como en el desarrollo del trabajo de tesis, la estudiante manifestó sus capacidades en investigación, utilizando técnicas y métodos deductivo e inductivo, analítico, sintético y la utilización de las técnicas de investigación bibliográfica y documental que comprueba que se realizó la recolección de bibliografía acorde al tema.

La contribución científica oscila en la recolección de información de diferentes leyes comparadas, que será legalmente hablando de gran apoyo a todas las personas que

LIC. WILBER JOEL NAVARRO VÁSQUEZ
ABOGADO Y NOTARIO
6 av. 3-11 Zona 4
Ciudad de Guatemala
Tel. 24730685- 532121203

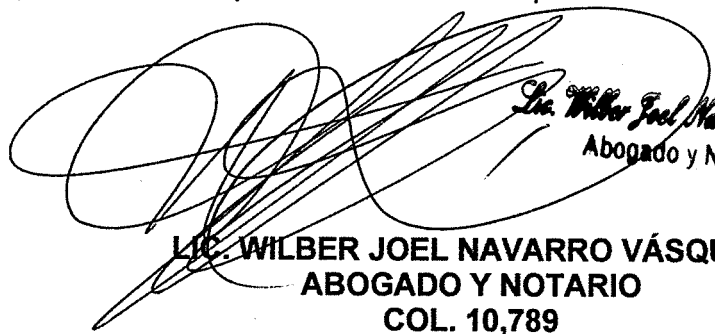


decidan proponer iniciativas de ley; abarcó las instituciones jurídicas relacionadas a los temas desarrollados, definiciones y doctrinas, así como el marco legal de la materia, el cual puede servir de base para otros trabajos de investigación en las diferentes ramas del derecho.

La estudiante aceptó las sugerencias realizadas durante la elaboración de la tesis, y aportó al trabajo sus propias opiniones y criterios, los cuales lo enriquecen, sin embargo, pueden ser no compartidos y sujetos a polémica, no obstante, se encuentran fundamentados, puesto que son planteamientos serios y ordenados que demuestran un buen manejo de criterio jurídico sobre la materia. Con respecto a la conclusión discursiva mi opinión es que es acorde al tema investigado y la utilización de la técnica de investigación bibliográfica que comprueba que se hizo la recolección de bibliografía actualizada.

Por lo expuesto **OPINO** que el trabajo del bachiller **ANDREA EB'ECH CH'EW MENDOZA MENDOZA**, se ajusta a los requerimientos científicos y técnicos que se deben cumplir de conformidad con las normativa respectiva, la metodología y técnicas de investigación utilizadas, la redacción, la conclusión discursiva y bibliografía utilizada, son congruentes con los temas desarrollados dentro de la investigación, por lo que al haberse cumplido con los requisitos mínimos establecidos en el Artículo en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y Examen General Público, resulta procedente emitir el **DICTAMEN FAVORABLE**, aprobando el trabajo asesorado.

Con muestra de mi consideración y estima, me suscribo, como atento y seguro servidor, no dejando la oportunidad de aprovechar la ocasión para reconocer el excelente trabajo de la ponente.

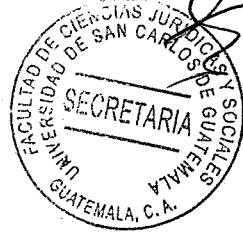


Lic. Wilber Joel Navarro Vásquez
Abogado y Notario

LIC. WILBER JOEL NAVARRO VÁSQUEZ
ABOGADO Y NOTARIO
COL. 10,789



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

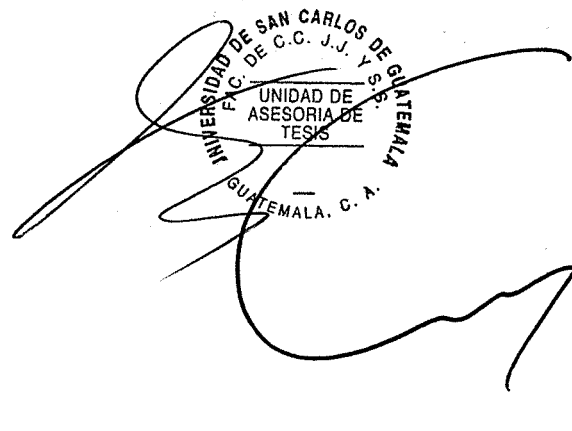


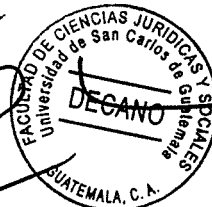
D. ORD. 80-2024

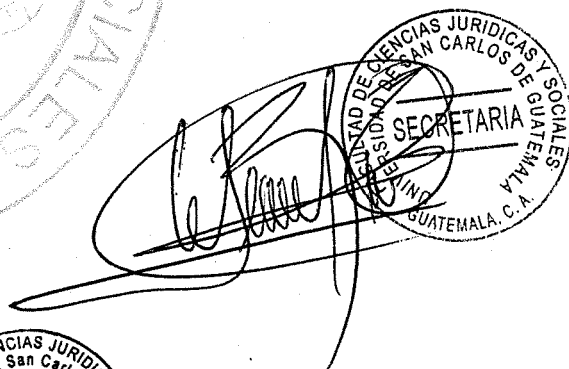
Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, veintiséis de enero de dos mil veinticuatro.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **ANDREA EB'ECH CH'EW MENDOZA MENDOZA**, titulado **IMPLEMENTACIÓN DE UNA FISCALÍA ESPECIALIZADA CONTRA EL CIBERCRIMEN EN EL MINISTERIO PÚBLICO EN LA REPÚBLICA DE 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.

HMAC/JIMR


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




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





DEDICATORIA

A DIOS:

Quien es mi guía, mi luz y mi fortaleza. Por permitirme llegar hasta aquí y por brindarme la oportunidad de alcanzar esta meta.

A MI PADRE:

Andrés Mendoza Matías a quien llevo en mi mente y en mi corazón y sé que desde el cielo comparte la alegría de este logro, a él por su amor, por su ejemplo de lucha y de superación. Con mucho amor y admiración para mi papá. Como una muestra de amor para honrar su memoria.

A MI MADRE:

Faustina Mendoza Pérez, quien es padre y madre para mi, a ti por el apoyo incondicional en esta meta y en todos los aspectos de mi vida. A ti por cada uno de tus esfuerzos, para que hoy yo pudiera estar aquí, Te amo.

A MIS HERMANOS:

Azucena por apoyarme y motivarme, por creer en mi y porque siempre cuento contigo, Andrés y Guillermo por su cariño y apoyo incondicional en cada etapa de mi vida. Los quiero mucho.

A MI CUÑADA:

Norma Kuchudakis y a mi sobrino Guillermo Alejandro por apoyarme y animarme en este proceso.



A MI FAMILIA:

Tíos y primos, por su cariño, por su apoyo y buenos consejos.

A MIS ABUELITOS:

Quienes creyeron en un mejor futuro para sus nietos, este logro es fruto de sus sacrificios y oraciones. Gracias.

A:

Horacio Ruiz Matamoros, quien ya se encuentra en presencia de Dios, a él por su apoyo incondicional en mi vida, familia y carrera profesional. Con cariño y admiración.

A:

La gloriosa Tricentenaria Universidad de San Carlos de Guatemala, por darme la oportunidad de haber sido una estudiante sancarlista y por haber sido el centro de estudios donde realicé mis sueños.

A:

La Facultad de Ciencias Jurídicas y Sociales, por los valiosos conocimientos adquiridos y por formarme como profesional del derecho.



PRESENTACIÓN

Este trabajo pertenece a la rama del derecho informático, penal y administrativo, por ello se utilizó el método cualitativo, pues en el mismo se logra determinar la necesidad de la implementación de una fiscalía especializada contra el cibercrimen en el Ministerio Público en la República de Guatemala.

El objeto de estudio fue el cibercrimen, en virtud que en Guatemala el Ministerio Público no está preparado y capacitado para actuar contra los delitos informáticos o ataques cibernéticos, estos delitos se ejecutan a través de plataformas digitales lo cual hace más difícil su investigación.

El sujeto de estudio es la necesidad de implementar en el Ministerio Público una fiscalía especializada contra el cibercrimen, con el propósito de realizar estudios e investigaciones sobre delitos informáticos y así lograr pronta acción debido al incremento de los ciberdelitos en el país.

El periodo está comprendido desde el mes de mayo del año 2021, al mes de marzo del año 2022 debido a la complicación en recaudación de información en el Ministerio Publico.

Por lo anterior el presente trabajo de tesis servirá como aporte académico a la Universidad de San Carlos de Guatemala, a estudiantes de la Facultad de Ciencias Jurídicas y Sociales como instrumento para el estudio y comprensión sobre la importancia de la implementación de una Fiscalía Especializada contra el cibercrimen en el Ministerio Publico que garantice el esclarecimiento y la investigación de los delitos ejecutados a través de medios informáticos e impedir que queden impunes por no contar con infraestructura equipo humano y tecnológico necesario.



HIPÓTESIS

Para la sociedad guatemalteca es sumamente importante que el Ministerio Público por mandato constitucional tenga la responsabilidad de los delitos relacionados con la informática, actualmente no existe una legislación específica aplicable a los delitos cibernéticos y el ente investigador no cuenta con una fiscalía especializada contra el ciberdelito.



COMPROBACIÓN DE HIPÓTESIS

La hipótesis del presente trabajo se comprobó aplicando el método analítico, por medio del cual se ordenó la recopilación de doctrina y la legislación relacionada; el método cualitativo, mediante el análisis de los delitos cibernético y su efecto en la sociedad; el método de interpretación, de gran ayuda para rescatar el sentido de las normas jurídicas en la legislación consultada exponiendo para el efecto la importancia de la implementación de una fiscalía especial en contra del cibercrimen dentro del Ministerio Público, con el fin de garantizar el proceso de investigación y esclarecimiento del delito cibernético, además con la implantación de la fiscalía especial se tendrá el equipo adecuado en infraestructura, equipo tecnológico y equipo humano, asimismo, capacitación y actualizaciones constantes al ente investigador y personal del Organismo Judicial, Ministerio Público y Policía Nacional Civil, específicamente a fiscales, direcciones de investigaciones y jueces, para que desde ya se comience a hacer un trabajo en conjunto en contra del cibercrimen.



ÍNDICE

Pág.

Introducción	i
--------------------	---

CAPÍTULO I

1. Ministerio Público	1
1.1. Definición del Ministerio Público	2
1.2. Funciones del Ministerio Público	5
1.3. Características del Ministerio Público	8
1.4. Principios que rigen el Ministerio Público	9
1.5. Organización del Ministerio Público	9
1.6. El Ministerio Público dentro de la administración pública	10
1.7. Regulación legal de la función del Ministerio Público	12
1.8. Objetivos generales y estratégicos del Ministerio Público	14
1.9. El ejercicio de la acción penal	15
1.10. Principal función investigativa del Ministerio Público	16
1.11. Actuación del Ministerio Público dentro del proceso penal guatemalteco	17

CAPITULO II

2. Derecho informático	19
2.1. Definición	21
2.2. Objeto y método	24
2.3. Características	24
2.4. Principios del Derecho Informatico	26
2.5. Fuentes	27
2.6. El bien jurídico tutelado	29
2.7. Contenido del derecho informático	30
2.8. Diferencia entre derecho informático e informática jurídica	32

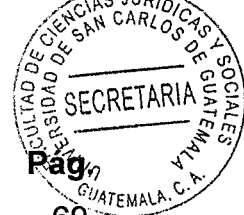
2.9. La informática.....	33
2.10. La informática jurídica.....	35

CAPÍTULO III

3. Delito informático.....	37
3.1. Definición de los delitos informáticos.....	39
3.2. Naturaleza y objeto.....	42
3.3. El bien jurídico tutelado en los delitos informáticos.....	43
3.4. Sujetos del delito informático.....	46
3.5. Características de los delitos informáticos.....	47
3.6. Elementos esenciales del tipo en el delito informático.....	48
3.7. Clasificación de los delitos informáticos.....	49

CAPÍTULO IV

4. Implementación de una fiscalía especializada contra el cibercrimen en el Ministerio Público en la república de Guatemala.....	53
4.1. Investigación del cibercrimen en Guatemala.....	55
4.2. La informática forense.....	57
4.3. La evidencia informática.....	60
4.4. El Ministerio Público y su función ante los delitos informáticos.....	62
4.5. La importancia de la aplicación de la informática dentro del derecho penal guatemalteco.....	63
4.6. La tecnología de información y comunicaciones respecto de la garantía de las personas en la persecución de delitos informáticos.....	65
4.7. Los principios del derecho respecto de la garantía de los derechos de las partes en la informática.....	65
4.8. Impacto de los delitos informáticos.....	67
4.9. La seguridad informática.....	68



4.10. El delito informático y su realidad procesal en Guatemala.....	69
4.11. Seguridad contra los delitos informáticos.....	71
4.12. La metodología de la investigación del Ministerio Público en los delitos informáticos.....	73
4.13. El procesamiento de la escena del crimen en los delitos informáticos.....	74
4.14. Inconvenientes en la investigación y el proceso pericial ante los delitos informáticos.....	77
4.15. Legislación nacional relativa al ciberdelito.....	78
4.16. Aporte al presente trabajo.....	80
 CONCLUSIÓN DISCURSIVA	 87
BIBLIOGRAFÍA	89

INTRODUCCIÓN

El presente trabajo abordará la necesidad de la implementación de una fiscalía especializada contra el cibercrimen en el Ministerio Público en la República de Guatemala, en virtud de que el cibercrimen es toda aquella actividad delictiva que se ejecuta a través de una computadora (o dispositivo de red) y que lo utiliza directa o indirectamente, esta forma de ejecutar delitos, experimenta un fuerte apogeo a nivel internacional, que contrasta con la débil preparación de las autoridades para hacerles frente.

La fiscalía especializada contra el cibercrimen es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o fraudes presentados.

En Guatemala no existe una fiscalía especial contra el cibercrimen dentro del Ministerio Público, es por ello la necesidad de creación y acción de esta, dentro del ente investigador y así poder brindar ciberseguridad a la población guatemalteca ya que la gravedad y complejidad del fenómeno, su relevancia nacional e internacional y su constante crecimiento tornan necesario potenciar la actuación del Ministerio Público en la materia, ampliando su capacidad de intervención y profundizando todos los ejes de trabajo que se vienen desarrollando.

El objetivo general de la investigación fue: Establecer la importancia de la implementación de una fiscalía especializada contra el cibercrimen en el Ministerio Público en la República de Guatemala, en el mismo se logró evidenciar que la implementación de esta fiscalía hace posible una investigación especializada que permitirá y facilitará la recaudación de pruebas y la detención de los ciberdelincuentes evitando con ello que dichos casos queden impunes.

Para el desarrollo del trabajo se utilizaron los siguientes métodos de investigación: cualitativo, analítico, sintético, inductivo, deductivo; y las técnicas de investigación empleadas fueron la documental y la científica jurídica.

Esta tesis está contenida en cuatro capítulos, de los cuales el primero, tiene como propósito el estudio del Ministerio Público dentro de la administración pública, sus principios, organización y función dentro del proceso penal; el segundo, trata las nociones generales del derecho informático sus fuentes, principios y características; en el tercero, se define el delito informático, sus características y el bien jurídico tutelado que violenta; el capítulo cuarto, se determina la importancia de la implementación de una fiscalía especializada contra el cibercrimen en el Ministerio Público, las deficiencias, obstáculos y la falta de capacidad del ente investigador al ejercer la persecución penal en los delitos cibernéticos.

Guatemala actualmente no se encuentra preparada para combatir la ciberdelincuencia ya que el Ministerio Público presenta carencia y deficiencias como equipo técnico y personal capacitado para la persecución e investigación dichas actividades delictivas, el presente trabajo de investigación analiza y evidencia que es necesario e indispensable la implementación de una fiscalía especial contra el cibercrimen en el Ministerio Público ya que permitirá la eficaz y eficiente acción del ente investigador para contrarrestar la ciberdelincuencia. Así también el presente trabajo puede utilizarse como instrumento de estudio y comprensión para futuras investigaciones.

CAPÍTULO I

1. Ministerio Público

La importancia del Ministerio Público como ente investigador y acusador estatal reside en su injerencia en el ámbito legal que le da origen y la necesidad de su implementación y funcionamiento como principal apoyo a la lucha contra la criminalidad y la impunidad, actuando atenta y constantemente dentro del proceso penal guatemalteco, llevando un control sobre los resultados y avances de dichas investigaciones y actuaciones judiciales que a medida de su evolución, acrecientan su eficiencia en el alcance de sus objetivos.

Es una institución auxiliar de la administración pública y de los tribunales encargada según la Constitución Política de la República de Guatemala, el Código Procesal Penal y la Ley Orgánica que rige su funcionamiento, del ejercicio de la acción penal pública, así como de la investigación preliminar para preparar el ejercicio de la acción.

El Ministerio Público es una institución que, con su actuación objetiva y apego al principio de legalidad contribuye a la modernización de la administración de justicia y a la consolidación del Estado de derecho.

Su misión es promover la persecución penal, la investigación de los delitos de acción pública, garantiza los derechos de las víctimas y vela por el estricto cumplimiento de las leyes del país y su visión es ser una institución eficiente, eficaz y transparente, que, con apego al principio de legalidad, contribuya a la consolidación del Estado de derecho.

El Ministerio Público es una entidad gubernamental la cual tiene como función esencial ejercer la acción penal en nombre de la sociedad, en todos aquellos en los que la ley le asigna competencia, con el objeto de recabar todos aquellos elementos para demostrar

si una persona ha participado o no en la comisión de un hecho delictivo, al Ministerio Público se le atribuye dentro de un estado de derecho democrático, la representación de los intereses de la sociedad mediante el ejercicio de las facultades de dirección de la investigación de los hechos que revisten los caracteres de delito, de protección a las víctimas y testigos, y de titularidad y sustento de la acción penal pública.

El Ministerio Público es el principal auxiliar de la justicia y de la administración pública, esta institución controla el estricto desempeño de las leyes guatemaltecas, también conduce las investigaciones de delitos y promueve la persecución penal, este en el ejercicio de sus funciones se desenvuelve con estricto apego a la ley, siempre trabajando con objetividad, imparcialidad y autonomía.

El jefe del Ministerio Público será el fiscal general y le corresponde el ejercicio de la acción penal pública. Deberá ser abogado colegiado y tener las mismas calidades que los magistrados de la Corte Suprema de Justicia y será nombrado por el Presidente de la República de una nómina de seis candidatos propuesta por una comisión de postulación, integrada por el Presidente de la Corte Suprema de Justicia, los decanos de las facultades de Derecho o de Ciencias Jurídicas y Sociales de las Universidades del País, el presidente de la Junta Directiva del Colegio de Abogados y Notarios de Guatemala y el Presidente del Tribunal de Honor de dicho Colegio.

1.1. Definición del Ministerio Público

Comenta que el Ministerio Público "es la institución unitaria y jerárquica dependiente del organismo ejecutivo y posee funciones como la intervención en otros procesos judiciales para la defensa de interés sociales, de ausentes, menores e incapacitados, y finalmente, como consultor y asesor de los jueces y tribunales."¹

¹ Ferreira Delgado, Francisco. **El Ministerio Público**. Pág. 295.

El Ministerio Público es el órgano encargado de cooperar en la administración de justicia velando por el interés del Estado, de la sociedad y de los particulares, mediante el ejercicio de las acciones pertinentes que le son asignada por la ley, haciendo observar el cumplimiento de las leyes y promoviendo la investigación y persecución de los delitos.

Expresa que al Ministerio Público también “es llamado Ministerio Fiscal es la institución estatal encargada, por medio de sus funcionarios (fiscales) de defender los derechos de la sociedad y del Estado es la institución estatal encargado, por medio de sus funcionarios de defender los derechos la sociedad y del Estado.”²

El Ministerio Público es la fiscalía u órgano acusador del estado, como representante de la sociedad, monopoliza el ejercicio de la acción penal, en nombre del Estado. Como representante de la sociedad, el Ministerio Público no persigue ningún interés propio, ni ajeno, sino que realiza llanamente la voluntad de la ley.

Refiere que el Ministerio Público “es una institución estatal de carácter público, quien actúa en defensa de los intereses sociales, ejerciendo las acciones penales y civiles para el resarcimiento y sanción de una conducta humana delictiva a través del proceso penal. Es la institución auxiliar de la administración pública encargada de la investigación y persecución de los delitos de índole pública velando por el estricto cumplimiento del ordenamiento jurídico guatemalteco que ejerce sus funciones acordes a lo establecido en la Constitución Política de la República de Guatemala y otras leyes.”³ La función que el Estado le designa al Ministerio Publico de ejercer la acción penal permite la intervención de este dentro de los procesos Judiciales para la investigación y esclarecimiento de hechos delictivos.

La Constitución Política de la República de Guatemala en su Artículo 251, define al

² Binder, Alberto. **Funciones y disfunciones del Ministerio Público**. Pág. 109.

³ Couture, Eduardo. **Vocabulario jurídico**. Pág. 385.

Ministerio Público de la siguiente forma, “El ministerio Público es una institución auxiliar de la administración pública y de los tribunales con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país. Su organización y funcionamiento se regirá por su ley orgánica.

Expone que el Ministerio Público como “es el organismo del Estado que realiza funciones judiciales ya sea como parte o como sujeto auxiliar en las diversas ramas procesales, especialmente en la penal, y que contemporáneamente efectúa actividades administrativas, pues como consejero jurídico de las autoridades gubernamentales, realiza la defensa de la legalidad.”⁴ El Ministerio Público desempeña la función judicial al presentarse ante los tribunales de justicia como parte o como sujeto auxiliar en los procesos.

La definición del Ministerio Público de Guatemala, reviste singulares características, toda vez que siempre se ha mantenido una trayectoria ligada a la órbita del Poder Ejecutivo, y sus funciones han sido simples y la vida histórica de la institución no es tan larga, se puede decir que el Ministerio Público aparece regulado dentro del Artículo 251 de la Constitución Política de la República de Guatemala el cual establece que el Ministerio Público es una institución auxiliar de la administración pública y de los tribunales de justicia.

La Ley Orgánica del Ministerio Público, Decreto Número 40-94 del Congreso de la República de Guatemala, lo define así: “El Ministerio Público es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por el estricto cumplimiento de las leyes del país. En el ejercicio de esa función, el Ministerio Público perseguirá la realización de la justicia, y actuará con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece.”

⁴ Garrone, José Alberto. **Diccionario manual jurídico**. Pág. 185.

El Ministerio Público es una institución moderna creada por el Estado para realizar la investigación en los hechos delictivos, tal como lo concibe su Ley Orgánica emanada de la reforma constitucional y procesal penal que le dio un giro sustancial a su existencia, se habla de institución con funciones autónomas procedente de las facultades que se le confirieron con exclusividad por parte del Estado.

1.2. Funciones del Ministerio Público

Hace hincapié al referirse a las funciones del Ministerio Público estableciendo “son las atribuciones que desempeñan un Órgano del Estado. El ejercicio de un Órgano o la actividad de un aparato, desempeño de un cargo, facultad de un oficio o tarea, ocupación, atribución, finalidad, acto público, hacer funciones, ejercer determinado cargo y/o suplir a un superior.”⁵ Las funciones del Ministerio Público son el conjunto de actividades que el Estado le designa y para las cuales fue creada, tiene encomendado promover ante los tribunales la acción de la justicia especialmente mediante la acusación penal y la defensa de la legalidad y del interés público tutelado por la ley.

La función del Ministerio Público es investigar y ejercer la acción penal lo que hace necesario emitir una nueva Ley Orgánica del Ministerio Público, que refleje la nueva realidad procesal de manera que la institución pueda cumplir con las funciones que dicho cuerpo legal le confiere.

El Artículo 2 de la Ley Orgánica del Ministerio Público, nos indica las funciones del Ministerio Público, sin perjuicio de las que le atribuyen otras leyes, las siguientes:

- Investigar los delitos de acción pública y promover la persecución penal ante los tribunales, según las facultades que le confiere la Constitución, las leyes de la República, los tratados y convenios internacionales.

⁵ Palomar De Miguel, Juan. **Diccionario para juristas**. Pág. 160.

- Ejercer la acción civil en los casos previstos por la ley, y asesorar a quien pretenda querrellarse por delitos de acción privada, de conformidad con lo que establece el Código Procesal Penal.
- Dirigir la Policía y demás cuerpos de seguridad del Estado, en la investigación de hechos delictivos.
- Preservar el Estado de derecho, y el respeto de los derechos humanos, efectuando las diligencias necesarias ante los tribunales de justicia. La ley le ha encomendado al Ministerio Público las anteriores funciones, y le determinará con precisión su ubicación institucional, manteniendo su relación con las demás instituciones del Estado, garantizando que no se abuse del poder que se le otorga, y de la autonomía que la ley le confiere.

El Artículo 24 BIS del Código del Código Procesal Penal le asigna al Ministerio Público la acción pública para que se realice la persecución penal de oficio, salvo los hechos perseguibles sólo a instancia de parte como lo son: la calumnia, la injuria, difamación y los que están condicionados a instancia particular o autorización estatal. Ejemplo los delitos de estupro, abusos deshonestos y violación. El ejercicio de la acción penal pública es único y le corresponde únicamente al Ministerio Público. La persecución penal, es asumida por el Ministerio Público, quien acusa en nombre del Estado de Guatemala.

Es aquí donde se establece el ejercicio de la acción penal, la investigación consistente en la serie de actividades para descubrir elementos que permitan el ejercicio fundado en la acción penal para la persecución del delito, y la sanción del delincuente.

El fiscal tiene que estar informado desde el momento de la detención, y estar presente en la primera declaración del imputado. El juez, juzga con base en las pruebas

aportadas, decide en materia penal si conforme al derecho sustantivo se ha cometido o no un acto tipificado en la ley.

El Ministerio Público deberá practicar todas las diligencias pendientes y útiles para determinar la existencia del hecho. Establecerá los partícipes y el conocimiento de circunstancias personales, las cuales servirán para valorar la responsabilidad, verificando el daño causado, si el fiscal decide proseguir la persecución penal, solicita al juez la aplicación de alguna medida coercitiva hacia el presunto imputado, y el juez, resolverá ordenando prisión preventiva o una medida sustitutiva, si el juez no estuviere de acuerdo con lo pedido, podrá rechazar la petición del Ministerio Público.

Si el Ministerio Público no encuentra suficientes méritos para proseguir con la persecución penal, solicitará al juez el archivo, el sobreseimiento o la clausura provisional de la denuncia, la querella o la prevención policial. El juez por su parte podrá admitir lo solicitado por el Ministerio Público y remitirá las actuaciones nuevamente; en caso contrario, si el juez dispone que se ejercite la persecución penal, y en su caso, dictar alguna medida de coerción, o alguna medida sustitutiva; el Ministerio Público puede ejercer la persecución penal aun cuando se haya dictado falta de mérito, y la debe ejercer cuando se dicte alguna medida sustitutiva.

Ejercer la acción civil, en los casos previstos por la ley: Le dará asesoría a quien pretenda querellarse, la acción civil deberá ser ejercitada antes que el Ministerio Público requiera la apertura del juicio, o sobreseimiento, vencida esta Oportunidad, el juez la rechazará sin más trámite. El Ministerio Público en cuanto a sus funciones y estructura, ha tenido cambios dividiendo las funciones en secciones separadas, hasta llegar al conocido Decreto Número 40-94 del Congreso de la República, es decir, la Ley Orgánica del Ministerio Público, la que actualmente está en vigencia. Al igual que toda institución Pública o Estatal, cuenta con secciones como: Procuraduría, Archivo, Contabilidad, Biblioteca, Bodega, y Almacén.

1.3. Características del Ministerio Público

Es una Institución, por ser el Ministerio Público el órgano principal del Estado, encargado de la acción penal pública, según la Constitución Política de la República de Guatemala, el Código Procesal Penal y la Ley Orgánica. Su función es autónoma porque actúa independientemente y en cumplimiento de las funciones que le atribuyen las leyes, no está subordinado a ninguno de los organismos del estado, sólo lo que establece la ley, según el Artículo 3. Decreto Número 40-94, Ley Orgánica del Ministerio Público. El Ministerio Público promueve la persecución penal, teniendo a su cargo el procedimiento preparatorio, y la dirección de la policía en su función investigativa:

- Investigación preliminar para preparar el ejercicio de la acción penal. Por medio de la investigación de delitos de acción pública; por delegación expresa del Estado,
- El Ministerio Público, actúa en representación de este, siendo una premisa básica, en el sistema acusatorio en el nuevo código Procesal Penal, la acción penal se regula como un deber del Estado de perseguir delitos que afecten intereses públicos.
- Velar por el estricto cumplimiento de las leyes del país. El Ministerio Público persigue la realización máxima de la justicia y deberá ejercer sus funciones con objetividad, imparcialidad y con apego al Principio de Legalidad.

Doctrinariamente, se asocian al Ministerio Público las características fundamentales de:

- Unidad, mediante la cual se determina que, aunque un ente esté conformado por varias personas, todas ellas conforman un solo órgano y están sometidas a una misma dirección.

- Indivisibilidad, característica que identifica la facultad de que el órgano acusador sea representado por cualquiera de los funcionarios que lo conforman y que tengan los requisitos legales para hacerlo.
- Independencia, además de ser un principio fundamental en los Estados Democráticos, es una característica que establece la total ausencia de vínculo alguno de sujeción a otro organismo o poder del Estado, sino únicamente a la ley.
- Jerarquía, característica que hace énfasis al orden interno que existe entre los funcionarios que integran el Ministerio Público, pues están adscritos en posición subordinada al jefe superior.

La regulación legal del Ministerio Público en Guatemala arroja un balance positivo en cuanto a las características señaladas. En el Artículo 5 de su Ley Orgánica, establece las características de unidad, indivisibilidad y jerarquía; y en el artículo 3 resalta la característica de autonomía funcional.

1.4. Principios que rigen el Ministerio Público

El Ministerio Público es un Órgano que tiene encomendado promover ante los tribunales la acción de la justicia, especialmente mediante la acusación penal y la defensa de la legalidad y del interés público tutelado por la ley. Los principios en que se rige el Ministerio Público son la unidad, la jerarquía, imparcialidad y la objetividad.

1.5. Organización del Ministerio Público

El Ministerio Público es una institución auxiliar de la administración pública y de los tribunales de justicia, cuyos fines principales son velar por el estricto cumplimiento de las leyes de Guatemala, así como la investigación y persecución de los delitos catalogados de acción pública velando por los intereses de la sociedad.

Menciona que el Ministerio Público “se encuentra integrado por los siguientes órganos el fiscal General de la República, Consejo del Ministerio Público, fiscales de distrito, fiscales de sección, fiscalía de delitos administrativos, fiscalías, agentes fiscales, auxiliares fiscales.”⁶ Los órganos del Ministerio Público están integrados jerárquicamente, cada uno con determinadas atribuciones que permiten el cumplimiento de sus funciones.

El Ministerio Público es la institución encargada de cooperar en la administración de justicia, velando por el interés del Estado, de la sociedad y de los particulares mediante el ejercicio de las acciones pertinentes, haciendo observar las leyes, y promoviendo la investigación y represión de los delitos, es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además vela por el estricto cumplimiento de las leyes del país.

1.6. El Ministerio Público dentro de la administración pública

El rol que juega el Ministerio Público dentro de la administración pública guatemalteca refleja la importancia de su actuar ya que como se enuncia a sí mismo como institución, auxilia la labor investigativa y acusatoria frente a los tribunales de los hechos punibles de índole pública, es decir, que afectan a la colectividad frente al creciente flagelo de la delincuencia y la impunidad en el contexto de los problemas de seguridad ciudadana que enfrenta el país en la actualidad y el temor meramente generalizado que cunde en la sociedad.

En este contexto, planteada la insatisfacción que el ejercicio de la acción penal produce en quienes han sufrido los efectos de algún delito y de quienes se consideran desamparados al momento de sufrir alguno, se debe luchar contra la delincuencia

⁶ Cárdenas Díaz, Irma Lucrecia. **El Ministerio Público en su función controladora de legalidad.** Pág. 287.

conjuntamente con otros cuerpos de seguridad con el que cuenta la República de Guatemala como lo son la Policía Nacional Civil por excelencia al servicio de la seguridad ciudadana permitiendo la efectiva administración de justicia y con ello el fortalecimiento de la credibilidad del sistema democrático en el aspecto que brinde certeza y seguridad de su actividad inquisitoria, con el fin de elevar la efectividad institucional y estatal.

Por mandato constitucional, se enfoca al Ministerio Público como auxiliar de la administración pública, lo cual conduce de manera inmediata a cuestionarse sobre el por qué, es decir, por qué motivo y en qué momento actúa este ente auxiliando a la administración pública en el entendido que, se le ha facultado para ejercer la investigación preliminar de los hechos delictivos de acción pública así como la acusación formal resultante de las investigaciones mencionadas con el fin de garantizar sus objetivos y alcanzar eficientemente su cometido.

Ministerio Público actuará independientemente, por su propio impulso y en cumplimiento de las funciones, como una institución auxiliar de la administración pública y de los tribunales de justicia.

Por lo anterior, se puede mencionar que el Ministerio Público es una Institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por el estricto cumplimiento de las leyes del país. En el ejercicio de esa función, el Ministerio Público perseguirá la realización de la justicia, y actuará con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece.

Se le considera como órgano auxiliar por su actividad coadyuvante del sistema estatal en la aplicación de las disposiciones necesarias para el cumplimiento de las leyes y la conservación y fomento del interés público en que están enfocados por una parte, su misión la cual enuncia: promover la persecución penal, dirigir la investigación de los

delitos de acción pública y velar por el estricto cumplimiento de las leyes del país y, por la otra parte su visión: ser una institución eficiente, eficaz y transparente, que con apego al principio de legalidad, contribuya a la consolidación del Estado de derecho.

En ese orden de ideas, teniendo al Ministerio Público como auxiliar de la administración pública a través del ejercicio de las funciones que se le imputan, a su vez, cabe resaltar, que cuenta con la colaboración de otras autoridades administrativas y organismos del Estado y de sus entidades descentralizadas, autónomas o semiautónomas tal como lo establece el Artículo seis de su Ley Orgánica que enuncia esta relación como la vinculación de esta institución con las demás que presten su colaboración y auxilio cuando así les realice el debido requerimiento en determinadas situaciones, estando estos obligados a prestarla sin demora y proporcionar los documentos e informes que les sean requeridos.

De esta manera se abarca la administración pública que ejerce el Ministerio Público derivado de la potestad que posee emanada de las leyes a efecto se desenvuelva con la autonomía que le es propia a su naturaleza jurídica desarrollada en este escrito anteriormente; así como el desapego de otras dependencias del Estado actuando en favor del desahogo laboral que suele concentrarse en los tribunales del país en su faena por aplicar la ley y la justicia mediante la persecución de actos punibles, descentralizando tales acciones que le competen al Estado en lo que se conoce como administración pública en el ámbito inquisidor, esto con el objeto de fomentar el progreso y el seguimiento de los procesos ventilados judicialmente a su cargo.

1.7. Regulación legal de la función del Ministerio Público

Es importante hacer mención que primordialmente se establece el marco legal del Ministerio Público, el cual proporciona las bases sobre las cuales la institución se erige y determina el alcance y naturaleza de su participación en el ámbito nacional, del cual se hace el recuento siguiente:

- a) Constitución Política de la República de Guatemala.
- b) Ley Orgánica del Ministerio Público, Decreto 40-94 del Congreso de la República de Guatemala.
- c) Código Procesal Penal, Decreto Número 51-92 del Congreso de la República de Guatemala.

El Ministerio Público es una institución pública de carácter constitucional, derivado que la base legal de su creación, organización y funcionamiento están fundamentados en la Constitución Política de la República de Guatemala según lo estipulado por el Artículo 251 que expresa lo siguiente: El ministerio Público es una institución auxiliar de la administración pública y de los tribunales con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país, es el único ente encargado de la persecución penal y dirige las investigaciones por medio de la policía nacional civil y demás cuerpos de seguridad, el Ministerio Público trabaja con el fin de la realización de la justicia adhiriéndose a las leyes guatemaltecas.

El Decreto Numero 40-94 del Congreso de la República de Guatemala, el que dicta la normativa respectiva y sienta la base legal propia del Ministerio Público empezando primeramente por los considerandos, los razonamientos que justifican jurídicamente la parte dispositiva del cuerpo legal, es decir, los que motivaron a la creación de esa fuente legal y que llevan implícito el hecho de la sustitución del Decreto Número 512 del Congreso de la República de Guatemala para que se adecúe a las formas de la Constitución Política de la República de Guatemala y que cumpla eficientemente con las funciones que le atribuye.

El nuevo Código Procesal Penal, Decreto Número 51-92 del Congreso de la República de Guatemala le asigna al Ministerio Público la función de investigar y ejercer la acción

penal, por lo que fue necesario emitir una nueva Ley Orgánica del Ministerio Público que reflejara la nueva realidad procesal de manera que la institución pudiera cumplir con las funciones que dicho cuerpo legal le confiere consolidando el estado de derecho garantizando la pronta y efectiva justicia penal con lo que, además, se asegura la paz y la seguridad ciudadana así como el respeto a los derechos humanos.

1.8. Objetivos generales y estratégicos del Ministerio Público

Tal como se ha ido desarrollando el contexto institucional del Ministerio Público, es fundamental conocer a fondo sus funciones y objetivos por medio de los cuales busca incesante el alcance de su misión y en el cual veremos cimentados los principios que lo rigen en su actuar y que en adelante se conocerán.

Asimismo, esta institución se encuentra enmarcada en el Artículo 107 del Código Procesal Penal indicando: "Función. El ejercicio de la acción penal corresponde al Ministerio Público como órgano auxiliar de la administración de justicia conforme las disposiciones de este código. Tendrá a su cargo el procedimiento preparatorio y la dirección de la policía nacional civil en su función investigativa dentro del proceso penal." El Ministerio Público se encuentra regulado de forma general en la Constitución Política de la República de Guatemala en su artículo 251, de forma especial en su Ley Orgánica y su función investigativa dentro del proceso penal lo regula el Código Procesal Penal Decreto Numero 51-92 del Congreso de la Republica.

También la propia Ley Orgánica del Ministerio Público Decreto 40-94 del Congreso de la República de Guatemala, señala su definición en el Artículo uno, así como sus funciones que debe desarrollar en su investigación, su organización, su régimen financiero y administrativo.

De todos es sabido que el Ministerio Público como sujeto auxiliar y procesal de un juicio penal, actúa en representación y defensa de la sociedad, le corresponde actuar al

producirse la noticia de un delito, investigar la misma, reuniendo todos los elementos necesarios para fundamentar su pretensión al momento de formular su acto conclusorio, ya que precisamente, su función es investigar los delitos de acción pública y promover la persecución penal.

1.9. El ejercicio de la acción penal

El proceso penal tiene como finalidad inmediata la averiguación, determinación y valoración de hechos delictivos, el establecimiento, en sentencia, de la participación del imputado y la determinación de su responsabilidad y la pena que le corresponde, así como la ejecución de esta. Mientras que se puede considerar como finalidad mediata del proceso penal la búsqueda de la actuación de la ley para lograr el fin supremo de justicia y paz social; puesto que el proceso penal moderno es un mecanismo de redefinición de conflictos individuales o sociales causados por hechos delictivos, lo que faculta implementar en ciertos casos, salidas diferentes a la de la pena para restaurar la tutela de bienes jurídicos y la convivencia social.

Por lo anterior, es que la reforma constitucional vigente desde 1993, otorgó al Ministerio Público el deber y el derecho de perseguir de oficio, en representación de la sociedad, los delitos de acción pública, aspecto básico del sistema acusatorio que separa la función de juzgar y la de acusar. Por ello, corresponde al Ministerio Público promover la investigación de delitos para los fines del proceso penal y ejercer, en nombre de la sociedad, la acción penal pública, para lo cual debe actuar sometido al principio de legalidad.

Es decir, que le corresponde la función de provocar e instar la actividad jurisdiccional del Estado y de propiciar que ésta se desarrollara a través del juez natural mediante los procedimientos establecidos en la ley, planteando las pretensiones que corresponda, de acuerdo con el principio de legalidad.

Es bajo este principio de legalidad que el Artículo 47 de la Ley Orgánica del Ministerio Público establece que en el ejercicio de sus funciones los fiscales estarán sujetos únicamente a la Constitución Política de la República de Guatemala, los Tratados y Convenios Internacionales, la ley y las instrucciones dictadas por su superior jerárquico, en los términos establecidos por la ley orgánica.

Sin embargo, como garantía al principio de legalidad, el Artículo 68 de la ley orgánica, regula que el fiscal que recibiera una instrucción que considere contraria a la ley, lo hará saber a quién emitió la instrucción, la remitirá, dentro de las veinticuatro horas siguientes, sin efecto suspensivo, junto con la objeción al superior jerárquico inmediato en el servicio, quien decidirá. Para ello, éste podrá escuchar a una junta de fiscales bajo su dirección o en casos complejos, solicitar dictamen al Consejo del Ministerio Público.

1.10. Principal función investigativa del Ministerio Público

El Ministerio Público es la institución auxiliar de la administración pública encargada de la investigación y persecución de los delitos de índole pública velando por el estricto cumplimiento del ordenamiento jurídico guatemalteco que ejerce sus funciones acordes a lo establecido en la Constitución Política de la República de Guatemala.

El Código Procesal Penal le asigna al Ministerio Público la función de investigar y ejercer la acción penal lo que hace necesario emitir una nueva Ley Orgánica del Ministerio Público, que refleje la nueva realidad procesal de manera la institución pueda cumplir con las funciones que dicho cuerpo legal le confiere.

Tal como en un principio, se atribuyó al Ministerio Público determinadas acciones y funciones por el mencionado cambio del que se ha hablado en el transcurso del presente texto, se le dio a este ente, en Guatemala aunado a la función principal inquisidora, primordialmente la función investigativa de los hechos constitutivos de un tipo penal en la legislación, en el supuesto en que en reiteradas oportunidades se ha

tenido una idea relativamente desviada de esta institución respecto de sus funciones por parte de la población que ven a la institución únicamente como inquisidora.

En otras palabras, ven a la institución como un querellante, siendo el caso que en realidad, el Ministerio Público no tiene ni debe tener un interés directo en la sentencia, ya sea esta condenatoria o absolutoria, sino más bien en lograr el esclarecimiento y la conducción a la verdad de los hechos que motivan un enfrentamiento judicial en los tribunales de la República basado en los medios de prueba que resulten de la investigación de la que se discute en este apartado, la que debe efectuarse con la pericia necesaria y adecuada para la obtención legal y correcta de los medios de investigación que llegan a fungir como prueba dentro del juicio.

Respecto de la obtención adecuada de los medios de investigación se desprende el presente estudio en virtud de la observancia de los protocolos establecidos para el efecto en el entendido que el seguimiento al pie de la letra de estos lineamientos, el Ministerio Público podría contar con elementos probatorios obtenidos de manera eficiente, legal para que en su oportunidad, sean examinados por el juzgador y forme su criterio respecto de la valoración de los mismos, ya que de esta manera la prueba al ser aceptada e introducida al proceso cumple con su objetivo.

El Ministerio Público únicamente podrá informar sobre el resultado de las investigaciones siempre que no vulnere el principio de inocencia, el derecho a la intimidad y la dignidad de las personas; además cuidará de no poner en peligro las investigaciones que se realicen. Deberá dirigir sus acciones tomando en cuenta los intereses de la víctima a quien deberá brindar amplia asistencia y respeto.

1.11. Actuación del Ministerio Público dentro del proceso penal guatemalteco

Corresponde al Ministerio Público ejecutar la acción pública dentro del proceso penal guatemalteco aferrándose a sus principios propios y los principios del proceso penal en



Guatemala, partiendo de su actuar como querellante y en su caso, acusador en los delitos de índole pública así como las demás facultades que le son atribuidas que en ningún momento deben sobrepasar ni confundirse con la de los jueces, en otras palabras.

El Ministerio Público no tiene la capacidad de declarar derechos por ser esta, facultad única y especialmente conferida a los jueces y magistrados que constituyen la Corte Suprema de Justicia como tal, en respuesta de la pretensión del actor.

En ese orden de ideas, tiene el Ministerio Público la función de provocar la actividad jurisdiccional del Estado y de propiciar que esta se desarrolle a través del juez mediante los procedimientos establecidos en la ley, planteando las pretensiones que correspondan de acuerdo con el principio de legalidad que lo rige.

CAPITULO II

2. Derecho informático

La informática como una ciencia que estudia el procesamiento lógico y automático de la información ha sido empleada en todas las actividades del ser humano, en busca de una mejor eficiencia y de un trabajo más rápido.

El derecho informático es la rama del derecho que regula los efectos jurídicos derivados de la informática y de las Tecnologías de Información y Comunicación (TIC); se especializa, además, en el estudio de las transformaciones del derecho como consecuencia del uso generalizado de las actividades tecnológicas.

El derecho informático cumple un rol importante en la prevención de situaciones no deseadas para los usuarios de las nuevas tecnologías de la información y cuando se presentan determinadas circunstancias que los afecten, facilita la incorporación de nuevas instituciones jurídicas que permitan crear confianza a las personas e instituciones que realizan tales operaciones, permitiendo de esta forma la solución de aquellos problemas generados por el uso de los medios electrónicos en la sociedad.

El derecho informático adquiere gran importancia por el desarrollo de un número cada vez mayor de elementos informáticos, electrónicos, ópticos y similares, que facilitan la vida del hombre, pero a su vez, le generan serias dificultades en su interacción con los demás seres humanos, surgiendo de esta manera una serie de circunstancias que permiten el desarrollo, fortalecimiento y perfeccionamiento del Derecho informático y sus instituciones jurídicas.

El derecho Informático va adquiriendo mayor importancia en los tiempos modernos, en vista que permite obtener las soluciones legales adecuadas a los problemas generados

por el uso de la informática en sociedad. El derecho también ha tenido que adaptarse a la llegada y evolución de Internet y las TIC (Tecnologías de la Información y la Comunicación), puesto que ha sido necesario (y sigue siendo necesario) regular jurídicamente estos ámbitos para evitar que se cometan abusos y delitos o se pueda sancionar aquellos que se han cometido. Por ese motivo existe el derecho informático.

El derecho informático y las nuevas tecnologías van de la mano, el ámbito de aplicación de esta rama del derecho es muy amplia; más allá de los crímenes cometidos a través de la informática, también se aplica en el derecho a la privacidad, el honor y la propia imagen, la protección de datos, las redes sociales, el comercio electrónico, la seguridad informática, la publicidad online, la defensa de los consumidores, la regulación del teletrabajo, los trámites telemáticos o los certificados y firmas digitales. En definitiva, el derecho informático está ahí donde las nuevas tecnologías nos han llevado a necesitar nuevas regulaciones y normativas para asegurar la seguridad jurídica de todos los interesados.

En el derecho informático se puede observar, la aparición de un fenómeno social que es la informática, creada por el hombre como un instrumento esencial para superar las dificultades generadas por la aceleración del progreso, y el derecho el receptor de los fenómenos sociales, surgiendo así múltiples relaciones entre ambos, impulsando la necesidad de adaptarse a la incorporación de estas relaciones en el ámbito jurídico.

Sé considera que el derecho informático es un punto de desviación o inclinación del derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la sociedad de la información, cambiando de este modo los procesos sociales, como los jurídicos, se observa en esta materia o rama del derecho, normas y procedimientos que están destinados a mediar los actos que nacen a causa del uso de la informática.

Entre el derecho y la informática, existen dos tipos de enfoques: El primero, hace referencia a lo instrumental, es decir, lo referente a la informática jurídica como

instrumento. El segundo, hace referencia a la informática como objeto del derecho. Al hacer un breve análisis relativo al derecho y la informática, en sus inicios existía una simple relación como herramienta instrumental para facilitar la vida cotidiana, en la actualidad su uso se va haciendo cada vez más indispensable en el desarrollo de los países y sistemas económicos, que, con la evolución tecnológica, se van haciendo de uso cotidiano.

Sin embargo, al considerar la informática como objeto del derecho se hace alusión al derecho informático en sí mismo, haciéndose imperante establecer la diferencia que existen para su mejor comprensión. La informática se caracteriza por ser un ámbito muy cambiante, esta ciencia jurídica analiza las modificaciones de la informática y/o las TICs respecto a la sociedad, con la finalidad de crear principios y normativas que logren regularla adecuadamente.

2.1. Definición

Establece que el derecho informático “es la rama del derecho que recoge aquellas normas que regulan los efectos jurídicos de la relación entre el derecho y la informática. Es una disciplina de las ciencias de la información que tiene por objeto la aplicación de la informática en el derecho, es la regulación jurídica de las nuevas tecnologías.”⁷

El derecho informático es la ciencia que estudia el empleo de los recursos informáticos para mejorar los procesos, análisis, investigación y gestión en el ámbito jurídico, es decir, es el empleo de software y hardware como instrumentos del derecho, para agilizar los procesos legales. No se trata de una rama del derecho, sino de las herramientas que se pueden utilizar dentro de este campo, como por ejemplo, lexnet, el sistema de gestión de notificaciones telemáticas desde los juzgados a los abogados.

⁷ Azpilcueto Hermilio, Tomas. **Derecho informático**. Pág. 180.

Refiere que el derecho informático “es un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el derecho y la informática, esta actividad involucra aquello referente a la contratación informática, delitos cometidos mediante su uso, relaciones laborales a que ella da lugar, litigios sobre la propiedad de programas o datos.”⁸

El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, teniendo en su haber (al menos hasta la fecha) incipientes antecedentes a nivel histórico; la interrelación entre el derecho y la informática, se crean unas relaciones intersubjetivas entre las personas naturales o jurídicas y de entes morales del Estado, y surgen entonces, un conjunto de reglas técnicas conectadas con el derecho, que vienen a construir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la ciencia informática con autonomía propia.

Hace hincapié al mencionar que el derecho informático “comprende el conjunto de doctrinas, principios e instituciones y normas, que regulan los bienes jurídicos que la informática crea y las acciones y/o responsabilidades de las personas derivadas del uso de la tecnología.”⁹

La sistematización de los programas tecnológicos ha permitido simplificar, organizar y agilizar, una gran variedad de actividades en el mundo moderno, lo que también ha propiciado un desarrollo significativo en distintas ciencias. Esta herramienta tecnológica, es imprescindible para la implementación de nuevos métodos de investigación, coadyuva en la búsqueda del desarrollo social y económico de las naciones, en pro de sus habitantes.

Expone que el derecho informático es una nueva rama del derecho que estudia las

⁸ Davara Rodríguez, Miguel Ángel. **Derecho informático**. Pág. 206.

⁹ Flores Salgado Lucerito, **Derecho informático**. Pág. 359.

normas jurídicas que regulan la conducta en las relaciones que surgen como producto del uso de la informática entre los seres humanos de una época y sociedades determinadas; así como los principios, doctrinas, técnicas e instituciones que determinan la manera de crear, modificar, interpretar y aplicar dichas normas jurídicas.”¹⁰

El derecho informático es la ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos, no se dedica al estudio del uso de los aparatos informáticos como ayuda al derecho, sino que constituye un conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. En otras palabras, que la informática en general desde este punto de vista es objeto regulado por el derecho.

Refiere que el derecho informático “es una rama de las ciencias jurídicas, que contempla a la informática tanto como instrumento (informática jurídica), como objeto de estudio (derecho informático), es la ciencia que basándose en los métodos de abstracción de procesos e interactuando con las normas legales, aplicaciones y relaciones jurídicas, permite el estudio objetivo de las incidencias del derecho en las actividades electrónicas (comercio electrónico, nombres de dominio, firma digital, el fraude electrónico).”¹¹

El derecho informático, como nueva creación jurídica, se encarga de buscar soluciones a los retos planteados por la evolución de las aplicaciones de las computadoras electrónicas. Esta rama del derecho está en constante seguimiento y estudio de los avances, adelantos y transformaciones tecnológicas a fin de ir planteando las medidas adecuadas que permitan una armónica convivencia social.

¹⁰ Tellez Valdés, Julio. **Derecho informático**. Pág. 96.

¹¹ Díaz García, Alexander. **Derecho informático, elementos de la informática jurídica**. Pág. 149.

2.2. Objeto y método

El derecho informático es una nueva disciplina Jurídica que tiene como objeto inmediato de estudio la informática y como objeto mediato la información. Su método científico se caracteriza por desarrollar las instituciones jurídicas informáticas e interrelacionarlas sistemáticamente con la realidad; así, se tiene que los problemas derivados del software, de la información computarizada, del hardware, firmware, shareware y otros bienes, son tratados desde sus distintos alcances en el ordenamiento legal, buscando coherencia y tratamiento integral.

El objeto de estudio del Derecho Informático no se ve afectado por la existencia de situaciones eventuales, sino que, por el contrario, su autonomía se va reforzando en el tiempo. La tecnología de la información puede permitir cambios esenciales en la labor jurídica permitiendo que se cumplan las aspiraciones de celeridad, precisión, mayor conocimiento y transparencia.

2.3. Características

Algunas de las características generales que se encuentra en el derecho informático se puede mencionar:

- a) Surge como consecuencia de las nuevas tecnologías de la Información.
- b) Es consustancial a la Informática Jurídica.
- c) Regula los bienes informáticos.
- d) A diferencia de otras ramas jurídicas, no es estático, se encuentra en movimiento permanente según la evolución de las nuevas tecnologías de la información.

- e) Es un Derecho moderno, (en comparación con otras ramas tradicionales del Derecho), ya que tiene sus orígenes en los problemas generados por la implementación de la computadora y la informática en la sociedad.
- f) Es un derecho íntimamente influenciado por las tecnologías en general, ya que esta se encarga de buscar soluciones a los retos planteados por la evolución de las aplicaciones de las computadoras electrónicas.
- g) Es un derecho que necesariamente debe ser legislado en leyes especiales, debido a que su objeto de estudio, así como sus formas de regulación son muy dinámicas.
- h) Es un derecho autónomo, con instituciones propias que se encarga de brindar soluciones legales a los problemas planteados por el avance científico en el ámbito de su competencia. Es importante indicar, que conforme transcurre el tiempo surgen nuevas dificultades legales no previstas por los profesionales del derecho, el legislador o el juez, pero que el Derecho Informático permite o está llamado a solucionar, hecho que refuerza y sustenta la característica en mención.
- i) Es un derecho íntimamente influenciado por las tecnologías en general, debido a que éstas han permitido un desarrollo sostenido de la computadora y su entorno, por ejemplo, en la actualidad se tienen una serie de problemas jurídicos generados por el uso de Internet en las diversas actividades de las personas.
- j) Es un derecho que se encuentra ligado al proceso de globalización, por lo que el jurista se encuentra obligado a resolver el problema del juez competente, el mismo que debe conocer y dar solución a determinado caso concreto, debiendo, asimismo, analizar todo aquello que esté relacionado con la ley aplicable a cada situación en particular.

Es preciso hacer mención que el derecho informático cumple un rol importante en la prevención de situaciones no deseadas para los usuarios de las Nuevas Tecnologías de la Información y cuando se presentan determinadas circunstancias que los afecten, facilita la incorporación de nuevas instituciones jurídicas que permitan crear confianza a las personas e instituciones que realizan tales operaciones, permitiendo de esta forma la solución de aquellos problemas generados por el uso de los medios electrónicos en la sociedad.

2.4. Principios de los derechos informáticos

Actualmente, la sociedad se encuentra en una evolución constante y el derecho es la ciencia que se encarga de la regulación de las personas en la sociedad y el mismo tiene que investigar y desarrollar los principios y las instituciones para la adecuación de las acciones que se derivan de dicha evolución de los derechos, de las personas; creaciones y relaciones en el ciberespacio existente.

El derecho informático, como toda rama del derecho, tiene distintos principios rectores que sirven como pilar fundamental para su efectivo funcionamiento y permanencia ante la constante transformación digital:

- **Principio de tipicidad:** toda conducta delictiva debe estar previamente escrita en una normativa vigente, nadie puede ser juzgado por una acción u omisión que en el momento no constituyan delito;
- **Principio de legalidad:** todo ejercicio y acción de un organismo jurisdiccional debe ser basado en una ley vigente y jamás a voluntad de las partes;
- **Principio de equivalencia funcional:** un documento emitido, firmado y consensuado por las partes de forma escrita, tendrá el mismo efecto que su homólogo en soporte informático;

- **Principio de neutralidad tecnológica:** las leyes no deben favorecer a ninguna tecnología en particular si existiesen otras con las mismas funcionalidades y validadas legalmente para firmas y certificados electrónicos;
- **Principio de inalteración del derecho preexistente de obligaciones y contratos:** el título del principio habla por sí solo. Cuando el contrato se perfecciona por vía electrónica, de ninguna forma se deben modificar los elementos esenciales del negocio jurídico celebrado si este ha cumplido con todos los extremos legales;
- **Principio de buena fe:** ante una duda de desconocimiento y desconfianza, debe privar la buena fe de las partes;
- **Principio de libertad contractual:** se refiere a la voluntad de las partes de expresar su intención de aceptar o no celebrar contratos por medios electrónicos. Si se vulnera la voluntad expresa de alguna de las partes, entonces el negocio jurídico se considerará ilícito.

El derecho informático adquiere gran importancia y trascendencia por el desarrollo de un número cada vez mayor de elementos informáticos, electrónicos, ópticos y similares, que facilitan la vida del hombre, pero a su vez, le generan serias dificultades en su interacción con los demás seres humanos, surgiendo de esta manera una serie de circunstancias que permiten el desarrollo, fortalecimiento y perfeccionamiento del derecho informático y sus instituciones jurídicas.

2.5. Fuentes

En el derecho informático, por ser una rama del derecho reciente, y por sus constantes cambios y avances, genera un problema práctico en cuanto a la ubicación de la normativa aplicable, como consecuencia sus fuentes se encuentran dispersas y

contenidas en todas las fuentes del derecho.

A nivel interdisciplinario, se tiene aquellas fuentes provistas por el mismo derecho (fuentes interdisciplinarias), como se describe de la siguiente manera:

- a) Legislación informática:** Son un conjunto de disposiciones, de regulaciones de normas obligatorias emanadas por la potestad legislativa, que regulan la sociedad y las relaciones de la informática.
- b) Doctrina informática:** Es un conjunto de ideas, opiniones sobre el derecho, teorías que se elaboran sobre el tratamiento de la informática, que este conjunto de opiniones puede ser libros, artículos, estudios, etc. y de estos se obtienen leyes. Siendo un papel importante ya que, analiza al fenómeno informático, de manera enriquecedora, para una legislación acorde en esta materia.
- c) Jurisprudencia informática:** Son los fallos, sentencias, resoluciones que tienen contenidos informáticos, en síntesis, son fallos con relación a temas informáticos."

Por otra parte, tenemos las fuentes transdisciplinaria, que son aquellas provistas por ciencias y técnicas, entre las que podemos mencionar:

- a) Sociología:** Encargada de estudiar los fenómenos que se dan en la sociedad dando pautas o medidas de que dirección deben tomar. Nos ayuda a comprender la transformación social, estudiando los fenómenos sociales buscando las causas que explican el surgimiento y su desarrollo.
- b) Economía:** Estudia los fenómenos económicos y las relaciones de producción. Dado a los adelantos tecnológicos, nos ayuda a comprender el desarrollo de la economía moderna que apoya a mantener y acrecentar la actividad económica.

- c) Filosofía:** Nos indica como serán las relaciones con las normas jurídicas, nos da la señal de la ley perfecta, un prototipo de ley optimizadora para el razonamiento, la base de la informática es la lógica formal. Nos ayuda en la construcción de conceptos técnicos (porque la tecnología estudia técnicas) en el desarrollo de razonamientos.
- d) Estadística:** Maneja datos, información, la ordena, clasifica, sistematiza, procesa, analiza.
- e) Política Económica:** Cuando hablamos de economía política, hablamos de una estrategia, de una planificación para llegar a un objetivo.
- f) Informática jurídica:** La informática jurídica es una ciencia que forma parte de la informática, es la especie en el género, y se aplica sobre el derecho empleando los recursos informáticos (hardware y software); para que se dé el tratamiento lógico y automático de la información legal. Se debe aclarar que no es una rama del derecho, sino una herramienta; siendo su temática fundamentalmente tecnológica.

En general se ocupa de dar soporte a la administración y gestión de las entidades. Entre sus aplicaciones podemos encontrar: "programas para el seguimiento de casos y expedientes, control de archivos, control de clientes y facturación, avisos y notificaciones, agenda de tareas, cálculos de impuestos y honorarios, formularios electrónicos, y otros.

2.6. El bien jurídico tutelado

El bien que ha sido lesionado directa o indirectamente o puesto en peligro por la comisión de una conducta delictiva, antijurídica, típica y culpable, y que es constitutiva de sanción penal, es en esencia la información; y que, por ser sustraída sin el consentimiento y la acción ejecutada por medios tecnológicos como herramienta para la

comisión de hechos delictivos continuados, puede y debe ser tipificado, regulado y sancionado como delitos contra los derechos fundamentales del ciber ciudadano.

El bien jurídico protegido en general es la información; sin embargo, es considerada de diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico y finalmente por los sistemas que la procesan o automatizan.

Los mismos se equiparán a los bienes jurídicos protegidos tradicionales tales como:

- La información;
- Patrimonio;
- Reserva, intimidad y confidencialidad de los datos;
- Seguridad y fiabilidad del tráfico jurídico y probatorio; y
- Derecho de propiedad.

2.7. Contenido del derecho informático

El derecho informático es el conjunto de normas jurídicas, principios e instituciones que regulan los bienes jurídicos que la informática crea y las acciones y responsabilidades de las personas en el uso de la tecnología. Ahora bien, el contenido del derecho informático es amplio y de constante desarrollo, ya que contempla las múltiples interacciones entre el derecho y la informática, se va basando en las problemáticas, más sobresalientes, a continuación, se menciona el siguiente contenido del derecho informático:

- a) El valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de elementos de prueba derivados de estos soportes entre los órganos jurisdiccionales,
- b) La protección de datos personales, ante el manejo inapropiado de informaciones nominativas que atenta contra derechos fundamentales de las personas.
- c) Los delitos informáticos, es decir, la comisión de verdaderos actos ilícitos en los que " se tenga a los computadores como instrumentos o fines.
- d) El flujo de datos transfronterizos, con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.
- e) La protección de los programas computacionales, como respuesta a los problemas provocados por la piratería de software que atenta contra la propiedad intelectual.
- f) Los contratos informáticos, en función de esta categoría contractual sui generis con evidentes repercusiones fundamentalmente económicas.
- g) La regulación de los bienes informacionales, en función del innegable carácter económico de la información como producto informático.
- h) La ergonomía informática, como aquellos problemas laborales suscitados por la informatización de actividades.

Para una mejor sistematización del derecho informático, se manifiesta que el contenido se puede establecer de la siguiente manera:

- a) Protección Jurídica de los datos personales.
- b) Flujo de datos transfronterizos e Internet.
- c) Protección jurídica de los programas de computación
- d) Delitos informáticos.
- e) Contratos Informáticos y comercio electrónico.
- f) Valor probatorio de los documentos electrónicos.

El derecho informático es una rama autónoma del derecho que se tiene que cumplir con una serie de estudios estructurales y bien complejos, los cuales abarcan como requisitos los principios, la doctrina y la investigación. El derecho informático, consiste en el vínculo de dos caminos; el del derecho y el de la informática. En lo relacionado al derecho informático, no puede considerársele como una rama autónoma del derecho, debido a que los conceptos tratan acerca de su propia incorporación al campo como tales en cada una de las otras disciplinas jurídicas. Por ende, los llamados delitos informáticos no son materia del derecho informático sino del derecho penal. Los contratos informáticos forman parte del derecho civil o mercantil según el caso.

2.8. Diferencia entre derecho informático e informática jurídica

- **El derecho informático (esencial u objeto del derecho):** Es de relación esencial,

ya que se derivada de la informática y la utilización de la tecnología que se aplica directamente al derecho, es decir, la razón por la que se admite la necesidad de regular lo necesario respecto a los delitos informáticos para proteger derechos de privacidad inherentes a la condición humana del ciudadano, en virtud de la nueva aplicación de usos tecnológicos a la vida cotidiana, ya sea en lo relacionado al ámbito natural-individual o jurídico-colectivo. Es el conjunto de principios y normas que regulan los efectos jurídicos, especializados en el tema de la informática, sus usos, aplicaciones e implicaciones dispuestas en el mundo de lo jurídico. En general, lo que se refiere a la protección derivada de la norma.

- **En contraste, la informática jurídica (especial o instrumental):** Es de relación especial, porque surge de esa necesidad de protección a esos derechos inherentes del cual el Estado es garante. Como herramienta tecnológica de uso cotidiano, en la aplicación del ejercicio técnico de los juristas en el desarrollo de sus actividades profesionales, en especial, en la defensa procesal de los derechos vulnerados como representantes del Estado, a través de sus órganos jurisdiccionales.

Es el sector normativo de los sistemas dirigidos a la regulación de las nuevas tendencias tecnológicas de la información, y la comunicación; es decir, se refiere a las propuestas normativas, teorías, análisis, investigaciones, estudios específicos, razonamientos jurídicos. Trata de la norma en sí. En resumen, es todo lo que tiene por objeto el analizar, interpretar, exponer y sistematizar esas normas fuente o documentos que se relacionan directa o indirectamente con el derecho.

2.9. La informática

La informática es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital; la informática se ha desarrollado rápidamente a partir de la segunda mitad del siglo XX, con la aparición de tecnologías tales como el circuito integrado, internet y el teléfono móvil.

La escritura permitió la existencia de un desarrollo fundamental para el derecho, al permitir plasmar el conocimiento para posteriormente estudiarlo y mejorarlo, ya no se tenía que transmitir de forma verbal de generación a generación; con la posible mala interpretación del conocimiento de una determinada información.

La informática es la ciencia que se encarga del procesamiento automatizado y lógico de la información de forma veloz y eficaz. Para alcanzar su objetivo, utiliza como recurso fundamental a la computadora, lo cual es el instrumento de procesar la información, un aparato electrónico que fue inventado para facilitar la utilización del volumen de la información que el género humano ha creado con el tiempo.

La informática abarca aspectos tales como:

- a) Cibernética,
- b) Informática,
- c) Información,
- d) Tecnologías de información y comunicaciones.

Con el desarrollo y auge de la informática aparecen bienes jurídicos, los cuales no existían en la sociedad como los son los siguientes:

- a) Programas de ordenador.
- b) Bases de datos automatizadas.

El ciberespacio surge debido a la evolución de las tecnologías de la información y comunicaciones. Después, también aparecen nuevas corrientes o medios de llamar a la relación existente entre el derecho y los fenómenos que se producen debido a la informática, entre el derecho y la tecnología, entre el derecho y las tecnologías de información y comunicaciones y entre el derecho y la internet.

2.10. La informática jurídica

La informática jurídica, ha sido una rama de estudio que actualmente ha cobrado mucha relevancia, en consecuencia, de que modernamente gran parte de las actividades cotidianas se llevan a cabo a través de aspectos relativos a la internet, lo que ha hecho necesario se realicen estudios y análisis, para dotar a esta de seguridad jurídica.

La informática jurídica estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal; las fuentes de producción jurídica, a través de la elaboración informática tanto los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho. En cuanto a la clasificación de la informática jurídica la misma es la siguiente:

- a) Informática jurídica de gestión.
- b) Informática jurídica de gestión registral.
- c) Informática jurídica en gestión operacional.

Diversos son los órganos del Estado que emplean los sistemas informáticos en el control de sus procesos o expedientes de orden administrativo según el caso correspondiente. En la sociedad guatemalteca ocurre en el comienzo de los procesos

en el centro de gestión penal y en el centro de servicios auxiliares de administración de justicia, cuando se comenzó a llevar una fiscalización de un control electrónico relativo al trámite de los procesos. Actualmente, en el Ministerio Público se cuenta con el sistema informático del control de casos del Ministerio Público (SICOMP).

a) Informática jurídica documental.

b) Documentación doctrinal:

En la mayor parte de los sitios se puede tener acceso gratuito, pero en otros si existe la necesidad de tener que realizar algún pago, para que la información sea proporcionada o bien para suscribirse al servicio. En la actualidad, el único sitio que proporciona información de importancia en materia doctrinal guatemalteca y con temas relacionados con el derecho es derecho.gt derecho guatemalteco, y en el que los autores nacionales o extranjeros pueden hacer publicaciones de sus artículos, puntos de vista doctrinarios y análisis en relación con el resto de las ramas del conocimiento: también proporciona otra clase de servicios que se relacionan al estudio del derecho.

CAPÍTULO III

3. Delito informático

El auge de la informática en los últimos años, la necesidad de las comunicaciones de manera electrónica ha dado como resultado que se cometan actos ilícitos que es necesario regular para proteger a las personas. El aspecto más importante de la informática radica entonces en que la información ha pasado a convertirse en un valor económico de primera magnitud.

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se realizaban manualmente.

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, 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.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica delitos informáticos, los cuales podrían definirse como toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.

La dependencia de la sociedad a las nuevas tecnologías de la información y de las comunicaciones, hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida. De esta cuenta,

cobra importancia la seguridad con la que han de contar los equipos informáticos y las redes telemáticas, con el fin y objeto de poner obstáculos y luchar con dichas conductas delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que estas sean efectiva y positivamente perseguidas y castigadas en el ámbito penal.

En igual forma, deben de desarrollarse los procedimientos técnicos de la recolección de evidencia en este tipo de delitos, a efecto de garantizar la certeza de los medios de prueba aportados a los procesos penales que se instauren por estas infracciones.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado que hoy en día en Guatemala, se observa aumentado en alto porcentaje. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar ningún documento de rastro.

Si bien es cierto, la gama de delitos informáticos que existen es inmensa, regular de manera efectiva los que se producen en Guatemala, representaría un gran avance en la aplicación de los diferentes tipos penales; toda vez que actuarían como elementos disuasivos 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.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, a las peculiaridades del objeto de protección, sea imprescindible; si se tiene en cuenta que los sistemas informáticos pueden entregar datos e informaciones sobre miles de personas, naturales o jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, identificación de las personas.

A ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, de carácter personal o sobre materias de las más diversas disciplinas a un Estado, o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje. No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

3.1. Definición de los delitos informáticos

Define al delito informático “como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular; de un elemento informático, ya sea hardware o software.”¹²

Para cometer un delito informático deben reunirse ciertas características, las cuales no son imprescindibles en otra clase de delitos; el primero de ellos es utilizar un elemento informático, esto es lógico pues debe utilizarse algún ordenador para consumir el hecho delictivo, este es el elemento principal en esta clase de delitos, también se puede comprender aquellas conductas que recaen sobre herramientas Informáticas, programas, ordenadores, como aquellas que valiéndose de estos lesionan otros intereses jurídicamente tutelados como son la intimidad y el patrimonio.

Expone que el delito de informática “es cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción

¹² Huerta, Marcelo y Libano, Claudio. **Delitos informáticos**. Pág. 138.

criminógena, o como mero símbolo; por su parte Julio Téllez Valdés entiende los delitos informáticos desde dos puntos de vista: típico y atípico.”¹³

El delito informático es aquel que se da con la ayuda de la informática o de técnicas anexas, son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico), en otras palabras son las acciones prohibidas por la ley, que se comete en contra de uno o varios de los elementos que integran un sistema de información o los derechos que del mismo se deriven (protección de datos, intimidad o privacidad, derechos de autor).

Refiere que el delito informático “es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas, en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por la segunda actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.”¹⁴

El delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software, se le considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito, se dirige a las propias tecnologías de la computación y las comunicaciones o incluye la utilización incidental de computadoras en la comisión de otros delitos.

Establece que el delito informático “abarca un conjunto de conductas de distintas características, que afectan bienes jurídicos diversos y que sólo son agrupadas bajo este concepto por su relación con el ordenador, ya que es toda acción u omisión

¹³ Palazzi, Pablo Andrés. **Delitos informáticos**. Pág. 249.

¹⁴ Acuario Del Pino, Santiago. **Delitos informáticos**. Pág. 370.

culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y sancionado con una pena.”¹⁵

En tal sentido, analizando el ordenamiento jurídico guatemalteco vigente, referente a esta materia, se puede decir que el término de delito informático no constituye por sí mismo una categoría delictiva, sino que se trata de usos indebidos de cualquier medio informático. En general, para gran parte de la doctrina no existe un delito informático, sino una realidad criminal compleja, vinculada a las nuevas técnicas de información, imposible de ser incluidas en un único tipo legal.

Comenta que el delito informático “es el conjunto de comportamientos dignos de reproche penal, que tiene por instrumento o por objeto, a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de vahados bienes jurídicos, es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.”¹⁶

Los delitos que se regulan en el Código Penal respecto al uso del internet o medios informáticos, es importante describir algunas figuras delictivas que a juicio de quien escribe, se circunscriben no necesariamente a la figura típica tal como se regula, sino que éstas se pueden cometer a través del uso de las computadoras y por ende del internet, sin qué en el Código Penal se encuentren reguladas como tal, siendo que a la fecha, podría ser que los jueces, que son quienes juzgan y sancionan, se encuentren en dificultades principalmente porque son figuras delictivas atípicas.

Además, los medios de prueba también son sui géneris que no sólo se debe tener conocimiento de la ley sino de cómo funciona el internet, a lo cual, podría ser que no

¹⁵ Nava Garces, Alberto Enrique, **Análisis de delitos informáticos**. Pág. 110.

¹⁶ Camacho Lasa, Luis. **El delito informático**. Pág. 245.

todos los jueces se encuentren preparados para ello, tomando en cuenta que recientemente se encuentra funcionando estas formas o redes de comunicación.

Concluyendo que los delitos informáticos constituyen aquella conducta típica, antijurídica, culpable y punible que se lleva a cabo con la ayuda de un medio informático con el fin de perjudicar tanto a una persona individual como jurídica, y que, mediante su regulación legal, y con los avances tecnológicos se garantiza el derecho a la privacidad de la información de las personas individuales y/o jurídicas.

3.2. Naturaleza y objeto

El objeto se enmarca en las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física. Conductas dirigidas a causar daños en el hardware o en el software de un sistema. Programación de instrucciones que producen un bloqueo total al sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han evolucionado hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: las conductas dirigidas a causar destrozos físicos y los métodos dirigidos a causar daños lógicos.

Como fin las conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla. La clasificación de estos delitos es muy amplia, por una parte, son conductas criminales que se valen de las computadoras como método o medio, y por otro lado están las que van dirigidas a efectuar daños tanto externos como internos a las computadoras, por consiguiente, es de suma importancia prestarle la debida atención ya que de una u otra forma podemos ser víctimas de nuestra información o de nuestro propio equipo de cómputo.

La naturaleza de los delitos informáticos es eminentemente jurídico penal ya que dichas conductas están reguladas en las leyes en materia penal.

3.3. El bien jurídico tutelado en los delitos informáticos

En términos generales, el bien jurídico tutelado es el bien o valor lesionado o puesto en peligro por la conducta del sujeto activo, jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales.

El bien jurídico tutelado nace de una necesidad de protección y se toma penal sólo si reviste una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de participación de los individuos en la sociedad.

Se debe tomar en cuenta que para recabar en forma adecuada la evidencia que compruebe la comisión de los delitos informáticos, es necesario que se tenga bien claro cuál es el bien jurídico que se tutela en este tipo de delitos. Dentro de los delitos informáticos, se puede decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una reinterpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos reinterpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Actualmente se presume que la emergente sociedad de la información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible.

Esto por cuanto la información puede no ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que la información

y otros intangibles son objetos de propiedad, la cual de conformidad con la Constitución Política de la Republica de Guatemala, está protegida, y debe definirse como un bien vital, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado.

En tal sentido, la protección de la información como bien jurídico protegido, debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señalan que la penalización de conductas se desenvuelva en el marco del principio de lesividad. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

Los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir, que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo. En conclusión, no se afecta un solo bien jurídico, sino una diversidad de ellos, al tenor de este criterio se puede decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afecta a una diversidad de ellos que ponen en relieve intereses colectivos.

Por lo cual, se puede indicar que el bien jurídico protegido es la información, pero está debe ser considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente, por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como el patrimonio, la reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.

También la seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos, así como el

derecho de propiedad, en este caso sobre la información o sobre los elementos físicos materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático.

En tal sentido, el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere. Por tanto, el nacimiento de la tecnología informática está proporcionando nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio).

Sin embargo, han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtenga; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaigan sobre la información personal registrada o sobre la información nominativa. Por tal razón se puede considerar que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Un ejemplo que puede aclarar esta afirmación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad de este y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona, al ver que su información personal es vista por un tercero extraño, que sin autorización ha vulnerado el sistema informático donde dicha información está contenida.

Pero detrás de ese bien jurídico encontramos otro bien colectivo que conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

3.4. Sujetos del delito informático:

Los sujetos involucrados en la comisión de esta clase de delitos son:

a) Sujeto activo: Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que la diferencia entre sí es la naturaleza de los delitos cometidos. En forma más concreta en cuanto a la característica del sujeto activo del delito informático; las personas que cometen los delitos informáticos son aquéllas 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. De esta forma, la persona que ingresa en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes de delincuente informático es tema de controversia; ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática pero sí de una actividad punible; en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

b) Sujeto pasivo: Sujeto pasivo o víctima del delito informático, 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, gobiernos, que

usan sistemas automatizados de información generalmente conectados a otros.

La determinación del sujeto pasivo es importante, toda vez que a través de su identificación se pueden conocer los diferentes ilícitos que cometen los delincuentes informáticos; debido a que muchos de los delitos son descubiertos casualmente por el desconocimiento del modus operandi de los sujetos activos.

En Guatemala, el fenómeno de la criminalidad informática o de los llamados delitos informáticos no ha alcanzado todavía una importancia mayor; esto por cuanto no se conoce dentro del entorno legal mucho sobre esta clase de infracciones, a pesar del efecto que se está viviendo; y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual.

3.5. Características de los delitos informáticos

El delito informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Los delitos informáticos presentan las siguientes características principales:

- a) Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
- b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

- c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serías pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan.
- e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- g) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- h) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- i) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

El delito informático es aquel delito que abarca cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena o como mero símbolo.

3.6. Elementos esenciales del tipo en el delito informático

El elemento descriptivo es apreciado a través de la vista u otros sentidos, en esta clase de delitos lo es, la computadora, bases de datos o registros informáticos, los bienes

materiales e intelectuales afectados a través de un sistema informático u ordenador

Debe entenderse que dicho elemento se aprecia intelectualmente y en este caso particular, para cometer delitos informáticos es necesario auxiliarse de la informática u otra ciencia para comprenderlos, en ese sentido dentro de los elementos normativos de este tipo de ilícitos están, los daños producidos a los equipos, a los programas o bases de datos, la pérdida patrimonial, la indemnidad sexual.

3.7. Clasificación de los delitos informáticos

A continuación, se clasifican los delitos informáticos, siguientes:

- a) Falsificación de documentos vía computarizada (tarjeta de crédito, cheques).
- b) Variación de los activos y pasivos en la situación contable de las empresas.
- c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude).
- d) Lectura, sustracción o copiado de información confidencial.
- e) Modificación de datos tanto en la entrada como en la salida.
- f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

- h) Uso no autorizado de programas de cómputo.
- i) Introducción de Instrucciones que provocan interrupciones en la lógica interna de los programas.
- j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- l) Acceso a áreas informatizadas en forma no autorizada.
- m) Intervención en las líneas de comunicación de datos o teleproceso.
- n) Programación de instrucciones que producen un bloqueo total al sistema.
- o) Destrucción de programas por cualquier método.
- p) Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- q) Estafas Electrónicas: A través de compras realizadas haciendo uso de la Internet.
- r) Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

En este tipo de delitos, también se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se puede asegurar que



entre esta clasificación podemos ubicar el pinchado de redes informáticas; así también, la interceptación de e-mail, en este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.



CAPÍTULO IV

4. Implementación de una fiscalía especializada contra el cibercrimen en el Ministerio

Público en la República de Guatemala

La evolución tecnológica ha generado un importante número de conductas nocivas que, aprovechando el poder de la información, buscan lucros ilegítimos y causan daños; esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso, sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

En la actualidad la informática se ha implantado en casi todos los países, tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, sin embargo, junto a las incuestionables ventajas que presenta comienza a surgir algunas facetas negativas, como, por ejemplo, lo que se conoce como criminalidad informática.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos, La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas). La idoneidad proviene básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente factible manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo

ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, a las peculiaridades del objeto de protección, sea imprescindible; si se tiene en cuenta que los sistemas informáticos pueden entregar datos e informaciones sobre miles de personas, naturales o jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancadas, financieras, tributarias, identificación de las personas.

A ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, de carácter personal o sobre materias de las más diversas disciplinas a un Estado, o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje, no son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La fiscalía especializada contra el cibercrimen es un desafío interdisciplinario que requiere un estudio detallado de la tecnología, los procesos y los individuos que permitan la conformación de un cuerpo de conocimiento formal, científico y legal para el ejercicio de una disciplina que apoye directamente la administración de la justicia y el esclarecimiento de los hechos alrededor de los incidentes o fraudes presentados.

Implementada dicha fiscalía, se podrían iniciar actividades de detección, prevención y seguimiento a actos delictivos informáticos con bases fundamentales de criminalística para la preservación y evaluación de medios tecnológicos, con la finalidad de reconstruir una secuencia de eventos sobre delitos informáticos para el posible esclarecimiento de acontecimientos y generar informes de resultados que permitan contribuir con un proceso judicial. Incluso se pretende incentivar a las autoridades y lectores a la creación y aprobación de la legislación adecuada para poder llevar a cabo el esclarecimiento y el proceso.

4.1. Investigación del cibercrimen en Guatemala

Como toda investigación de un delito, el cibercrimen tiene formas y procedimientos para su adecuada investigación, generalmente la investigación suele iniciarse con una denuncia realizada por los particulares afectados o solicitud del juzgado competente.

El cibercrimen es una actividad delictiva que afecta o abusa de una computadora, una red informática o un dispositivo en red, la mayor parte del cibercrimen, pero no todo, lo perpetran cibercriminales o hackers que desean ganar dinero. El cibercrimen lo cometen personas u organizaciones, algunos cibercriminales están organizados en grupos, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas. Otros son hackers novatos. En raras ocasiones, el cibercrimen tiene como objetivo dañar las computadoras por motivos distintos a la obtención de dinero. Estos pueden ser políticos o personales.

Desde que existen los ordenadores, ha existido la ciber delincuencia, sin embargo, con millones de ataques informáticos y casi mil millones de víctimas de actividades de delincuencia cibernética cada año, el crimen cibernético nunca ha estado tan extendido como ahora. Cualquiera puede caer víctima del ciber crimen, y el hecho de que todos estemos conectados virtualmente nos pone a todos en un riesgo incluso más grande.

El cibercrimen es cualquier actividad criminal que implica un ordenador, ya sea el objetivo del delito o la herramienta, cada año, la economía mundial pierde miles de millones de dólares como resultado de la actividad cibercriminal. Siga leyendo para aprender más sobre las maneras más comunes de cometer delitos informáticos y descubrir cómo protegerse en internet. El cibercrimen es toda aquella actividad que transgrede, en la que una computadora (o dispositivo de red) es atacada y/o utilizada directa o indirectamente.

Guatemala es un país que ha evolucionado en la tecnología durante los últimos diez años, en el cual se ha visto que se han incrementado los delitos por medio del uso de ésta, ahora los delitos informáticos se encuentran de moda, solo basta ver los medios de comunicación quienes muestran la realidad de dichos delitos día a día, a cada hora una persona especialmente mujeres y niños son objeto de un ciberdelito, por ejemplo, acoso, secuestro, difamación, robo de información.

Guatemala tiene un alto consumo de tecnología por lo cual es más vulnerable al crimen organizado y de pandillas, ya que estos aprovechan los recursos tecnológicos afectando a usuarios, instituciones públicas y privadas, persecuciones, seguimientos, rastreos y procesos judiciales. Las garantías del proceso penal en Guatemala fueron diseñadas para regular investigaciones que se llevan a cabo en entornos físicos, sin embargo, en la actualidad un número cada vez mayor de casos son investigados y resueltos en base a la utilización de evidencia digital.

El inconveniente con los procesos penales en Guatemala es que no se cuenta con una

ley relacionada que regule este fenómeno, solo iniciativas que han sido guía para investigaciones que no se han aprobado y por lo tanto no tienen validez en un proceso penal.

Aunque no se cuenta con estrategia nacional de seguridad cibernética, existe una entidad de seguridad cibernética llamado Equipo de Respuesta a Incidentes de Seguridad Informática Nacional, el CSIRT-gt, grupo que opera bajo el Ministerio de Defensa, este ha recibido capacitaciones de la Organización de Estados Americanos, OEA, y otras instituciones internacionales y recientemente el Ministerio de Gobernación se une al interés en ir avanzando en los términos de seguridad cibernética en Guatemala.

4.2. La informática forense

Es una ciencia la cual tiene como objeto preservar, obtener y presentar datos o documentos que han sido procesados electrónicamente y guardados en soportes de almacenamientos informáticos, es una práctica que cada día es más utilizada debido a que en la actualidad todos usan las nuevas tecnologías y que es de ayuda para resolver casos judiciales.

Los entes de seguridad del Estado, como, policías y peritos informáticos forenses, utilizan herramientas y procesos específicos para la recolección de información en dispositivos electrónicos que van desde computadoras, teléfonos móviles hasta servidores de correos electrónicos. Un dispositivo electrónico siempre dejará una prueba o registro digital y aunque sea o no un delito informático podrá ser analizado para incorporar a un caso judicial.

En principio se puede definir a la informática forense como, una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos informáticos y donde se utiliza el análisis forense de las evidencias digitales, en

fin, toda información o datos que se guardan en una computadora o sistema informático.

Establece que la Informática forense “es la ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en un juzgado o tribunal competente.”¹⁷

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en soportes informáticos. Se trata de una práctica cada vez más habitual debido al uso que actualmente todos realizamos de las nuevas tecnologías, y que permite resolver casos policiales o judiciales.

A la informática forense se le ha dado diferentes denominaciones como, por ejemplo, computación forense, análisis forense digital o exanimación forense digital. La informática forense se caracteriza principalmente por la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de la identificación, recolección y análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y los elementos de convicción necesarios. La escena del crimen es el computador y la red a la cual éste está conectado.

La ciencia forense siempre ha basado su experiencia y su accionar en estándares de práctica y entrenamiento, a fin de que las personas que participan o trabajan en este campo científico tengan la suficiente probidad profesional y solvencia de conocimientos

¹⁷ Santodomingo Garachana, Adolfo. **Introducción a la informática**. Pág. 138.

para realizar un buen trabajo en su área de experiencia.

Esta situación debe ser igual en el campo de la informática forense, es por tanto necesario que las personas encargadas de este aspecto tengan parámetros básicos de actuación, no sólo en la identificación, incautación y recolección de evidencias digitales, sino también en su procesamiento, cumpliendo siempre con los principios del debido proceso.

El objetivo principal de la informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal. Es importante señalar que la informática forense necesita de una estandarización de procedimientos y de acciones a tomar, esto debido a las características específicas que las infracciones informáticas presentan.

Son entonces estas propiedades que contribuyen a la existencia de una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales, es uso tan intensivo que se hace de redes, software y dispositivos, expone a los usuarios y a las empresas a todo tipo de ataques, fraudes y robos. En el caso de las compañías, son especialmente susceptibles al espionaje industrial.

En conclusión, la informática forense por tanto será la ciencia forense formal que se encarga del estudio de los métodos y técnicas de identificar, extraer, analizar, preservar y presentar a través de técnicas y herramientas la información, que permitan al investigador forense digital poder entregar un informe en donde presente los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar, y a la actividad que realiza el investigador es la investigación forense o exanimación forense aplicando los métodos y técnicas desarrolladas por la informática forense

4.3. La evidencia informática

Cuando se comete un delito, tanto de orden común, en el que se vean involucrados medios informáticos, como delitos informáticos propiamente, muchas veces la información que directa o indirectamente se relaciona con el hecho delictivo queda almacenada en forma digital dentro de un sistema informático. Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierten en evidencia digital como prueba de la infracción cometida.

Para recabar dicha evidencia se hace necesario utilizar los procedimientos técnicos y legales y la rigurosidad científica que provee la informática forense, a fin de descubrir a los autores del delito cometido. La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material. De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el tribunal alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

Se puede indicar que la evidencia digital es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático; en este sentido, la evidencia digital, es un término utilizado de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal.

La informática trabaja en dos escenarios sobre los cuales realizará el perito sus respectivos análisis, uno de ellos es el hardware (evidencia material) que se refiere a los componentes físicos de un sistema informático como el monitor o pantalla, impresora, módem, router, entre otros, y el otro se refiere al componente lógico es decir, a los programas computacionales, esto es, un conjunto de instrucciones para ser usadas por el ordenador con el objeto de obtener un determinado proceso o resultado.

En cuanto a donde debe ser ubicada la evidencia en este tipo de delitos, se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en esta (evidencia digital). Esta distinción es de gran utilidad al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital.

En este contexto la evidencia electrónica o hardware se referirá a todos los componentes físicos de un sistema informático, mientras que la evidencia digital o información se referirá a todos los datos, mensajes de datos y programas almacenados y transmitidos usando el sistema informático.

Esa labor debe ser llevada a cabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta, en la medida posible, la información contenida en el disco de un sistema comprometido, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

La prueba pericial informática es el medio de prueba, de suma importancia para cualquier actuación judicial que precisen conocimientos científicos o técnicos especializados. Las evidencias electrónicas son rastros existentes en los equipos informáticos que, debidamente preservados, y puestos en relación con información existente en otros ordenadores o en el contexto de otras evidencias o de hechos probados permiten demostrar que se ha llevado a cabo una acción, por medios informáticos o no, e, incluso, quien o quienes la han llevado a cabo.

Hay que recordar que la evidencia en el derecho procesal penal es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella, y en este tema en particular, la evidencia digital es cualquier mensaje de datos almacenado y transmitidos por medio de un sistema de información que tenga relación con la comisión de un acto que

comprometa gravemente dicho sistema y que posteriormente guía a los investigadores al descubrimiento de los posibles infractores.

Es importante también establecer claramente cuál es el papel que juega la informática forense en relación con la persecución penal de investigación de delitos informáticos. Para lograr establecer dicho rol, se debe examinar la actuación del perito frente a la ocurrencia de delitos, estrategias para evitarlos, recomendaciones adecuadas, conocimientos requeridos, en fin, una serie de elementos que definen de manera inequívoca el aporte que éste brinda en el manejo de los casos de delitos informáticos.

4.4. El Ministerio Público y su función ante los delitos informáticos

El Ministerio Público fue creado con base en el Artículo 251 de la Constitución Política de la República de Guatemala. Este Artículo, establece que el Ministerio Público es una institución auxiliar de la administración pública y de los tribunales, con funciones autónomas siendo eficiente, eficaz y transparente, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país, perseguir la realización de la justicia, y actuar con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece.

Como institución el Ministerio Público debe de desarrollar los principios contenidos en la Constitución Política de la República, al señalar que esta institución es auxiliar de la administración pública, con el objeto de garantizar dentro del marco legal todos aquellos actos desarrollados por las diversas instituciones que integran la estructura orgánica del Estado; en ese sentido también se establece que la institución del Ministerio Público es auxiliar de los tribunales con funciones autónomas, le corresponde la acción pública con el objeto de la averiguación de un hecho señalado como delito y de las circunstancias en que pudo ser cometido, al establecimiento de la posible participación del sindicado; el pronunciamiento de la sentencia respectiva y la ejecución de la misma.

Por lo anterior, se estima que la naturaleza jurídica del Ministerio Público lleva implícitas dos funciones una dentro del ámbito del derecho administrativo, al regular las actuaciones de los particulares dentro de la administración pública y la otra para establecer la participación culpable o inculpable del sindicado. Ambas acciones persiguen un solo fin como lo es la observancia del estricto cumplimiento de las leyes en el país, lo cual viene a fortalecer los principios democráticos de armonía y concordia dentro de la sociedad y fundamentalmente el fortalecimiento del régimen de legalidad.

La Ley Orgánica del Ministerio Público, establece la siguiente definición en Artículo 1 sobre dicha institución, la cual dice: El Ministerio Público es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por el estricto cumplimiento de las leyes del país. En el ejercicio de esa función, el Ministerio Público perseguirá la realización de la justicia, y actuará con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece.

4.5. La importancia de la aplicación de la informática dentro del derecho penal guatemalteco

La progresión que ha generado la tecnología va de la mano con la información y comunicación debido a la globalización que tiene y para ello los juristas han tenido la necesidad de enfrentar profundamente el impacto y las consecuencias que las mismas han generado dentro de las estructuras del derecho guatemalteco. El desarrollo de la masticación de las grandes tecnologías de información se debe realizar con un verdadero análisis de la suficiencia del ordenamiento jurídico guatemalteco actual para regular las nuevas posiciones, los nuevos escenarios, en donde se observan los problemas del uso y abuso de la actividad informática y su repercusión en el territorio guatemalteco.

El ser humano es eminentemente social, no puede vivir ni limitarse a su individualidad.

Tan antiguo como las necesidades más fundamentales de los mismos es el de prestarse colaboración, para vencer los obstáculos que en la vida y su historia ha aparecido como uno de los resultados de esa convivencia social. En la actualidad la informática tiene un crecimiento inmenso a nivel mundial, abarcando todos los ámbitos de las relaciones sociales, por lo que se debe de enfrentar a grandes cambios en los aspectos comerciales, civiles, administrativos y jurídicos.

En el Decreto Número 33-96 del Congreso de la República de Guatemala, se implementaron delitos informáticos dentro de la legislación guatemalteca, siendo un verdadero avance en materia penal e informática, pero existe deficiencia en el sistema de justicia para la aplicación de dichas normas, ya que resulta plenamente ser un derecho vigente pero no positivo, lo cual violenta y genera una serie de problemas ante el resguardo de los derechos humanos de datos personales de la población.

Actualmente, existe mucha responsabilidad del Estado de Guatemala ante la protección de datos personales y el incremento de delitos informáticos, y como estos han afectado y siguen siendo violentados de diferentes formas y con resultados que, afectado plenamente los derechos de los afectados, dando a conocer que el mismo Estado es incapaz por medio del Ministerio Público para enfrentar este tipo de flagelos y en la cual como se indica es un derecho vigente pero no positivo.

La importancia de los procesos penales respecto a la protección de datos personales y el seguimiento a los delitos informáticos en Guatemala, y sobre todo la necesidad de reformar las normas para que estas sean plenamente vigentes y positivas, acoplándolas más a la realidad de vulnerabilidad y a la falta de capacidad del Ministerio Público para enfrentar este problema. Así también, deben de darse los avances necesarios y aplicar los avances de la tecnología para que la informática sea parte del derecho como una herramienta real.

4.6. La tecnología de información y comunicaciones respecto de la garantía de las personas en la persecución de delitos informáticos

En la actualidad la informática se incorpora a las ciencias del conocimiento humano, siendo la computadora la herramienta de mayor evidencia de la informática; ocupando un lugar bien importante dentro de los procesos de automatización de la información. La informática en combinación con el desarrollo de las telecomunicaciones y su fácil acceso han permitido a la ciudadanía guatemalteca la libre comunicación para que la misma no se encuentre limitada por factores como el tiempo, distancia y costos.

La combinación de redes, computadoras y de telecomunicaciones accesibles y la necesidad de compartir información originó el internet, si, dicha red mundial de computadores permite a las personas interrelacionarse mediante otro medio corporal distinto al de la presencia física como tal. Pero, de igual forma en el llamado mundo físico, se pueden adquirir derechos y a la vez contraer obligaciones mediante los negocios de carácter electrónico.

La informática como la internet, ciencia, técnica o procedimiento ha contado con una incorporación bastante lenta e inclusive limitada en el derecho, lo cual surge derivado a distintas razones; que van desde la falta de conocimientos de sus aplicaciones hasta apatía y desinterés. Dentro de la formación profesional del derecho se le prepara en conceptos, principios y conocimientos relativos a las ciencias sociales y jurídicas. Pero, existe un diverso conocimiento en ciencias exactas o técnicas que se relacionan de manera estrecha con el derecho vigente en Guatemala, entre ellas la informática.

4.7. Los principios del derecho respecto de la garantía de los derechos de las partes en la informática

En los últimos años, especialmente alentados por el adelanto de la tecnología en las comunicaciones, se ha tomado tan notable impulso al tema de los derechos humanos

que, incluso, el desarrollo de una sociedad no sólo se verifica en función de avances económicos, financieros o científicos sino, además, en función del valor de observancia que los ciudadanos y los gobernantes tienen respecto de los derechos fundamentales.

Pero para que los individuos ejerzan sus derechos humanos, no se requiere que estén consagrados en una Constitución o en una ley, ni dependen de una normatividad preestablecida pues son anteriores a la comunidad política e independientes a sus reconocimientos jurídicos y al Estado mismo. Es decir, el derecho humano prevalece se dé o no reconocimiento por un cuerpo legislativo o por el Estado.

La integridad y privacidad del ser humano reside, entonces, en su capacidad de poseer, ejercer y exigir sus derechos para su conocimiento y pleno desarrollo, sin licencia o previa autorización del Estado; incumbiéndole a éste sólo garantizar que estos derechos básicos se ejerzan plenamente y arreglados al bien común.

Este arreglo al bien común conlleva a que algunos derechos, aun fundamentales, pueden ser limitados en aras de mantener un cierto orden en la comunidad política; pero una limitación que no implique la apropiación de derechos o el despojo de libertades que sería invertir el orden de valores al ubicar a la persona humana al servicio del Estado, cuando la realización del hombre es su propia existencia y es su capacidad para obrar en valores.

Ahora bien, justamente la esencia de la concepción humanista radica en ello: que los valores supremos se realizan en el hombre y para el hombre, en libertad y en equilibrio e igualdad de oportunidades para todos; entendiéndose con esto que la realización del hombre no concluye por ejercer sólo sus libertades sino, además, en armonía con las libertades de los demás. En esa línea de ideas, los principios del derecho entonces deben de generarse en cuanto al deberes, dando con ello la garantía de necesidad para las partes en la informática.

4.8. Impacto de los delitos informáticos

A medida que se va ampliando la internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o piratería informática, el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en paraísos informáticos; o sea, en países que carecen de leyes o experiencia para seguirles la pista.

En Estados Unidos de América se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancadas y de crédito.

Otros delincuentes de la informática pueden sabotear las computadoras para ganar ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados gusanos o virus, que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

Algunos virus dirigidos contra computadoras elegidas al azar, que originalmente pasaron de una computadora a otra por medio de disquetes infectados; también se

están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas descargados de la red.

Además de las incursiones por las páginas particulares de la red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía.

La proliferación de los delitos informáticos ha hecho que las personas sean cada vez más escépticas a la utilización de tecnologías de la información; las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios; por ejemplo, el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer este tipo de delitos; por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global. Asimismo, se advierte que las empresas que poseen activos informáticos importantes son cada vez más celosas y exigentes en la contratación de personal para trabajar en estas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral.

La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos; por lo que el componente educacional es un factor clave en la minimización de esta problemática.

4.9. La seguridad informática

Se define como el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya

sean estos individuales o conectados a una red frente a posibles ataques premeditados y sucesos accidentales.

En la prevención de la delincuencia informática los ataques a la información dirigidas a la revelación no autorizada de la misma, de la modificación o destrucción accidental o intencional o la incapacidad para procesar esa información son algunos de los aspectos más importantes que se deben de proteger.

La seguridad informática a su vez está dividida en cinco componentes a saber:

- Seguridad física
- Seguridad de datos
- Back up y recuperación de datos
- Disponibilidad de los recursos
- Análisis forense

4.10. El delito informático y su realidad procesal en Guatemala

El Código Penal, como se desarrolló en el capítulo II del presente trabajo, contiene dentro de su capítulo VII, los Artículos 274 “A” al 274 “G” que regula los siguientes delitos informáticos:

- Alteración de programas.

- Reproducción de instrucciones o programas de computación.
- Destrucción de registros informáticos.
- Manipulación de información.
- Uso de Información.
- Programas destructivos.
- Registros prohibidos.

El problema en la persecución penal de los delitos informáticos radica en que este tipo de infracciones son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión en la consumación del delito, y esto sumado a no contar en con una policía capacitada para investigar dichos hechos, el personal del Ministerio Público no tiene la capacitación necesaria que pueda dar las directrices para la correcta investigación y recolección de evidencia de dichos actos delictivos.

Por otro lado no se cuenta con una legislación especial que regule estas conductas de forma actualizada, la necesidad de las herramientas tecnológicas científicas que ayuden al examen de la evidencia digital y su posterior presentación como medio de prueba ante los tribunales de justicia manteniendo de siempre la cadena de custodia y la identidad de la evidencia, la necesidad de que los juzgadores conozcan sobre la materia para poder interpretar la evidencia digital, para resolver de la manera más justa y objetiva los procesos en los delitos informáticos.

Tomando en cuenta que este tipo de delitos evolucionan a gran velocidad y son

producto de la evolución de la delincuencia con el apareamiento de las nuevas tecnologías de la información, se debe de contar con una unidad especial para la investigación y persecución de estas infracciones informáticas, pero además existen varios problemas que en la realidad procesal es importante desarrollar.

4.11. Seguridad contra los delitos informáticos

Aunque los consumidores tienden a agrupar sus intereses juntos por debajo del término de la seguridad general; hay realmente varias partes de la seguridad que confunden. La seguridad significa guardar algo seguro: "Para guardar objetos seguros, es necesaria la autenticación, es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.

La autorización es decir el permiso a una persona o grupo de personas de poder realizar ciertas funciones. La privacidad o confidencialidad, es el más obvio de los aspectos y se refiere a que la información sólo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La integridad de datos, la integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada o copiada, bien durante el proceso de transmisión o en su propio equipo de origen.

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor. Controles de acceso, esto es quien tiene autorización y quien no para acceder a una pieza de información determinada.

La importancia de lo que se está asegurando y el riesgo potencial, involucra dejar uno de estos requerimientos o tener que forzar niveles más altos de seguridad; por lo que la comprensión de los elementos de seguridad y cómo ellos trabajan en el mundo físico,

puede ayudar para explicar cómo estos requerimientos se encuentran en el mundo de la red y dónde se sitúan las dificultades. Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad.

En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas y preocuparse de hacerlas cambiar periódicamente. Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas; siendo los mecanismos más usados para la protección de la red interna de otras externas los filtros o cortafuegos.

La lista de filtros se aplica secuencialmente, de forma que la primera regla que el paquete cumpla será marcar la acción a realizar para descartarla o dejarla pasar; debido a que la aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos. De igual manera, el cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje; en otras palabras, asegurar que proviene de quien dice, de esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma.

La firma digital garantiza la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión, se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje; las firmas son especialmente útiles cuando la información debe atravesar redes sobre las que no se tiene control directo y, en consecuencia, no existe posibilidad de verificar de otra forma la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede hacerse con la clave pública correspondiente a dicha persona o institución, si

efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo.

4.12. La metodología de la investigación del Ministerio Público en los delitos informáticos

La investigación de los delitos informáticos corresponde al Ministerio Público, esta institución, con el objeto de realizar los fines del proceso en cuanto a la averiguación del delito, las circunstancias en que pudo haberse cometido, la determinación de la posible participación del sindicado y su condena debe plantearse una metodología de su trabajo de investigación.

Para tal efecto, con fecha 1 de febrero del año 2006, el fiscal general, formula la Instrucción Número 001-2006, Instrucción General para la Aplicación de la metodología de la Investigación Criminal, dicha instrucción tiene por objeto mejorar la planificación, ordenamiento, control y seguimiento de las investigaciones criminales realizadas por los funcionarios del Ministerio Público, a efecto de que se realiza una construcción efectiva y lógica de la acusación.

Dicha instrucción señala que en la investigación debe aplicarse un método que permita construir progresivamente una teoría para cada caso, debiendo elaborarse una hipótesis criminal preliminar hasta culminar con la conclusión que permitirá ejercer con éxito la acción penal ante los órganos jurisdiccionales.

En dicho método debe incluirse un plan de investigación, el cual entre sus componentes debe incluir el componente probatorio, en el cual se determinarán los medios que se utilizarán para probar los elementos facticos. En el caso particular de los delitos informáticos, y ante la necesidad de apoyo de un investigador criminal especializado, en el plan de investigación se deberá establecer la necesidad del peritaje informático o digital para la comprobación de este tipo de delitos.

De conformidad con dicha instrucción, para realizar una investigación adecuada se deberá tomar en cuenta la guía básica para la solicitud de análisis sobre indicios levantados en la escena del crimen, allanamientos, inspecciones o registros, la cual constituye un instrumento orientador para el requerimiento de análisis técnicos o científicos a realizarse sobre los indicios encontrados.

Al realizarse un análisis sobre la Guía básica para la solicitud de análisis, se logra determinar que la misma no incluye análisis sobre evidencia informática o digital; razón por la cual se puede considerar que esta instrucción al no abarcar la evidencia informática, no orienta a los Fiscales sobre qué debe de solicitarse a los técnicos o peritos, en el caso del peritaje de la evidencia digital o informática.

4.13. El procesamiento de la escena del crimen en los delitos informáticos

Dentro del trabajo de investigación, el Ministerio Público, considera que la escena del crimen constituye el primer escenario de investigación de los delitos flagrantes, por lo que su adecuado procesamiento permitirá dotar a los fiscales, de indicios que le posibiliten construir y posteriormente reafirmar, desestimar o modificar la hipótesis del caso investigado, con lo cual podrá tomar una serie de decisiones en tomo a sus actividades de investigación.

Ante dicha situación, el fiscal general, con fecha 30 de octubre del año 2006, formula la Instrucción General No. 7-2006, denominada Instrucción General para la Aplicación del Manual de procedimientos para el procesamiento de escenas del crimen. En dicha Instrucción se establece que el procesamiento de la escena del crimen tiene por objeto inspeccionar el área, fijar la escena, recolectar y resguardar todo objeto material, sin importar el tamaño, que esté relacionado con un presunto hecho delictivo y que permita establecer la existencia del hecho y las circunstancias en que pudo ser cometido.

En el caso particular de los delitos informáticos, es de tomar en cuenta la particularidad

de este tipo de delitos y la forma en que puede presentarse la escena de este tipo particular de delitos.

El Manual que habilita dicha instrucción, establece que debe elaborarse un plan de procesamientos por parte del fiscal, en el caso de los delitos informáticos, debe tomarse en cuenta lo particular de este tipo de delitos, las posibles escenas del crimen que pueden presentarse y lo especial de la evidencia informática. En tal sentido, en la elaboración del plan de procesamiento de la escena en un delito informático o digital, el fiscal deberá evaluar si el técnico especialista del Departamento de recolección de evidencias del Ministerio Público, posee la capacidad y técnica necesaria para realizar la recolección de las evidencia digitales, en virtud de que para la recolección de las mismas, como quedo establecido anteriormente, se deben utilizar procedimientos específicos para evitar la contaminación de la evidencia o pérdida de información.

Si se considerará que dichos técnicos no tienen la capacidad necesaria, deberá acompañarse o solicitar el auxilio de un Perito en Informática Forense, para que este proceda a la recolección de la evidencia digital, pudiendo el técnico levantar o recopilar toda aquella evidencia que no sea digital.

Será responsabilidad del Perito en Informática Forense, la recolección de la evidencia, el mareaje y embalaje de esta, lo cual lo realizará de conformidad con las técnicas especiales correspondientes, a efecto de garantizar su pureza y conservación y que más adelante no se promuevan objeciones en cuanto a la evidencia recabada y se garantice su admisibilidad como medio probatorio en la etapa del juicio penal.

En tal sentido, se debe entender que la Instrucción y Manual a los que se hace referencia, es una guía general para el procesamiento de escenas de crimen, y no puede contener o referirse a cada caso en particular, razón por la cual consideramos que, por lo particular de la materia en los delitos informáticos, debiera de existir una instrucción especial en cuanto al manejo de escena del crimen en este tipo de delitos.

Cabe hacer mención que en algunos casos se puede presentar la situación de la incautación y el bloqueo de sistemas informáticos completos, al igual que en el caso de cualquier otra prueba. La incautación de todo un sistema informático puede resultar técnicamente inviable, o bien ser desproporcionada por tratarse de un entorno con muchos usuarios a los que interesa el contenido de los datos.

Cuando se pretende obtener datos para determinadas investigaciones, las facultades legales tradicionales pueden resultar insuficientes a causa de: a) problemas relacionados con la obtención de acceso al sistema informático; b) la naturaleza intangible de los datos; y c) el hecho de que los datos puedan estar almacenados en un sistema conectado, situado fuera del local registrado.

Queda establecido que el problema que se presenta por parte de las instituciones llamadas a realizar la persecución penal de los delitos informáticos, es la falta de preparación, tanto del Ministerio Público, como de la Policía Nacional Civil, esto por un lado por la falta de infraestructura necesaria, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de este tipo de delitos, así como la falta de información por parte de los Fiscales y agentes de investigación de la Policía Nacional, en virtud de no existir una Unidad Especializada para la investigación de este tipo de delitos.

Por otro lado también, la falta de preparación de jueces y magistrados, quienes se ven confundidos por la particular especialidad del tema y su común confusión con los delitos de orden común.

4.14. Inconvenientes en la investigación y el proceso pericial ante los delitos informáticos

Como se ha determinado hasta aquí, la investigación de la delincuencia informática no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los peritos informáticos buscan vestigios digitales que de acuerdo con sus características suelen ser volátiles y de vida corta.

Es preciso considerar que la internet brinda grandes beneficios a los usuarios, pero su fácil acceso también podría perjudicarlos. Los usuarios de internet corren un alto riesgo de ser perjudicados mediante actos delictivos como la estafa, o cualquier otro ataque, relacionados con las tecnologías. Las cifras sobre los delitos informáticos son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos.

Es importante considerar los retos particulares que están latentes a todo nivel e incluso para los actores involucrados, en el manejo de los Delitos Informáticos, sean estos el Ministerio Público, la Policía Nacional Civil, la Corte Suprema de Justicia, investigadores, y hasta la misma sociedad. Se puede mencionar como retos que se deben superar con relación al delito informático, los siguientes:

- 1) Marco legal inadecuado.
- 2) Formación profesional de los peritos e investigadores.
- 3) Limitaciones tecnológicas.
- 4) Creación de un protocolo para la ejecución del peritaje informático.

4.15. Legislación nacional relativa al cibercrimen

Se considera la acción como la potestad de la persona para provocar la actividad del órgano jurisdiccional a efecto de que se satisfaga la pretensión expuesta; en el ámbito penal la acción penal recae en el ente encargado de la persecución penal y/o el agraviado, quienes pueden acudir a los juzgados y/o tribunales competentes para ejercer sus correspondientes pretensiones en contra del sindicado o sindicados de la comisión de un delito o falta.

En los casos de los delitos informáticos, la acción penal es del tipo denominado acción pública de oficio, es decir, competencia del Ministerio Público y del querellante adhesivo; esta tesis se sustenta sobre la siguiente base: los delitos informáticos no están expresamente establecidos dentro de los delitos de acción pública dependiente de instancia particular contemplados por el Artículo 24 ter del cuerpo legal anteriormente citado. Tampoco lo están en los delitos de acción privada estatuidos por el Artículo 24 Quáter.

Es preciso hacer hincapié que los delitos enunciado por el Artículo citado la Ley de Derecho de Autor y Derechos Conexos por el Artículo 138 se derogó las literales a, d, e, f del Artículo 24 Quáter del Código Procesal Penal; y la Ley de Propiedad Industrial por el Artículo 220 se derogó las literales b y c; Barrios Osorio sustenta la tesis de que ante estas derogatorias se abre la puerta a la persecución mediante la acción penal pública, criterio que fundamenta en la clasificación penal por sus formas de ejercicio y en la ley especial de la materia, Ley de Derecho de Autor y Derechos Conexos y Ley del Organismo Judicial.

La legislación guatemalteca se basa en el Código Penal el cual menciona en el Artículo 274 de los incisos "A" al "F" los siguientes delitos informáticos

- **Destrucción de registros informáticos**

Será quien destruyere, borrar o de cualquier modo inutilizare registros informáticos.

- **Alteración de programas**

Será quien destruyere, borrar o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras o sistemas inteligentes.

- **Reproducción de instrucciones o programas de computación**

Quien sin autorización del autor copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

- **Registros prohibidos**

Al que creare un banco de datos o registro informático de datos que puedan afectar la intimidad de las personas.

- **Manipulación de información**

El 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 facilitar o alterar los estados contables con la situación patrimonial de una persona física o jurídica.

- **Uso de información**

A quien sin autorización utilice los registros informáticos de otros o ingresare por

cualquier medio a su banco de datos o archivos electrónicos. Según la unidad de delitos informáticos de la Policía Nacional Civil los delitos más frecuentes son los siguientes:

- Registros prohibidos.
- Robo de información
- Pornografía infantil
- Secuestro vías redes sociales
- Estafas

Es necesario esclarecer el marco normativo, aunque el Código Penal describe tipos perfectamente adaptables a los delitos informáticos, y pese a la creación de nuevas figuras para este medio, existen lagunas que dificultan la aplicación de los mismos: los actos cometidos a distancia, por ejemplo, la introducción de pornografía infantil o los daños producidos a una página web, en el que no existe regulación sobre el tema son ejemplos de acciones que dificultan la determinación de la jurisdicción competente.

4.16. Aporte al presente trabajo

La solución en la práctica en todo nivel siempre es la creación o ampliación del sistema de justicia como parte importante y primer paso para mejorar las condiciones para aplicar las leyes; la creación de la Fiscalía de Delitos Informáticos dentro de la estructura del Ministerio Público es de suma importancia como primer paso trascendental, pero deben de tomarse en cuenta una serie de elementos más que permitan que las leyes en dicha materia se apliquen de forma pronta y efectiva, y esto debe de ser el recurso humano y financiero, así como la ampliación a los lugares más

lejanos del país, tomando en consideración que muchos de los delitos se dan en lugares lejanos de las cabeceras departamentales o municipales.

La necesidad de promulgar un proyecto de ley que establezca una jurisdicción especial respecto al tema de delitos informáticos, como único medio viable en la actualidad no es suficiente, para lograr brindar una protección real a las personas en este ámbito, pero si debe de ser parte de las nuevas políticas que se deben de tomar en cuenta y en consideración para mejorar las condiciones para aplicar la norma penal.

Como consecuencia de todo lo referido, se han implementado, en la mayoría de los países, instrumentos jurídicos con el objetivo de tutelar y sancionar aquellos que, sin reparo alguno, lesionen un derecho de la persona por medio de las redes. Guatemala no debe de ser la excepción, y, de hecho, se ha caracterizado por tener un desarrollo amplio en esta materia particular de la ciencia jurídica, denominada delitos informáticos, por lo tanto, se debe de plantear un análisis particular de los mecanismos procesales existentes para tutelar, regular y sancionar las ofensas en este tipo de sistemas y sobre todo de profesionalizar de mejor manera a la institución encargada de la persecución penal.

Lo anterior, partiendo de una premisa: los mecanismos existentes, no permiten dar una adecuada protección del bien jurídico ambiente, y todos los elementos que en él se encierran, por lo cual debe de existir una fortaleza de las instituciones, siendo en el presente caso el Ministerio Público creando la Fiscalía específica de delitos informáticos.

Se debe reformar del Artículo 30 de la Ley Orgánica del Ministerio Público, Decreto Número 40-94 del Congreso de la República de Guatemala, incorporando la Fiscalía de Delitos Informáticos; esta ley establece lo referente a la organización de dicha institución, indicando que de las veintidos fiscalías existentes las mismas deben de ser competentes para atender todo el territorio nacional y que es el Fiscal General previo acuerdo del Consejo del Ministerio Público, el que podrá crear las secciones que consideren necesarias para el buen funcionamiento del Ministerio Público.

Por lo anterior y lo establecido en el punto preliminar de la presente investigación para que exista y se de vida a la Fiscalía de delitos informáticos debe de existir una reforma al Artículo 30 incorporando con ello a la fiscalía en el numeral 9. Dicha Fiscalía, debe de contener dentro de sus funciones específicas como lo establece el mismo Artículo 30, las que faciliten y permitan que el Ministerio Público pueda cumplir en forma cómoda y plena de las obligaciones que como ente de persecución penal debe de tener, tomando en consideración que dentro de la misma creación de la Fiscalía.

Asimismo, debe de considerarse dentro de las funciones de persecución que se deberán por parte del Ministerio Público realizar algunas pesquisas como parte del proceso de identificación, siendo la primera parte de las funciones determinar en número de dirección del atacante para ello hay que revisar con detenimiento los registros de conexiones de red como también los procesos y servicios, ya que muchas veces tienen alevosía y ventaja personas que saben y pueden manipular programas.

Así mismo debe de tomar en cuenta la información en fragmentos de las evidencias como lo es la disponibilidad de información para que pueda ser recuperada en el momento que se necesite, la memoria virtual o archivos temporales, así como los borrados, también restos de e-mail, con el objeto de dar solución a dicha investigación, así entonces al modificar el Artículo 30 de la Ley Orgánica del Ministerio Público se pueden obtener varios beneficios entre los que también deben de considerarse que dentro del proceso de análisis e investigación de las evidencias digitales. Es necesario valorar las mismas de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se puedan aportar en un proceso.

En Guatemala no existe una fiscalía especial contra el cibercrimen dentro del Ministerio Público, pero la realidad del país requiere la necesidad de creación y acción de esta; la nueva fiscalía especializada en Guatemala podría intervenir en casos donde se debe localizar a imputados por medio de Internet, la gravedad y complejidad del fenómeno, su relevancia nacional e internacional y su constante crecimiento tornan necesario

potenciar la actuación del Ministerio Público en la materia, ampliando su capacidad de intervención y profundizando todos los ejes de trabajo que se vienen desarrollando.

Los objetivos del área informática para la Fiscalía contra el cibercrimen deben ser enfocados en función de satisfacer el incremento de los problemas actuales relacionados con los ataques informáticos promoviendo en las víctimas el deseo de denunciar dichos actos ilícitos buscando crear en su comunidad la confianza en base a juicios justos, hallando a los culpables, teniendo indicios sustentables e irrefutables que no puedan ser cuestionados o invalidados para ser presentadas frente a un juez con el fin de que el criminal sea procesado y enjuiciado, empleando una correcta cadena de custodia y modelos para el análisis de las evidencias recopiladas.

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato, en tal sentido siendo el Ministerio Público encargado de la persecución penal debe de contar con el personal, medios o unidades necesarias para el esclarecimiento de la verdad.

La fiscalía especializada contra el cibercrimen debe ser creada con el fin de combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieren un tratamiento especializado desde la investigación, la recolección y el manejo de evidencias y prueba digital. En consecuencia, su finalidad es brindar el apoyo científico a través de dicha unidad para el esclarecimiento de la verdad histórica.

La fiscaliza especializada contra el cibercrimen, deberá ser creada para combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital, y porque no decirlo del personal capacitado para su manejo; los tipos

penales de competencia exclusiva de esta fiscalía deberían de ser acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes.

La fiscaliza especializada contra el cibercrimen contaría con una unidad para brindar apoyo técnico-jurídico a los agentes fiscales en la realización de diligencia, reciben asesoramiento en cuanto a la realización de diligencias de investigación vinculadas al uso de sistemas informáticos. Como se ha evidenciado las unidades especializadas del Ministerio Público son de vital importancia para la investigación, por lo cual se hace necesario su existencia, debido a que aún no existe esta fiscalía y considerando la evolución que en los últimos años ha tenido la delincuencia común y organizada, al extremo que ya utilizan equipo tecnológico para el robo de información confidencial y luego cometer hechos delictivos de tipo informáticos.

Por ejemplo: el robo de identidad, el robo de información por parte de trabajadores que laboran en el sistema bancario, quienes valiéndose de su condición de trabajadores de confianza y teniendo acceso a información netamente confidencial, realizan débitos de las cuentas monetarias o de ahorro, de los cuentahabientes con fines lucrativos, de los cuales ya existen casos que, de hecho, se encuentra en Proceso Penal.

Con la creación de la fiscaliza especializada contra el cibercrimen en el Ministerio Público ayudará a recuperar la credibilidad en el sistema de justicia y además contribuirá a la mayor certeza jurídica del órgano contralor de la investigación en cuanto a la aplicación de la ley en casos concretos, además, facilitaría la cooperación internacional en casos en los que se vean involucradas personas de otros países que hayan cometido delitos cibernéticos en nuestro territorio. Igualmente, es indispensable que los agentes fiscales estén actualizados en este tema.

Finalmente debe de evaluarse que la creación de la fiscalía de delitos informáticos



conlleva una serie de responsabilidades directas que van de la persecución penal hasta un buen desarrollo de pruebas científicas durante un proceso, siendo necesarios dentro de la reforma respectiva tomar en consideración dichos elementos.



CONCLUSIÓN DISCURSIVA

Los delitos informáticos o ciberdelitos se ejecutan a través de plataformas digitales lo cual hace más difícil su investigación, pero no imposible si se trabaja juntamente con más instituciones y convenios internacionales que fortalezcan la persecución y esclarecimiento de estos delitos y amparen las leyes establecidas. En la actualidad el ente investigador no está preparado para controlar las emergencias sobre ciberseguridad, ni atender las necesidades de las víctimas de un delito informático ya que no se cuenta con un respaldo legal que permita no solo persecuciones e investigaciones, sino tener planes de reacción solida dentro y fuera del territorio nacional que ampare a los ciudadanos de Guatemala.

La creación de una Fiscalía Especial en contra del Ciberdelito dentro del Ministerio Público, con el fin de garantizar el proceso de investigación y esclarecimiento del delito, con la creación de esta fiscalía se tenga el equipo adecuado en infraestructura, equipo tecnológico y equipo humano, asimismo, que se capacite y actualice al personal del ente investigador, organismo judicial y Policía Nacional Civil, para que desde ya se comience a hacer un trabajo en conjunto en contra del cibercrimen.

La legislación penal guatemalteca otorga todas las posibilidades para que se pueda dar seguimiento a los delitos informáticos, no obstante, el Ministerio Público no cuenta con una fiscalía especializada contra el cibercrimen, no cuenta con la tecnología para dar seguimiento a las acciones ilícitas cometidas por la internet, no garantizando con ello la seguridad, integridad, dignidad de la población respecto a este tipo de delitos.





BIBLIOGRAFÍA

ACUARIO DEL PINO, Santiago. **Delitos informáticos**. Primera ed., Quito, Ecuador: Ed. Puce, 2003.

AZPILCUETO HERMILIO, Tomas. **Derecho informático**. Quinta ed., Buenos Aires, Argentina: Ed. Abeledo-Perrot, 1978.

BINDER, Alberto. **Funciones y disfunciones del Ministerio Público**. Sexta ed., ciudad de Guatemala: Ed. Palacios, 1997.

CAMACHO LASA, Luis. **El delito informático**. Séptima ed., Madrid, España: Ed. Dykinson, 1,990.

CARDENAS DÍAZ, Irma Lucrecia. **El Ministerio Público en su función controladora de legalidad**. Primera ed., ciudad Guatemala: Ed. Mayte, 1994.

COUTURE, Eduardo. **Vocabulario jurídico**. Tercera ed., Montevideo, Uruguay: Ed. Piedra Santa, 1986.

DAVARA RODRÍGUEZ, Miguel Ángel. **Derecho informático**. Primera ed., Madrid, España: Ed. Aranzadi, 1993.

DÍAZ GARCÍA, Alexander. **Derecho informático, elementos de la informática jurídica**. Sexta ed., Bogotá, Colombia: Ed. Leyer, 2002.

FERREIRA DELGADO, Francisco. **El Ministerio Público**. Octava ed., Bogotá, Colombia: Ed. Temis, S.A. 1988.

FLORES SALGADO, Lucerito, **Derecho Informático**. Decima ed., Distrito Federal, México: Ed. Porrúa, 2001.

GARRONE, José Alberto. **Diccionario manual jurídico**. Quinta ed., Buenos Aires, Argentina: Ed. Artes Gráficas candil, 1989.



HUERTA, Marcelo y LIBANO, Claudio. **Delitos informáticos**. Segunda ed., Santiago de Chile: Ed. Jurídica Cono Sur, 2007.

NAVA GARCES, Alberto Enrique. **Análisis de delitos informáticos**. Octava ed., Distrito Federal, México: Ed. Porrúa, 2005.

PALAZZI, Pablo Andrés. **Delitos informáticos**. Cuarta ed., Buenos Aires, Argentina: Ed. Ad-Hoc, 2,000.

PALOMAR DE MIGUEL, Juan. **Diccionario para juristas**. Onceava ed., Distrito Federal, México: Ed. Porrúa, 2000.

SANTODOMINGO GARACHANA, Adolfo. **Introducción a la informática**. Sexta ed., Madrid, España: Ed. Ariel S.A., 1997.

Legislación:

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

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

Código Procesal Penal. Decreto Número 57-92, del Congreso de la República de Guatemala, 1992.

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

Convenio sobre la ciberdelincuencia de la Unión Europea. Budapest, Hungría, noviembre 2,001.