

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

**INCUMPLIMIENTO DEL ESTADO ANTE LA FALTA DE PROTECCIÓN
Y SEGURIDAD JURÍDICA DE LA SOCIEDAD POR DELITOS DE
ORIGEN CIBERNÉTICO**

ANA LUCÍA MIRANDA LÓPEZ

GUATEMALA, MARZO DE 2024

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

**INCUMPLIMIENTO DEL ESTADO ANTE LA FALTA DE PROTECCIÓN Y
SEGURIDAD JURÍDICA DE LA SOCIEDAD POR DELITOS DE ORIGEN
CIBERNÉTICO**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

ANA LUCÍA MIRANDA LÓPEZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, marzo 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:	Licda. Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic. Rodolfo Barahona Jácome
VOCAL III:	Lic. Helmer Rolando Reyes García
VOCAL IV:	Lic. Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br. Gustavo Adolfo Oroxom Aguilar
SECRETARIO:	Lic. Wilfredo Eliú Ramos Leonor

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente:	Lic. Rene Siboney Polillo Cornejo
Vocal:	Lic. Olga Aracely López Hernández
Secretario:	Lic. Heber Dodanin Aguilera Toledo

Segunda Fase:

Presidente:	Lic. Hector Manfredo Maldonado Méndez
Vocal:	Lic. Evelyn Johanna Chevez Juárez
Secretario:	Lic. José Alfredo Pinto Sequen

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.
veinticuatro de marzo de dos mil veintiuno.

Atentamente para el (a) Profesional, LUIS ALBERTO PATZAN MARROQUIN
para que proceda a asesorar el trabajo de tesis del (a) estudiante
ANA LUCIA MIRANDA LOPEZ, con carné 200616484
intitulado INCUMPLIMIENTO DEL ESTADO ANTE LA FALTA DE PROTECCIÓN Y SEGURIDAD JURÍDICA DE LA
SOCIEDAD POR DELITOS DE ORIGEN CIBERNÉTICO.

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 LERIOS ROBRIGUEZ
Vocal I en sustitución del Decano

Fecha de recepción 15 / 10 / 2021

Asesor(a)
(Firma y Sello)

LUIS ALBERTO PATZAN MARROQUIN
ABOGADO Y U. TITULO

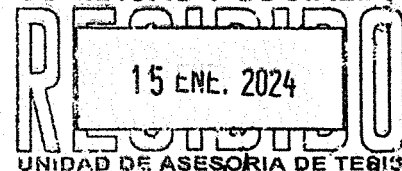
Licenciado Luis Alberto Patzán Marroquín
Abogado y notario
8 avenida 10-24 zona 1, Ciudad de Guatemala



Guatemala, 31 de agosto del 2023

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

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES



Honorable Jefe de la Unidad de Tesis:

De conformidad con la notificación de nombramiento de esta unidad, de fecha 24 de marzo de dos mil 2021, en donde se me otorga el nombramiento como **ASESOR** del Bachiller **ANA LUCÍA MIRANDA LÓPEZ**, carné 200616484; en la elaboración del trabajo titulado: **"INCUMPLIMIENTO DEL ESTADO ANTE LA FALTA DE PROTECCIÓN Y SEGURIDAD JURÍDICA DE LA SOCIEDAD POR DELITOS DE ORIGEN CIBERNÉTICO"**, me complace manifestarle lo siguiente:

A) El trabajo de la Bachiller Ana Lucía Miranda López es un adecuado aporte jurídico, dado que evidencia la ausencia de normas jurídicas que permitan la protección por parte del estado ante los delitos de naturaleza cibernética.

B) Los métodos y técnicas que se emplearon para la realización de la presente investigación de tesis fueron acordes para el desarrollo de cada uno de los capítulos, presentación, hipótesis, comprobación de la hipótesis, introducción y conclusión discursiva, para lo cual el sustentante utilizó, el método deductivo, para establecer los principios, teorías y doctrinas que asentaron el trabajo de análisis y síntesis; el método sintético, fue empleado para establecer las causas, efectos y consecuencias sociales y jurídicas del tema objeto de la investigación.

C) De conformidad con el contenido capitular de la presente investigación evidencia una correcta redacción, lo que permite comprender los elementos que analiza y la postura jurídica que le da fundamento a su exposición.



Licenciado Luis Alberto Patzán Marroquín
Abogado y notario
8 avenida 10-24 zona 1, Ciudad de Guatemala

D) La contribución jurídica y social de la presente investigación es de vital importancia, dado que el estado de Guatemala, no ha implementado políticas orientadas a la protección y seguridad de las personas que sean víctimas de delitos cibernéticos.

E) En la conclusión discursiva de la investigación refleja un adecuado nivel de síntesis, debido a que el sustentante estableció los elementos centrales que configuran los supuestos teóricos para establecer los principales hallazgos en torno a cada capítulo realizado, con lo cual logro exponer los factores que producen las consecuencias jurídicas y sociales del incumplimiento del estado de Guatemala ante la falta de protección y seguridad jurídica por los delitos de naturaleza cibernética.

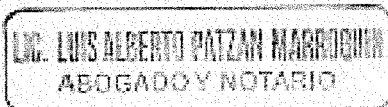
F) Igualmente la investigación refleja un adecuado uso de la información bibliográfica, la cual resulta actualizada, tomando en consideración los principios del derecho administrativo, derecho informático y del derecho constitucional, que son el fundamento de la investigación realizada.

G) Así mismo manifiesto expresamente que no me une vínculo como pariente dentro de los grados de ley con la Bachiller **ANA LUCÍA MIRANDA LÓPEZ**.

En consecuencia, emitido dictamen **FAVORABLE**, en el sentido que el trabajo de tesis desarrollado por la Bachiller **ANA LUCÍA MIRANDA LÓPEZ**, quien se identifica con el número de carné 200616484, cumple con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, aprobando el trabajo asesorado.

Sin otro particular, me suscribo de usted, atentamente.

Licenciado Luis Alberto Patzán Marroquín
Abogado y notario Colegiado: 14377





USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

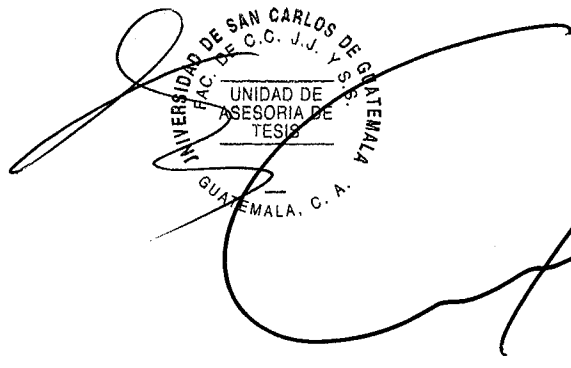


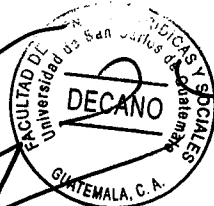
D. ORD. 66-2024

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, **ANA LUCÍA MIRANDA LÓPEZ**, titulado **INCUMPLIMIENTO DEL ESTADO ANTE LA FALTA DE PROTECCIÓN Y SEGURIDAD JURÍDICA DE LA SOCIEDAD POR DELITOS DE ORIGEN CIBERNÉTICO**. 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:** Como ser supremo que representa la máxima sabiduría del universo.
- A MIS PADRES:** Fredy Amílcar Miranda González y Lilia Melva López Zamora, por darme la vida y ser un ejemplo de superación para mí, instruyéndome siempre por el camino correcto de los buenos principios.
- A MI ESPOSO:** César Mejía, por su paciencia, amor, apoyo y comprensión durante mis estudios logrados para alcanzar la meta propuesta.
- A MI HIJA:** Zoe Romina por ser mi amor, por ser el motor de mi vida; mi inspiración para seguir luchando día a día, mi motivo para ser mejor y darle un buen ejemplo.
- A MIS HERMANOS:** Francisco Javier y Pedro Julio por ser flexibles y solidarios brindándome siempre su apoyo incondicional a favor de mi superación profesional, ya que al igual que yo comparten estos momentos de felicidad.
- A MI SOBRINA:** Emma Kamila, por ser luz y amor en mi familia, como enseñanza en la trayectoria de su vida.

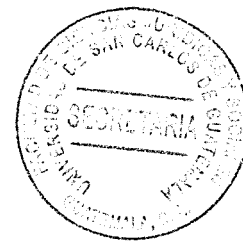


PRESENTACIÓN

La informática es aplicada en muchas áreas de la actividad humana como industria, investigación, entretenimiento, comunicaciones, transportes, química e ingeniería, entre otras de singular importancia; es precisamente ese flujo de información, lo que ha propiciado el incremento paulatino de ilícitos informáticos, es de esta manera como la siguiente investigación es de tipo cualitativa porque describe los principales aspectos que de una u otra manera confluyen para la manifestación de la problemática y se ubica esencialmente dentro de la rama del derecho penal y secundariamente en el derecho informático, dada la naturaleza del problema de investigación.

Es así como se consideró como sujeto de estudio al Estado de Guatemala, debido a su abierto incumplimiento para brindar protección y seguridad jurídica a la sociedad, en tanto que el objeto de estudio fueron las conductas delictivas o atípicas que encajan para considerarlos como tal; el periodo de estudio se localiza entre los años 2015 al 2019, considerando en ese contexto, desarrollar la misma dentro del Municipio de Guatemala, Departamento de Guatemala.

El principal aporte de la investigación gira en torno a identificar las deficiencias jurídicas e institucionales que reflejan la debilidad del aparato estatal para brindar protección y seguridad jurídicas a la sociedad por delitos de índole cibernética y que en plena era de la globalización, dejan una huella imborrable en muchas actividades en las que se ven involucradas las tecnologías de vanguardia, que por eso mismo son susceptibles de generar también cualquier afectación a bienes jurídicos protegidos y que es precisamente lo que se pretende explicar en la presente investigación.



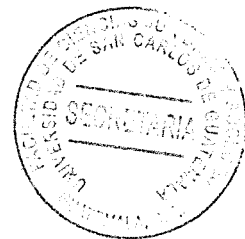
HIPÓTESIS

Derivado del incumplimiento del Estado para proteger a la sociedad guatemalteca por la comisión de todo tipo de delitos informáticos, se genera una evidente inseguridad jurídica que vulnera los derechos esenciales de la población, a través de la utilización de todo tipo de herramientas tecnológicas y/o aplicaciones informáticas que fungan como elementos centrales para la afectación de un bien jurídico como los datos personales, la suplantación de identidad y actividades relacionadas con el fraude electrónico de las actividades comerciales y financieras de los ciudadanos, circunstancia que denota las deficiencias del aparato estatal para brindar la protección correspondiente y genera la necesidad de disponer de un marco jurídico específico en materia de delitos cibernéticos, por ende es preciso efectuar el análisis conciso de las iniciativas de ley que por diversos factores no han podido trascender como ley dentro del Congreso de la República de Guatemala.



COMPROBACIÓN DE HIPÓTESIS

A efecto de poder comprobar fehacientemente la hipótesis expuesta como respuesta tentativa al problema, se utilizó el método inductivo, en virtud que se estimó de suma utilidad efectuar la generación de juicios particulares que permitieran arribar a conclusiones generales, todo ello en el afán de evaluar el incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos de origen cibernético, siendo necesario también utilizar las técnicas de investigación bibliográfica y documental, circunstancia que permitió comprobar la hipótesis en mención.



ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Derecho informático.....	1
1.1. Antecedentes.....	1
1.2. Definición.....	5
1.3. Características.....	8
1.4. Sujetos del delito.....	10
1.5. Clasificación.....	16

CAPÍTULO II

2. Principales delitos cibernéticos.....	19
2.1. Delitos relacionados con el contenido.....	20
2.2. Clasificación legal de los delitos informáticos regulados en Guatemala...	22
2.2.1. Alteración de programas.....	22
2.2.2. Delitos de reproducción de instrucciones o programas de computación.....	23
2.2.3. Programas destructivos.....	24
2.2.4. Destrucción de registros informáticos.....	26
2.2.5. Uso de información.....	27
2.2.6. Manipulación de información.....	30
2.2.7. Registros prohibidos.....	31



CAPÍTULO III

	Pág.
3. Indicios y evidencia cibernética.....	33
3.1. Antecedentes.....	33
3.2. Definición.....	37
3.3. Características.....	42
3.4. Clasificación.....	47
3.5. Procedimiento para su recolección.....	52
3.6. Diferencias entre indicio y evidencia digital.....	54

CAPÍTULO IV

4. Incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos de origen cibernético.....	57
4.1. Conceptualización de la protección y seguridad jurídica.....	57
4.2. Alcances y limitaciones de la investigación criminal en delitos cibernéticos.....	61
4.3. Vulnerabilidad de la sociedad por delitos de origen cibernético.....	64
4.4. Iniciativas del Estado para tipificar los delitos cibernéticos en Guatemala	68
4.5. Perspectivas de la sociedad guatemalteca sobre los delitos cibernéticos.	71
CONCLUSIÓN DISCURSIVA.....	75
BIBLIOGRAFÍA.....	77

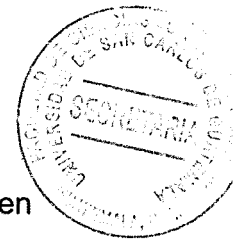


INTRODUCCIÓN

Dentro de las consideraciones centrales que propician el desarrollo del proceso investigativo, es consistente efectuar primeramente la anotación de que el Estado de Guatemala tiene como premisa el bienestar de la sociedad y sus habitantes tal como se contempla en el Artículo 2 de la Constitución Política de la República de Guatemala, determinándose también que tiene como objetivo brindar los mecanismos necesarios para el resguardo tanto físico y mental de sus habitantes, circunstancia se alcanza a través de mecanismos estatales que brinden a sus habitantes, seguridad, justicia y certeza jurídica.

En ese orden de ideas, el Estado a través de la promulgación del Decreto Número 17-73 del Congreso de la República de Guatemala, Código Penal y basado en el Artículo 274 del mismo, resguardó en forma vaga e imprecisa, los derechos antes mencionados, en virtud que se limita a juzgar los hechos delictivos surgidos del uso del internet como son la alteración, reproducción de instrucciones y programas, sin embargo la sociedad ha evolucionado, como lo han hecho otros derechos humanos; sin embargo el Estado ha incumplido con el resguardo de la sociedad al no emitir leyes que están acordes a los actos delictivos actuales, los cuales son perpetrados por medios cibernéticos.

Durante la investigación se alcanzó el objetivo general que consistió en determinar el incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos de origen cibernético; en tanto que se comprobó la siguiente hipótesis: Derivado del incumplimiento del Estado para proteger a la sociedad guatemalteca por la comisión de todo tipo de delitos informáticos, se genera una evidente inseguridad jurídica que vulnera los derechos esenciales de la población, a través de la utilización de todo tipo de herramientas tecnológicas y/o aplicaciones informáticas que fungen como elementos centrales para la afectación de un bien jurídico como los datos personales, la suplantación de identidad y actividades relacionadas con el fraude electrónico de las actividad comerciales y financieras de los ciudadanos, circunstancia que denota las deficiencias del aparato estatal para brindar la protección



correspondiente y genera la necesidad de disponer de un marco jurídico específico en materia de delitos cibernéticos, por ende es preciso efectuar el análisis conciso de las iniciativas de ley que por diversos factores no han podido trascender como ley dentro del Congreso de la República de Guatemala.

La estructura de los capítulos se distribuyó de la siguiente manera: en el primero, se describieron las generalidades del derecho informático; en el segundo, se abordaron los principales delitos cibernéticos; en el tercero, se hizo énfasis en el tema de los indicios y evidencia cibernética; finalmente el cuarto, se enfocó en el incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos cibernéticos.

A partir del contenido desarrollado en la estructura capitular, fue necesario recurrir a la utilización de los métodos inductivo y deductivo, toda vez que se requirió la generación de juicios particulares que facilitaran el arribo a la formulación de conclusiones generales y viceversa; en tanto que las técnicas aplicadas a la investigación fueron la documental y bibliográfica, entre estos, libros, leyes, reglamentos, revistas, periódicos y complementariamente todo material doctrinario que facilitara el desarrollo e integración de la totalidad de fuentes motivo de consulta.

A través de la conceptualización de los temas motivo de análisis, se considera proyectar una investigación si bien general, complementaria a los muchos documentos académicos que sobre el tema de los delitos cibernéticos o informáticos se han abordado; sin embargo, es oportuno señalar que lo que se pretende es profundizar y actualizar mucho del contenido existente hasta la fecha y también porque siempre ha generado la discusión del mismo, sin llegar a consensos reales en cuanto al alcance real y efectivo del problema, por ende la presente investigación, se estima sin lugar a dudas que servirá de sustento para el desarrollo de futuros estudios en la materia.



CAPÍTULO I

1. Derecho informático

Dentro de la valoración inicial de la problemática de investigación, se estimó razonable efectuar la aproximación jurídica y doctrinaria al concepto de derecho informático, para el efecto es preciso abordar sus antecedentes, definición, importancia, características y regulación, a fin de generar un flujo de información consistente.

1.1. Antecedentes

“En Europa, entre 1960 y 1970, a nombre de derecho y cibernética, se inicial el uso de aplicaciones informáticas en ámbitos legales, tanto regulando derechos personales como en campos de investigación. El investigador célebre Mario Lasono en 1968 propone sustituir por iuscibernética el término de jurimetria, para luego acuñarse el término derecho informático como se mencionó con anterioridad en Alemania en 1970 por el profesor Steinmüller”.¹

Así es como paulatinamente en los últimos años, cobra difusión el concepto de sociedad de la información y su promoción creciente en el ámbito público, que refiere, a la aplicación de cuestiones derivadas de innovaciones tecnológicas productoras de un cambio en el modelo económico, político, social y jurídico legal, como un ciclo de

¹ Salgado, Martín Alejandro. **Derecho informático. Documentos electrónicos: concepción, validez y eficacia probatoria.** Pág. 17.



evolución humana, con características claramente diferenciadoras de cualquier otro estadio de la cultura universal.

“El auge de la sociedad de la información se halla ligado al nacimiento de las Tecnologías de la Información y las Comunicaciones (TICs) que actúan sobre la mayor parte de los procesos técnico-económicos. Como consecuencia de esto y del desarrollo de redes, se produce la acumulación de cantidades de información de fácil acceso, que desencadena una serie de transformaciones culturales, sociales y culturales que conducen a la sociedad de la información a cobrar formas y características propias.

A fines del Siglo XX, surge un medio comunicacional que une de manera innovadora a las personas de todas partes del mundo, que desafía fronteras, tiempo y espacio, libre y con una fuerte voluntad de autorregulación: El Internet, cuyo nombre proviene de la acepción traducida al español de redes interconectadas que, trata de la conexión de millones de computadoras entre sí a una red mundial y descentralizada, que provoca un sustancial cambio en la sociedad y su manera de vincularse”.²

A través de esta aseveración se considera haber expuesto un antecedente general de lo que en la actualidad es el derecho informático y a la vez refleja el largo camino que ha debido recorrer para convertirse en lo que es en la actualidad.

“A finales de la década de los ochentas, se permite la proliferación de redes personales y locales. En 1986 se da la ruptura del monopolio de uso público por parte de Estados

² **Ibíd.** Pág. 18.



Unidos al momento que la National Science Foundation se conecta a ARPANET. En 1990 a partir de las innovaciones que introdujo la National Science Foundation se consolidó una nueva esfera de comunicación que remplazó a ARPANET y se denominó NSFNET. Se produjo un protocolo específico de comunicación denominado GOPHER que facilitó la comunicación en tiempo real.

A inicios de los noventas la red adquiere en nombre de INTERNET, como una alternativa universal que brinda libre acceso, fundada en diversas conexiones adheridas con el tiempo e inducidas por la actividad económica”.³

Con este planteamiento, se conocen los orígenes mas precisos de esta rama del derecho y como la misma ha ido evolucionando a pasos agigantados, pues la naturaleza del mismo requiere su actualización constante.

“Al respecto, es pertinente destacar que el primer contacto entre Derecho e Informática inicialmente limitó su enfoque al uso de las tecnologías para el mero almacenamiento de datos legales. Sin ser exhaustivos, se pueden identificar por lo menos tres etapas en este sentido. La primera, situada en los años 60-70, se dirigió a la construcción de bases de datos jurídicas a nivel de la administración pública. En la segunda etapa, años 80-90, la difusión de las computadoras, permitió el uso individual de la tecnología para la recolección y la redacción de textos jurídicos: la tecnología entró en el mundo privado de los bufetes de abogados y jueces que escriben textos legales.

³ Quiñónez Rodríguez, Ana Luisa. **El profesional del derecho frente a la informática jurídica en Guatemala**. Pág. 16.



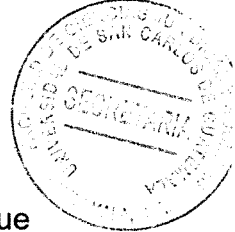
En una tercera etapa, finales de los 90 en adelante, domina el uso de Internet. En esta etapa la difusión de tecnologías aplicadas al uso diario del derecho es global y permite intercambiar propuestas, contratos, documentos legales, etc., llegando a ser un recurso para el mismo gobierno electrónico, visto en términos generales como el uso de las TIC por parte del sector público con el fin de mejorar los servicios y aumentar la transparencia y la *accountability* de los gobiernos”.⁴

Acorde la serie de preceptos que se han venido exponiendo, se estima que en torno al derecho informático, los aspectos iniciales que deben tomarse en consideración que engloban al derecho informático, son inicialmente el concepto derecho, para conocer posteriormente el derecho informático.

“Atendiendo a su etimología la palabra derecho proviene de las voces latinas *directum* y *dirigere*, que significan: conducir, enderezar, gobernar, regir, llevar rectamente una cosa hacia un término o lugar señalado, guiar, encaminar; por lo que en sentido lato, derecho quiere decir: recto, igual, seguido, sin torcerse a un lado ni a otro. La voz latina *jus*, con la que se designó en Roma al derecho, no es más que una contracción de *jussum*, participio del verbo *jubere*, que significa mandar.

En sentido general podemos decir que el derecho es un conjunto de normas jurídicas que regulan las relaciones de producción, consumo, intercambio y distribución. Regula la conducta que deben observar las personas dentro de una sociedad en relación con el

⁴ Gamboa, Jacopo. **Panorama del derecho informático en América Latina y el Caribe**. Pág. 3.



Estado, en sus relaciones económicas y con sus semejantes. Son las reglas que establecen el comportamiento de la persona dentro la sociedad”.⁵

Este planteamiento es esencial para poder conocer a profundidad el concepto de derecho informático, en virtud que si no está claro el primero, se dificultaría disponer de mayores juicios lógicos para entender el funcionamiento de este apartado.

1.2. Definición

“Es el conjunto de disposiciones dirigidas a la regulación de las nuevas tecnologías de la información y la comunicación”.⁶

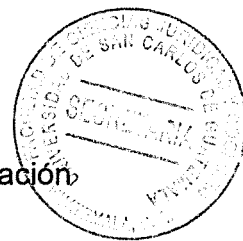
Se considera que esta rama del derecho, en esencia consiste en el conjunto de normas, aplicaciones, procesos, y relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la Informática jurídica, así como la evolución del Derecho en general. Tiene como objetivo regular la actividad jurídica, utilizándola como instrumento que simplifique al profesional del derecho el ejercicio de su profesión.

“Es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática”.⁷ Derivado de este planteamiento, se estima que es una rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos

⁵ Bosch Castro, Fulvio Homero. **Elementos fundamentales del derecho**. Pág. 18.

⁶ *Ibíd.* Pág. 20.

⁷ Altmark, Daniel Ricardo. **Informática y derecho**. Pág. 64.



como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos.

“El conjunto de doctrinas, principios y normas jurídicas que estudian las modernas tecnologías de la información, los derechos y obligaciones que nacen de la utilización de la computadora, la internet y el ciberespacio, en busca de la protección de sus usuarios en particular y de la humanidad en general”.⁸

El Derecho informático 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. Es decir, que la informática en general desde este punto de vista es objeto regulado por el Derecho.

En concordancia con esta serie de preceptos, es pertinente manifestar que esta vertiente jurídica 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. El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, que tiene en su haber antecedentes a nivel histórico.

⁸ Barrera López, Horacio Mauricio. **El derecho informático en la curricula universitaria**. Pág. 38.



“El derecho de la informática, como instrumento regulador del fenómeno informático en la sociedad, no ha sido estudiado del mismo modo que la informática jurídica, porque se ha dado más importancia a los beneficios que a los eventuales perjuicios que puedan traer consigo las computadoras respecto al derecho y la sociedad en general. Entre el reducido grupo de tratadistas sobre el derecho de la informática, algunos consideran a este una categoría propia que obedece a sus reglas; que surge como una inevitable respuesta social al fenómeno informático y que por ello es un derecho en el que su existencia precede a su esencia”.⁹

La conceptualización de este derecho permite hasta cierto punto un grado de creatividad amplio sin que trascienda a otros niveles mucho más prácticos o especulativos, de esta manera se estima necesario y consistente exponer un planteamiento mucho más concreto sobre este tema en particular; de esta manera se requiere efectuar algunas otras aproximaciones sobre este concepto en particular.

“Es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”.¹⁰

Congruentes con el planteamiento anterior, es razonable considerar que esta rama del derecho se considera como un conjunto de leyes plenamente estructuradas, en virtud que existen diversos ordenamientos jurídicos nacionales e internacionales que hacen énfasis preciso en el fenómeno de la informática.

⁹ Vivant, Michel. **Derecho de la informática**. Pág. 104.

¹⁰ Tellez Váldez, Julio. **Derecho Informático**. Pág. 14.

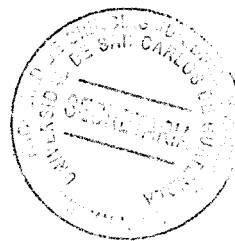


Tradicionalmente, el derecho y las tecnologías de información y comunicaciones pertenecían a dos materias distintas, siendo resumidamente el primero una disciplina que estudia la regulación de la conducta humana en la sociedad y las segundas un conjunto de servicios, redes, aplicaciones y herramientas tecnológicas cuya incorporación en las actividades del quehacer productivo y social, redundan en la mejora de la calidad de vida de las personas.

“Es el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones. Otros autores lo definen como conjunto de leyes, normas y principios aplicables a los hechos y actos derivadas de la informática. Es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que existe algún bien que es o deba ser tutelado jurídicamente por las propias normas”.¹¹

De acuerdo con los preceptos doctrinarios expuestos en la definición anterior, se estima de manera razonable que esta vertiente jurídica en particular, refiriéndose al derecho informático, se ha constituido en una renovada área jurídica, focalizada en la regulación de lo relativo a la información que fluye en línea, es decir, a la informática y a la telemática, consciente de lo anterior en esta rama del derecho también se localizan sentencias sobre el ámbito informático y sobre todo los razonamientos focalizados en cuanto al análisis e interpretación, exposición y críticas hacia el sector normativo que proyecta esta rama del derecho en particular.

¹¹ <https://previa.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf> (Consultado: 20 de diciembre de 2020).



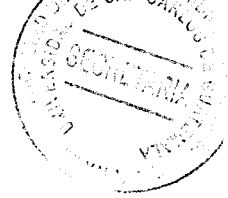
1.3. Características

“A diferencia de la política informática, la legislación informática es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso de la informática, es decir, aquí se trata de una reglamentación de puntos específicos, pero esta circunstancia necesariamente implica las siguientes consideraciones:

- a) Si se recurriría a un cuestionamiento de las reglas existentes para determinar si es posible su aplicación análoga frente al problema o si sería necesaria una ampliación en cuanto a su ámbito de cobertura.
- b) Esperar la evolución de la jurisprudencia dada la creciente presentación de casos ante los órganos jurisdiccionales en los que se fijan pautas resolutorias o al menos conciliatorias.
- c) Crear un cuerpo de nuevas reglas integrándolas a ordenamientos ya existentes, o que den lugar a una nueva ley de carácter específico. A nuestro parecer, esta última es la opción más indicada”.¹²

En concordancia directa con los preceptos vertidos con anterioridad, es consistente manifestar que esta rama del derecho, en esencia se ha tornado en interdisciplinaria, básicamente porque tiene como aspecto medular el estudio y sobre todo el desarrollo

¹² Tellez, Valdez. **Op. Cit.** Pág. 26.



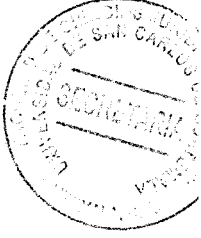
de las tecnologías que vayan dirigidas a la investigación científica, particularmente de aquellas desavenencias jurídicas.

Atendiendo esta serie de preceptos, es de suma utilidad señalar que en el área del derecho informático se considera que efectivamente si existe legislación específica en otros países como España e incluso Colombia en la cual se contempla todo lo relativo al ámbito de las tecnologías, cosa contraria en Guatemala que aún es una deuda pendiente, aun cuando se han presentado diversas un par de iniciativas que tienen como propósito fundamental regular este tipo de actividades dentro de la vida cotidiana de las personas y como tal se ha prestado también a la comisión de diversos delitos donde intervienen definitivamente una amplia gama de herramientas tecnológicas.

De esta manera, resulta razonable señalar que toda la legislación que eventualmente pueda generarse al respecto debe sustentarse principalmente en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de diferentes naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

1.4. Sujetos del delito

En materia penal, la ejecución de la conducta punible supone la existencia de dos sujetos, un sujeto activo y un sujeto pasivo. Se parte de la idea que sólo las personas (físicas o individuales), pueden cometer delitos, en virtud que sólo estas personas tienen la capacidad intelectual y razonamiento para dirigir sus acciones.



Atendiendo esta consideración, resulta razonable señalar al respecto que necesariamente dentro de estos preceptos, el bien jurídico será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. En este orden del titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente ser un tercero.

En el Código Penal guatemalteco, el sujeto activo por su participación en el delito se clasifica en autores y cómplices. En lo que se refiere a los delitos informáticos, las personas que los cometen, las cuales tienen ciertas características, como lo es, un alto grado de conocimientos, recursos, habilidades, destrezas especiales, para el manejo de la informática y tecnologías de la información y comunicaciones -T.I.C-, generalmente por la actividad laboral que realizan se encuentran en lugares donde se maneja la información de carácter sensible o bien son hábiles en el manejo de los sistemas informáticos, aun cuando, en muchas ocasiones, sus actividades no faciliten la realización de este tipo de delitos.

Siempre en concordancia con la serie de preceptos relacionados con el derecho informático, se requiere puntualizar de manera concreta que los sujetos activos de este tipo de delitos son de una gran diversidad y la diferencia entre ellos radica, en la naturaleza de los delitos cometidos, de tal manera que, el individuo que ingresa en un sistema informático sin intenciones de cometer algún delito es muy diferente de la persona que labora para una institución bancaria o inclusive en el aparato estatal para generar cualquier información encaminada a desvirtuar, fraguar algún fraude u cualquier otra conducta que lesione un bien tutelado.



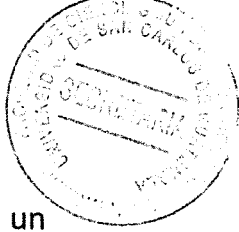
A pesar de lo anterior, teniendo en cuenta las características mencionadas de las personas que cometen los delitos informáticos, los estudiosos en la materia los han catalogado como delitos de cuello blanco; esto derivado que en la época que se empiezan a descubrir estas actividades se estableció que los sujetos activos que se dedicaban a cometer estas conductas son personas de cierto nivel socioeconómico y la realización de las conductas no puede explicarse por carencias económicas, ni por mala habitación, por falta de recreación, por no tener un alto nivel de educación, un bajo nivel intelectual, menos aún por problemas emocionales. Existen diferentes formas de denominar al sujeto activo de los delitos informáticos, sin embargo, no se pueden considerar sinónimos, entre las diferentes formas de sujetos activos se encuentran:

a) Hacker

“Intruso o pirata informático, en la mayoría de los casos, son programadores o personas inadaptadas que se dedican a realizar conductas ilícitas utilizando las computadoras”.¹³

Este término ha sido utilizado para denominar a toda persona experta en una rama de la informática y las telecomunicaciones como programación, software y/o hardware. Los hackers crean páginas señuelos con interés para el usuario el cual utiliza la excusa de las cookies para obtener esta información o incluso más información confidencial sin que el usuario pueda darse cuenta con el fin de encontrar víctimas para estudiar y encontrar agujeros o atajos en la seguridad en los usuarios

¹³ Montaña Álvarez, Alejandro Armando. **La problemática jurídica en la regulación de los delitos informáticos**. Pág. 23.

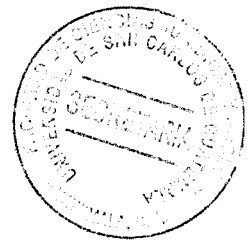


Los hackers buscan e intentan permanecer poco tiempo en ellos al día con lo que un ataque puede llevarse a cabo durante días o sólo tocar los archivos de interés sin acceder un número determinado de archivos que levante sospechas, al terminar para no ser detectado conforme a su dirección de correo electrónico o dirección de identificación pública, utiliza editores dentro del sistema infiltrado para borrar o cambiar su mismo correo o dirección de identificación pública.

b) Cracker

En cuanto al presente apartado, es de vital importancia señalar que el término Crack es una palabra proveniente del idioma inglés la cual significa romper o partir, cambiar bruscamente, y se ha venido a utilizar como un sustantivo para nombrar a las personas que se dedican a acceder en lugares prohibidos dentro del internet para destruir. Estas personas son consideradas en el ámbito informático, más peligrosas, pueden ser hackers al mismo tiempo, poseen gran capacidad de programación, amplios conocimientos en criptografías y criptoanálisis.

En este mismo orden se requiere señalar que este tipo de sujetos, de manera concreta se dedican a acceder o introducirse en los sistemas informáticos prohibidos, estimándose que esto ocurre tanto de empresas privadas como entidades de gobierno, nacionales y extranjeras para robar, destruir y distribuir programas comerciales pirateados, crean todo tipo de virus para su beneficio e incluso para venderlos a terceros, su intención es violentar los derechos de autor, más que por simple curiosidad y búsqueda de conocimiento como el hacker.

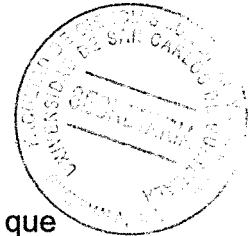


c) Phreaker

Proviene de la palabra freak, la cual es una palabra en inglés, que significa que algo o un acontecimiento es altamente inusual o irregular, la palabra phone quiere decir teléfono y la conjunción de ambas palabras nos da como resultado la palabra phreaker la cual significa la manipulación de un teléfono o un sistema de telecomunicación de forma ilícita para hacer llamadas sin pagar por las mismas.

Lo expuesto en los incisos anteriores, en esencia son actividades ilegales para enriquecerse, destruir o actos terroristas contra equipos informáticos los cuales en su mayoría son sistemas de telefonía fija o móvil celular, televisión de paga para obtener servicio gratuito mediante tecnología de avanzada comprada o creada por ellos mismos. En su evolución se han enfocado en ingresar a sitios bancarios para robar cuentas bancarias y números de tarjetas de crédito, o incluso de crear números de cuentas usando programas originales de las empresas de tarjetas de crédito y siempre son auxiliados con grandes sistemas de cómputo armados por ellos mismos.

En este mismo orden de ideas, se considera que en cuanto al concepto de sujeto pasivo, se considera que es la persona individual o colectiva quien sufre las consecuencias de la comisión de un delito siendo la sociedad y la víctima o agraviado en primer término, pero además es necesario tomar en cuenta que, en principio, el sujeto pasivo del delito, es la persona física o jurídica que resiente la conducta o actividad delictiva, es el titular del bien jurídicamente tutelado vulnerado o puesto en peligro por la conducta del responsable.

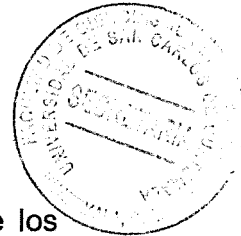


Por medio del estudio del sujeto pasivo se posibilita conocer los diferentes ilícitos que se cometen a los activos informáticos, con objeto de prever las acciones ilícitas antes mencionadas debido a que muchos de los delitos son descubiertos por casualidad, desconociendo la forma de operar de los sujetos activos, es decir la mayor parte de las veces no se tienen indicios de cómo lo realizan.

En Guatemala ha sido casi imposible establecer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de ellos no son descubiertos o no son denunciados a las autoridades competentes y si a esto se suma la falta de una adecuada legislación que proteja a las víctimas de estos delitos, la falta de preparación técnica y jurídica por parte de fiscales, investigadores y peritos para poder brindar más y mejores elementos de convicción a los encargados de la administración de justicia.

A lo anterior debe sumarse el temor por parte de las empresas a denunciar por las consecuentes pérdidas económicas, al quedar al descubierto que no cuentan con una plataforma de seguridad informática que proteja de manera eficientes los sistemas informáticos y por ende la información que se almacena y se procesa, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada cifra negra.

Mediante la divulgación de posibles conductas ilícitas por el uso de las computadoras o tecnologías de la información, que se puede alertar a las posibles víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática y si a esto se suma la creación de una adecuada legislación que proteja los intereses y derechos



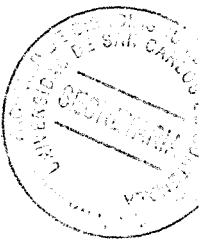
de los titulares de medios informáticos así como los que se originan del uso de los mismos, lo que se complementa con una eficiente preparación al personal encargado de la investigación, y a la administración de justicia para atender estas conductas ilícitas, se avanzaría mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse no sólo en Guatemala, si no a nivel mundial.

Los organismos internacionales han adoptado resoluciones similares para educar a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de las autoridades encargadas de hacer cumplir la ley, para detectar, investigar, prevenir y sancionar los delitos informáticos, surgiendo por consiguiente la necesidad de que dentro de la legislación guatemalteca resulte imperativo el establecimiento de un marco normativo en la materia.

1.5. Clasificación

Existen clasificaciones doctrinarias y legales de los delitos informáticos, derivado a su especialidad y complejidad, se establece una clasificación atendiendo al carácter dual de las conductas ilícitas informáticas, ya sea como medio de cometer las conductas prohibidas o bien como objeto de estas conductas, también se pueden clasificar atendiendo al bien o bienes jurídicos tutelados.

- a) "Como instrumento o Medio. En esta categoría se encuentran las conductas criminológicas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.



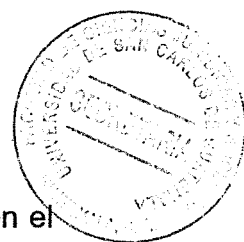
- b) Como fin u objetivo. En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física”.¹⁴

En lo que se refiere a la clasificación de los delitos informáticos de acuerdo a su fin u objeto, actividades que consisten en programación de instrucciones que producen un bloqueo total o parcial en un sistema informático, destrucción de programas, daño a la memoria o a los sistemas de almacenamiento interno, secuestro electrónico de soportes magnéticos en los que se almacena valiosa información con fines de chantaje, canje, entre otros.

El Consejo de Europa en el convenio llamado Convenio sobre la ciberdelincuencia, el cual a la fecha ha sido ratificado por veintidós países europeos y otros 22 lo han firmado, y donde Guatemala no forma parte de este grupo; es un instrumento jurídico internacional que expone y describe una serie de conductas en materia informática, que clasifica como tipos penales.

Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest el 23 de noviembre de 2001, entrando en vigor el 1 de julio de 2004. Es el único instrumento que cubre cada una de las áreas relevantes para la legislación en materia informática (derecho penal sustantivo, derecho penal adjetivo y cooperación internacional).

¹⁴ Molina Salgado, Jesús Antonio. **Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial**. Pág. 105.

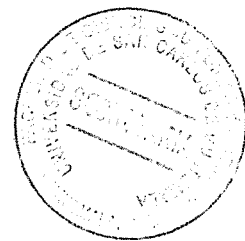


El convenio busca aplicar con carácter de prioridad, una política criminal común con el objeto de proteger a la sociedad de la denominada y creciente delincuencia informática, a través de la legislación adecuada y el fomento de cooperación internacional derivado de su carácter transnacional, sostenido en la creencia de que la lucha contra este fenómeno criminal requiere de todo el apoyo y colaboración internacional.

El convenio clasifica los delitos informáticos en cuatro grupos, dependiendo el o los bienes jurídicos que protege:

- a) "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los datos informáticos.
- b) Delitos informáticos
- c) Delitos relacionados con el contenido
- d) Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines".

Puede notarse la gama de aspectos que deben tomarse en consideración el grado de incidencia que tiene estos delitos en la realidad guatemalteca, debiéndose destacar que afectan en algún momento la estabilidad económica, política, social y cultural de los ciudadanos afectados.



CAPÍTULO II

2. Principales delitos cibernéticos

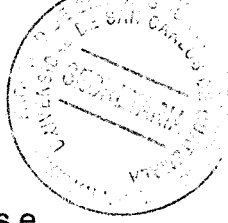
Dentro del contenido de este capítulo, necesariamente se requiere hacer énfasis en las principales figuras normativas que se estima y deben incluirse dentro de una eventual norma legal para tipificar eficientemente cualquier actividad encaminada a vulnerar un derecho o bien, siempre que en el proceso se utilice un mecanismo informático.

La comisión de estos tipos penales afecta a un bien que en los últimos tiempos ha adquirido una gran importancia como lo es la información, pudiéndose establecer al respecto, la siguiente definición: "Es el conjunto de datos alfanuméricos, numéricos o lógicos que representan la expresión de un conocimiento, que pueden utilizarse para la toma de decisiones".¹⁵

Al respecto del planteamiento anterior, resulta de suma importancia señalar que la información representada por medio o bien a través de datos informáticos, destacándose entre estos aspectos, la manipulación, alteración, sustracción o bien la supresión de la información, circunstancia que evidentemente puede causar perjuicios tanto legales como patrimoniales tanto a personas individuales como colectivas.

Los tipos penales que se describen en esta clasificación son:

¹⁵ Barrios Osorio, Omar Ricardo. **Derecho e informática. Aspectos fundamentales.** Pág. 23.

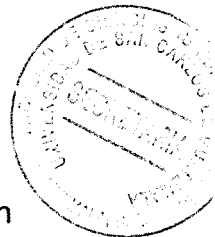


- a) Falsificación informática. Introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles o inteligibles directamente.
- b) Fraude informático. Actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: introducción, alteración, borrado o supresión de datos informáticos; cualquier interferencia en el funcionamiento de un sistema informático; con la intención de obtener de forma ilegítima un beneficio económico.

2.1. Delitos relacionados con el contenido

En esta clasificación regula lo que se refiere a la pornografía infantil, que de acuerdo al Convenio de Budapest, se entiende como todo material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca menor adoptando un comportamiento sexualmente explícito; c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

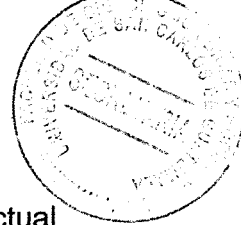
Las nuevas tecnologías actualmente son utilizadas para realizar este tipo de conductas han merecido que sean tipificadas y sean perseguibles penalmente, lastimosamente a nivel nacional no se le ha tomado la importancia debida y no se tienen los mecanismos necesarios tanto para su prevención como para su investigación y persecución, con la finalidad de proteger a los menores de edad contra estos ilícitos.



A nivel internacional, la pornografía infantil es un aspecto que ha tomado gran relevancia, el hecho que las nuevas tecnologías sean utilizadas para realizar este tipo de conductas ha merecido que sean consideradas conductas delictivas y sean perseguibles penalmente; protegiendo de esta forma la integridad de los menores de edad, quienes se han visto expuestos a ser víctimas de estos delitos.

El Convenio de Budapest, regula lo que se refiere a delitos relacionados con la pornografía infantil. Comisión deliberada e ilegítima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos.

Este apartado hace referencias a acciones ilícitas que vulneren la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, que hasta la fecha ampara a nivel internacional el derecho de los autores; así como las asumidas por el Tratado de la Organización Mundial de Propiedad Intelectual (O.M.P.I) sobre derechos de autor, de igual forma como las obligaciones asumidas en aplicación de la Convención Internacional sobre la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, Convención de Roma y del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados



con el comercio y el Tratado de la Organización Mundial de Propiedad Intelectual (O.M.P.I), sobre Interpretación o Ejecución y Fonogramas

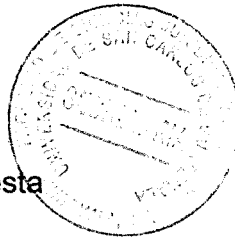
2.2. Clasificación legal de los delitos informáticos regulados en Guatemala

El Decreto número 33-96 del Congreso de la República de Guatemala, que entró en vigencia el tres de julio de 1,996, adiciona al Código Penal lo relativo a los delitos informáticos. El cuarto considerando de este Decreto establece: Que los avances de la tecnología obligan al Estado a legislar en bien de la protección de derecho de autor en materia informática, tipos que nuestra legislación no ha desarrollado.

Los delitos informáticos se encuentran regulados en el Título IV de los delitos contra el patrimonio, con el objeto de proteger las creaciones de la propiedad intelectual, así como derechos humanos intrínsecos de las personas como lo es la intimidad personal. Para clasificar los delitos informáticos regulados en el Código Penal, se analizarán desde el punto de vista del bien jurídico en la norma tipo, para tener una visión más amplia de los mismos y lo que el legislador protegió en la ley.

2.2.1. Alteración de programas

El Código Penal, en el Artículo 14 adiciona el Artículo 274 "B" establece: Alteración de programas. La misma pena. Del artículo anterior se aplicará al que altere, borrar o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras. El bien jurídico tutelado en el Artículo 274 "B", es uno de los elementos de los sistemas



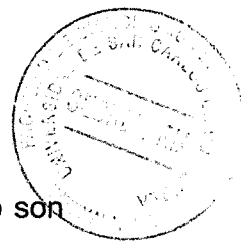
de información como lo es: las instrucciones o los programas de ordenador, esta protección es en cuanto a su funcionamiento.

Al respecto el legislador establece en cuanto a la inutilización de las instrucciones, se refiere a que con dolo no se permita utilizar una o varias de las aplicaciones o funciones del programa de ordenador y en cuanto a la inutilización de los programas que utilizan las computadoras se refiere a que los mismos no pueden ejecutarse o que se encuentran bloqueados.

En este caso se puede hacer mención a la denominada bomba de tiempo, que consiste es un programa que se adhiere de forma oculta a los programas de ordenador de los sistemas de información, para que en determinado tiempo o situación generen un bloqueo al funcionamiento del sistema o impidan el acceso a usuarios autorizados. En la mayoría el sujeto activo son los administradores del sistema, como alguna forma represiva contra los propietarios de empresas; también se dan casos externos, pero de por medio está la comisión de otros ilícitos como estafa y extorsión, al exigir cantidades dinerarias con el objeto de ya continuar con el daño a los sistemas informáticos.

2.2.2. Delitos de reproducción de instrucciones o programas de computación

El Artículo 15 del Decreto 33-96 del Congreso de la república adiciona el Artículo 274 "C", al Código Penal el cual establece: "Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de 500 a 2,000 quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las



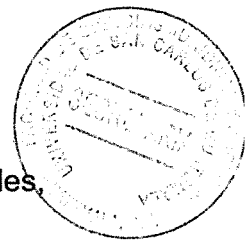
instrucciones o programas de computación”. En este caso el bien jurídico tutelado son los derechos de autor y derechos conexos del creador del programa de ordenador o la persona a quien cedió sus derechos.

En materia de programas de ordenador la persona individual o jurídica titular de los derechos de autor (morales, patrimoniales, conexos) o sus herederos, gozan del derecho exclusivo a su reproducción, distribución, importación y exportación de copias, accesos, traducción, entre otros derechos. Lo anterior queda establecido en la Ley de Derechos de Autor y Derechos Conexos Decreto 33-98 del Congreso de la República de Guatemala y determinado en los contratos que celebre con quien cede algunos de los derechos de que goza en su calidad de autor.

Se ha podido establecer con base a la información y estadísticas que proporcionan los medios de comunicación y los entes interesados, que el delito de reproducción de instrucciones o programas de computación, es el delito informático más cometido a nivel mundial. El acceso a equipo de computación o sistemas informáticos, facilitan la comisión de este delito; a ello se le suma la falta de conocimiento en materia informática en aspectos técnicos y legales, el alto costo de algunos programas de ordenador y los errores en la redacción de los contratos de desarrollo y de licencia.

2.2.3. Programas destructivos

El Decreto 33-96 del Congreso de la República de Guatemala en el Artículo 19 adiciona el Artículo 274 "G" al Código Penal, el cual establece: "Programas destructivos. Será

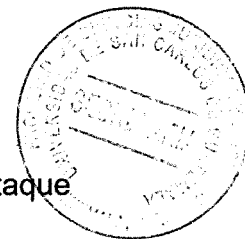


sancionado con prisión de seis meses a cuatro años, y multa de 200 a 1,000 quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación. En este caso se protege, de los programas destructivos fundamentalmente dos elementos de los sistemas de información, que son: a) Los registros y b) los programas de ordenador (software)".

Existen programas informáticos denominados virus electrónicos, virus digitales o programas perjudiciales. Los virus se definen como, los programas de ordenador que tienen por objeto introducirse en los sistemas informatizados para causar algún daño a la información, al sistema operativo, a los programas en general y se considera que algunos pueden llegar a dañar el hardware.

Estos programas han causado pérdidas patrimoniales a nivel mundial que se calculan en millones de dólares de los Estados Unidos de América. En Guatemala ha tenido consecuencias de factor económico considerable, pero no existen estadísticas o estudios al respecto para los usuarios.

Entre los programas informáticos perjudiciales, algunos dañan a la propia computadora, mientras que otros utilizan la computadora para atacar otros elementos de la red, es decir son utilizadas como instrumento o medio; estos programas pueden permanecer inactivos hasta que se desencadena por algún motivo, como por ejemplo, una fecha determinada, causando graves daños modificando o destruyendo datos.

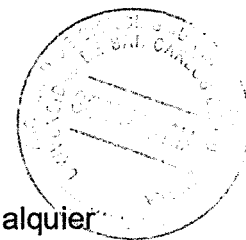


Otros programas parecen benignos, pero cuando se activan, desencadenan un ataque perjudicial (los denominados caballos de Troya); otros programas (denominados gusanos) no infectan programas con virus, pero crean réplicas de ellos mismos, estas crean a su vez nuevas replicas y de ese modo se termina por invadir el sistema. Por esta razón las personas que utilizan los sistemas de información deben de protegerse según el nivel de riesgo, con un programa antivirus; los niveles de seguridad dependen de la información y de la interconexión con otras redes.

El tipo penal se perfecciona cuando el programa destructivo se distribuye o se pone en una o varias computadoras, en una red interna o externa o la internet, aquí es cuando concurren todos los elementos que describe el tipo penal, aunque este no logre el daño que se tiene propuesto en virtud de detección o se elimine por un antivirus o se impida el ingreso a la red por cualquier medio.

2.2.4. Destrucción de registros informáticos

El Decreto Número 33-96 del Congreso de la República de Guatemala, en el Artículo 13 adiciona el Artículo 274 "A" al Código Penal el cual establece: destrucción de registros informáticos. "Será sancionado con prisión de seis meses a cuatro años y multa de 200 a 2,000 mil quetzales, el que destruyere, borrar o de cualquier modo inutilizare registros informáticos. La pena se elevará en un tercio cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial. El bien jurídico se define como registro informático, que consiste en la base de datos creada por el sistema informático utilizada para la toma de decisiones".

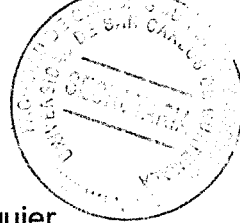


El Artículo 274 "A" establece tres verbos rectores destruir, borrar o de cualquier modo (...); en ese sentido destruir información se refiere a que el sujeto activo del tipo penal destruya la información, lo que equivale a cambiar su naturaleza de tal forma que no pueda recuperarse por medios electrónicos (el original instalado). Al establecer borrar, se refiere a eliminar de forma física de los dispositivos de almacenamiento la información. La frase o de cualquier modo deja abierta una variedad de posibilidades, como en el caso que con intención se grabe información sobre la existente, o utilice algún dispositivo para afectar el acceso a los registros informáticos.

Aunque la víctima cuente con una copia de seguridad de la información, no es causa para eximir de responsabilidades al sujeto activo. El Artículo 274 "A" también divide los registros en privados y públicos, considerando como un agravante cuando es contra los registros públicos. Debido a ello, se estima que en ausencia de legislación que determine que debe entenderse por registro públicos se interpreta que se refieren a los registros informáticos a cargo de la administración pública y que contienen datos personales. Otro criterio establece que se refiere a la naturaleza de los datos o información, es decir que los registros serán públicos aun cuando sean almacenados, procesados y/o automatizados por un ente privado.

2.2.5. Uso de información

El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 18 adiciona el Artículo 274 "F" al Código Penal el cual establece: uso de Información. Se impondrá prisión de seis meses a dos años y multa de 200 a 1,000 quetzales al que, sin



autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

En este caso se puede determinar que se protegen dos aspectos:

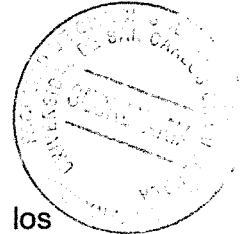
- a) Los registros informáticos, en lo que se refiere a la utilización no autorizada y
- b) El acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos.

Los cuales se desarrollan a continuación.

– Registros informáticos.

La persona que crea un registro informático de datos lícitos, tiene la facultad de disponer de quienes tendrán autorización para hacer uso del mismo. La utilización autorizada de los registros puede ser directa al computador que los tiene almacenados, en línea (red interna y externa) e inclusive pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas e inclusive un usuario autorizado para acceder al sistema, pero no para utilizar de forma distinta los registros informáticos.

Cuando un sujeto sin la autorización del titular de ese registro informático hace uso del mismo estaría incurriendo entonces en el delito de uso de información. El Artículo 274



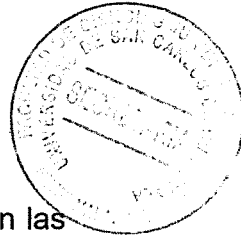
"F", contiene una forma de redacción muy limitada y puede hacer incurrir a los encargados de administrar justicia en error. En el caso de utilizar esos registros informáticos en otro sistema de información automatizado, se estaría incurriendo en el delito establecido, le genere ese uso lucro o no. Se puede dar la situación que sea una persona quien extrae el registro y otra persona la que lo utilice en su sistema, esto puede estar en concurso con otros delitos.

El simple uso de ese registro informático lo que convierte al mismo en delito, en virtud que es necesario determinar algunas características de esa información (que sean datos automatizados) para establecer si es ilícita o no esa conducta. Un ejemplo claro es cuando una persona visita un sitio web por motivos de investigación, trabajos académicos, estudios y en su trabajo hace uso de un registro informático sin la autorización, pero hace la correspondiente referencia.

- Acceso no autorizado a los bancos de datos o archivos electrónicos.

Para poder ingresar a un sistema de información se debe de estar autorizado, esta aprobación de acceso consiste, en el permiso que se le otorga a un usuario para poder hacer uso del sistema de información.

Un ejemplo de autorización a un sistema informático es el que se utiliza en las entidades bancarias: en estos casos los trabajadores tienen autorización para ingresar a determinados niveles del sistema; el receptor pagador del banco tiene acceso para

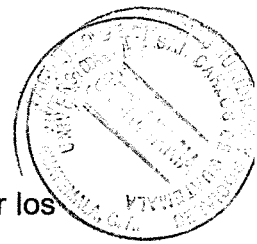


administrar e ingresar información al sistema en el ingreso o retiro de cantidades en las cuentas bancarias, pero no puede acceder a los estados de cuenta de la persona titular de la cuenta, el jefe de la agencia bancaria si tiene esta última competencia, pero no puede otorgar transferencias electrónicas por determinados montos, las cuales deben ser autorizadas por el superior de éste y así consecutivamente (según esté diseñado el sistema). Cuando el acceso al sistema lo realiza una persona que no está autorizada se encuadra esa acción a este delito. Es importante señalar que el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, inclusive si no realiza ninguna acción con la información.

2.2.6. Manipulación de información

El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 17 adiciona el Artículo 274 "E" al Código Penal el cual establece: "Manipulación de Información. Se impondrá prisión de uno a cinco años y multa de 500 a 3,000 quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica".

Este tipo penal lo comete el titular, propietario o usuario de los datos, cuando utilizando programas de computación o registros informáticos diseñados para incumplir obligaciones con el Estado o engañar a otras personas altera la información automatizada.

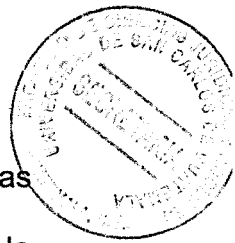


Este tipo penal parte de dos supuestos: el primero ocultar que se refiere a esconder los datos para que no puedan ser encontrados; el segundo alterar o distorsionar se refiere a cambiar los datos o darles a los datos un valor distinto al real. Además, debe determinarse el grado de participación de la persona que es autor o creador del programa de computación que permite esa administración ilícita de la información, la participación de la persona que ingresa la información y la persona que la utiliza.

En cuanto a la persona que ingresa datos tampoco tendría responsabilidad, porque esconderlos, duplicarlos o alterados, no es delito. La persona que los utiliza, que realiza la acción de ponerlos en conocimiento del Estado o de otra persona es la que comete el ilícito. Si el que ingresa los datos tiene conocimiento posterior del hecho tipificado como delito tendría la calidad de encubridor, y si tiene conocimiento que van a ser utilizados con fines ilícitos tendría participación como autor o cómplice según el caso.

2.2.7. Registros prohibidos

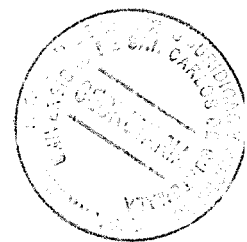
El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 16 adiciona el Artículo 274 "D" al Código Penal el cual establece: "Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de 200 a 1,000 quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas". El bien jurídico es la intimidad de la persona, pero para poder definir de mejor forma este bien jurídico es importante determinar que son datos personales. Al respecto la Ley de Acceso a la Información Pública Decreto 57-2008 del Congreso de la República de Guatemala en el Artículo 9 numeral uno define los datos



personales como: “Los relativos a cualquier información concerniente a personas naturales o identificables. Se entiende entonces que los datos personales es la Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”.

La Ley de Acceso a la Información Pública tiene una definición de datos sensibles o datos personales sensibles, en el Artículo 9 numeral 2, el cual establece: “Que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencias o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza. Entonces datos sensibles son aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”.

Se define como intimidad o privacidad, el derecho del individuo a ejercer el control de aquella información de sí mismo, que desee compartir con otros, de la cantidad que de la misma facilite a otros del momento en que desee hacerlo. La violación a esta norma surge cuando se crean bases o bancos de datos que al ser administrados de forma inadecuada o bien adquiridos de una forma ilegal, que entren en la esfera de la intimidad de las personas se estaría cometiendo el delito de registros prohibidos.



CAPÍTULO III

3. Indicios y evidencia cibernética

En este capítulo se describe de forma generalizada, las principales acepciones existentes en torno a los conceptos de indicios y evidencia cibernética, para el efecto se requiere hacer énfasis en sus antecedentes, definición, características, clasificación, procedimiento para su recolección y las diferencias entre indicio y evidencia digital.

3.1. Antecedentes

En torno a este apartado histórico de lo que se conoce como evidencia digital, se debe realizar primero un análisis a la institución de la prueba penal, es pertinente señalar algunas concepciones doctrinarias, a fin de contrastar el momento histórico en el que se dieron los primeros pasos sobre su consideración dentro de un litigio, conflicto o debate como se le conoce en la actualidad.

“Desde el surgimiento de las primeras formas o intentos de derecho positivo, por ejemplo: el denominado Código de Hammurabi, que era un conjunto de reglas escritas en una estela de piedra, del pueblo sumerio, en el cual predominaban sanciones draconianas, como la llamada Ley del Talión; se aprecia, que ya se manifiesta, aunque de manera muy embrionaria el derecho a probar. En efecto, en dicho conjunto de normas, tan antiguo, denominado por muchos primitivo, se vislumbra ya la necesidad de probar, en un afán humano tan importante como la vida misma: determinar a los



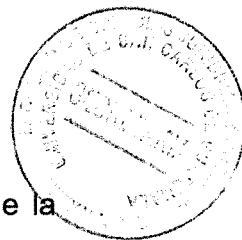
responsables de un crimen sin perjudicar a los inocentes. Allí igualmente, se vislumbran, primitivos afanes, por defender lo que hoy en día conocemos como un principio sustancial, que se encuentra hondamente ligado al derecho penal y a la prueba: el Principio de Presunción de Inocencia”.¹⁶

Es una forma generalizada de concebir los registros históricos de la prueba penal, en ese orden de ideas, se requiere profundizar en torno a estos preceptos, para el efecto, se plantea la siguiente definición: el derecho penal resulta tan antiguo como la humanidad, básicamente porque rige o regula en esencia el accionar del ser humano, consecuentemente se aplica cuando se realizan acciones y/o omisiones que ponen en peligro un bien jurídico protegido por alguna ley en particular; el derecho penal empezó a evolucionar luego de suscitarse el periodo o época de la venganza privada, en donde cada quien se procuraba justicia por mano propia.

Esta circunstancia fue posteriormente atenuada por la ley del talión que era una venganza proporcional al daño ocasionado al sujeto pasivo, surgiendo luego otra forma de venganza privada, conocida oportunamente como la composición, misma que se presentaba cuando el ofensor entregaba al ofendido o a su familia cierta cantidad de bienes o especies para no padecer en carne propia, la venganza de los ofendidos.

De ahí que tanto en la venganza privada cómo en la venganza divina la aplicación del derecho penal, la prueba se obtenía en forma primitiva por medio de supersticiones y

¹⁶ <http://blog.pucp.edu.pe/blog/nuevoprocesopenal/2013/11/15/los-antecedentes-mas-antiguos-de-la-prueba/> (Consultado: 08 de enero de 2020).

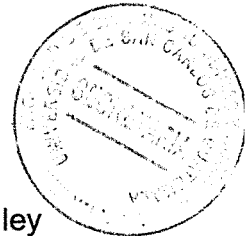


los jueces se apegaban a encontrar la verdad de los hechos delictivos a través de la manifestación de la divinidad, no utilizando la razón para la solución de los diversos casos sometidos a su conocimiento, siendo esto una forma de derecho penal primitivo, en sus manifestaciones sustantiva, adjetiva y probatoria.

El derecho procesal penal fue evolucionando de conformidad con los sistemas políticos que surgieron durante la historia por lo que en esta evolución se llegó al punto en que los jueces tenían que aplicar la razón en la valoración de los elementos de prueba en los hechos penales sometidos a su conocimiento, apareciendo los sistemas inquisitivo y acusatorio; es a partir de estos sistemas donde surgió netamente la institución que hoy se denomina prueba penal.

Se comprende con mucha mayor precisión, los aspectos que engloban el concepto de prueba, esencialmente en cuanto a sus registros históricos, cuando se inició con su utilización y que demuestra la forma en que gradualmente se ha ido perfeccionando y en el caso de la legislación guatemalteca, hasta quedar plasmado en el Decreto Número 51-92 Código Procesal Penal.

“Un adagio latino, por demás evidente, proclama: *demonstrationis veritas* (prueba es la demostración de la verdad). Lo arduo, dada la infinidad de las convicciones humanas, consiste en establecer cuando está algo demostrado; si bien el problema se reduce en lo procesal, por cuanto la parte triunfa cuando logra que el juzgador admita como real lo que ella afirma o que desconozca lo que ella niega. Las partidas entendían por prueba la averiguación que se hace en juicio de alguna cosa dudosa o bien la producción de



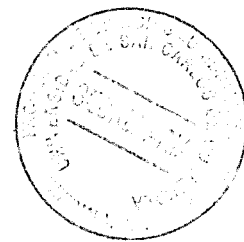
los actos o elementos de convicción que somete el litigante, en la forma que la ley previene, según derecho, para justificar la verdad de los hechos alegados en el pleito”.¹⁷

De acuerdo con esta concepción, es importante señalar que el estudio de los elementos de prueba a través del desarrollo evolutivo del derecho penal, ha variado considerablemente desde su inicio hasta la época actual, esto es debido a que en sus inicios o en la llamada época de la venganza privada, donde las personas en virtud de la violencia que existía, no hacían mayor cosa por averiguar la verdad de los hechos, sino se dedicaban a ocasionar un daño como el que se les había causado, con sus propias manos, por lo que no existían normas jurídicas que regulaban como se debía de probar los delitos u ofensas que cometían las personas dentro de la sociedad.

En la segunda época del derecho penal, se consideraban únicamente las pruebas que recaudaba la iglesia a través de sus sacerdotes en los juicios divinos, sin importar los procedimientos a través de los cuales se incorporaban al proceso, en ese contexto, eran formas muy violentas, sin que la contraparte pudiera hacer efectivo el principio de defensa.

Durante la época de la venganza pública, aparecen las primeras leyes penales, en donde se regulan la totalidad de los elementos probatorios, pero el principal siguió siendo la confesión, misma que podía ser obtenida a base de la tortura u otras formas violentas que en la actualidad son abiertamente ilegales.

¹⁷ Turtón Ávila, William Harold. **Necesidad de incluir un medio de impugnación en la audiencia de ofrecimiento de prueba en el proceso penal guatemalteco.** Pág. 68.



3.2. Definición

“Indicio es todo rastro, vestigio, huella, circunstancia y en general, todo hecho conocido, mejor dicho, debidamente comprobado, susceptible de llevarnos por la vía de inferencia, al conocimiento de otro hecho desconocido”.¹⁸

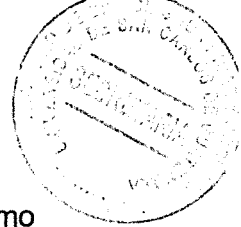
En relación con este planteamiento, el hecho considerado en concreto debe estar debidamente probado, para que adquiera la categoría de prueba, en el momento procesal oportuno y que ese hecho comprobado en virtud de una inferencia lleva al conocimiento de otro hecho desconocido; en esencia, la prueba indiciaria consiste en una actividad probatoria de naturaleza necesariamente discursiva e indirecta, cuya fuente es un dato comprobado, y se concreta en la obtención del argumento probatorio mediante una inferencia correcta, que posteriormente va adquiriendo un sustento mucho más concreto, hasta convertirse en prueba.

“Es la reunión e interpretación de una serie de hechos y circunstancias relativos a un injusto determinado que se investiga, a efectos de intentar acceder a la verdad de lo acontecido por vía indirecta”.¹⁹

El autor pretende exponer que a través de la prueba indiciaria lo que se hace es probar directamente los hechos mediatos para deducir de estos aquellos que tienen un gran significado para la causa que se pretende probar.

¹⁸ Dellepiane, Antonio. **Nueva teoría de la prueba**. Pág. 101.

¹⁹ Desimoni, Luis María Madrid España. **La prueba indiciaria**. Pág. 98.



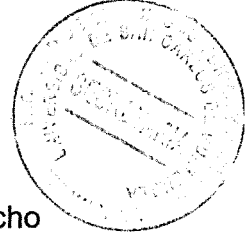
“La prueba circunstancial se basa en el valor incriminatorio de los indicios, y tiene, como punto de partida, hechos y circunstancias que están probados y de los cuales se trata de desprender su relación con el hecho inquirido, esto es ya un dato por complementar, ya una incógnita por determinar, ya una hipótesis por verificar, lo mismo sobre la materialidad del delito que sobre la identificación del culpable y acerca de las circunstancias del acto incriminado”.²⁰

La prueba circunstancial puede ser explicada de una mejor manera con huellas dactilares, que pueden probar la presencia de una persona en particular en la escena del delito o su contacto con un objeto utilizado en el delito.

Es esencial que la prueba por indicios como actividad probatoria es utilizada ante la insuficiencia o falta de pruebas directas, los que debidamente acreditados pueden servir de base para desvirtuar la presunción de inocencia. En términos generales se puede conceptuar al indicio como el hecho o dato conocido indubitavelmente probado y por el que a través de un razonamiento lógico o presunción se acredita la existencia de otro hecho desconocido pero que está íntimamente vinculado al primero.

En segundo lugar, el indicio como razonamiento o proceso lógico inherente a su esencia exige la conexidad indispensable entre el acto inicial y el hecho a probar, recordemos que lo que se quiere lograr con el indicio es probar un hecho que no cuenta con medios directos que permitan conducir a concluir un resultado, careciendo en un

²⁰ Suprema Corte de Justicia de Colombia. **Valoración de la prueba circunstancia**. Pág. 3.

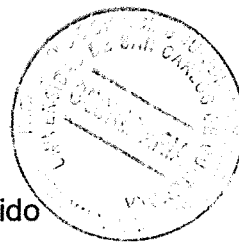


primer momento el cognoscente de medios que permitan captar la convicción del hecho central a probar.

En cuanto al manejo de la evidencia digital, se ha indicado que no existe un manual o un protocolo para el manejo de la misma, manual que debe ajustarse a ciertas normativas nacional o internacionales, con el objeto de asegurar sus características propias para que puedan ser valoradas dentro de un proceso penal, principalmente en la etapa en donde se origina la prueba, en la etapa de juicio.

A nivel nacional con la entrada en vigencia de la Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, regula aspectos procedimentales para reconocer jurídicamente el valor de las comunicaciones electrónicas, definiendo a las mismas como toda comunicación que las partes hagan por medio de mensajes de datos. Durante el desarrollo de una investigación criminal, se puede llegar a contar con elementos de investigación que aportarán información para el esclarecimiento de un hecho categorizado como delictivo, en este proceso suele tomarse como sinónimos los términos indicio, evidencia y prueba; en ese sentido, indicio puede ser definido como acepción de prueba o bien en el de objeto, huellas, signo, rastro, es decir de simple hecho o conducta.

En materia probatoria penal no se puede hablar de presunción, derivado que cualquier resolución que se emita utilizando como fundamento una presunción violenta los principios de inocencia y de defensa, al dar por acreditados hechos sino se presenta



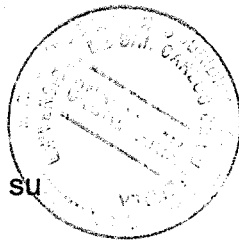
prueba en contrario. En otras ramas del derecho se denomina presunción, en sentido propio, a una norma legal que sustituye en forma absoluta la demostración del hecho, pues se tienen por acreditado si se establecen la existencia de las circunstancias que basan la presunción y sin admitir demostración en contrario.

Regularmente en la jurisprudencia y en la ley, se utiliza de manera incorrecta el término presunción, como sinónimo o equivalente a indicio, tratando talvez de captar con el término presunción, la conclusión a que se puede llegar partiendo de un indicio. Es importante señalar que indicio y presunción, son dos conceptos diferentes, el problema ha surgido cuando en muchas ocasiones se utilizan como sinónimos.

"La evidencia digital se constituye en todos aquellos datos e información histórica y presente almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia".²¹

De acuerdo con este planteamiento susceptible de localizar en fuentes doctrinarias, se estima de manera razonable que en esencia la evidencia de índole digital, no es más que aquella información almacenada en algún tipo de dispositivo electrónico, que mediante el expertaje correspondiente, puede pasar a formar parte del cúmulo de elementos de convicción que puede y son susceptibles de utilizar en el proceso penal correspondiente y que permitirá descubrir eventualmente la verdad histórico de un hecho tipificado como delito.

²¹ Del Pino, Santiago Acurio. **Delitos informáticos, generalidades**. Pág. 10.



“Es el conjunto de datos en formato binario, esto se comprende en los archivos, su contenido o referencias a éstos, que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático”.²²

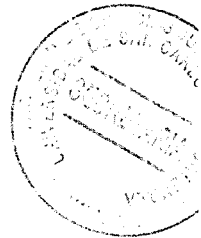
Se comprende a través de este planteamiento que en esencia este aspecto guarda estrecha relación con el planteamiento anterior, únicamente que expresado de una forma diferente, pues utiliza para el efecto un lenguaje técnico, pero que siempre es un tipo de información almacenada en algún dispositivo electrónico.

“La evidencia digital como objetos de datos en relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento de multimedia, que no son más que cadenas de unos y ceros, es decir de información binaria o digital grabada en un dispositivo magnético (como discos duros o los disquetes), en uno de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD)”.²³

Justamente como se ha venido exponiendo, el concepto de evidencia digital siempre hace énfasis a la información que es susceptible de localizar en dispositivos de almacenamiento, con la salvedad que en esta definición se hace énfasis en los tipos específicos de unidades en que se puede localizar, denominando con nombre propio a dichos elementos a fin de generar una mayor comprensión sobre este aspecto. En ese contexto, referirse en concreto a la finalidad de la prueba, no solo es referirse a los

²² López Delgado, Miguel. **Análisis forense digital**. Pág. 19.

²³ Reyes, Anthony. Investigación del cibercrimen. Pág. 34.



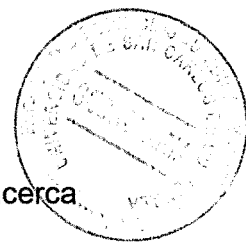
hechos susceptibles de ser probados, sino también a las afirmaciones que las partes realizan en torno a dichos hechos.

3.3. Características

Los elementos característicos de la evidencia digital, necesariamente deben ser los que doctrinariamente han sido determinados para la prueba en general, pues no puede concebirse que la evidencia digital al ser un medio probatorio, pueda tener características diferentes a las ya establecidas genéricamente para la prueba.

Es necesario enfatizar en los preceptos contenidos en los Artículos 181 y 183 del Decreto Número 51-92 Código Procesal Penal, donde se señalan las características que debe tener la prueba para ser admisible.

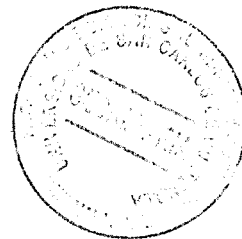
- a) **Objetiva:** La prueba no debe ser fruto del conocimiento privado del juez ni del fiscal, sino que debe provenir al proceso desde el mundo externo, siendo de esta manera controlada por las partes. Por ejemplo, si el juez conoce de un hecho relevante relacionado con el proceso a través de un amigo, no podrá valorarlo si no es debidamente introducido al proceso. El código en su artículo 181 limita la incorporación de la prueba de oficio a las oportunidades y bajo las condiciones previstas por la ley.
- b) **Legal:** La prueba debe ser obtenida a través de medios permitidos e incorporada de conformidad a lo dispuesto en la ley.



- c) Útil: La prueba útil será aquella que sea idónea para brindar conocimiento acerca de lo que se pretende probar.
- d) Pertinente: El dato probatorio deberá guardar relación, directa o indirecta, con el objeto de la averiguación. La prueba podrá versar sobre la existencia del hecho, la participación del imputado, la existencia de agravantes o atenuantes, el daño causado, etc.
- e) No abundante: Una prueba será abundante cuando su objeto haya quedado suficientemente comprobado a través de otros medios de prueba.
- f) Relevancia: La prueba es relevante cuando se funda un juicio de probabilidad, la idoneidad convencional es conocida como relevancia o utilidad de la prueba. Asimismo, la prueba debe ser relevante, es decir, que el elemento de prueba que se incorpora al proceso no solo debe tener relación con el hecho que se investiga, sino que además, debe permitirle al juez que la valora, obtener un grado de certeza y probabilidad sobre la verdad formal de los hechos.

La prueba en el proceso penal acusatorio, como es el caso de Guatemala, está constituida por aquella actividad que han de desarrollar las partes acusadoras en colaboración con el Tribunal a objeto de desvirtuar el estado de no culpabilidad respecto del delito que se le atribuye o derecho a la presunción de inocencia, el cual es el punto de partida de toda consideración probatoria en un proceso penal que se inicia con la verdad provisional o interina de que el imputado es inocente.

“Los caracteres básicos de la prueba en el proceso penal acusatorio son los siguientes:

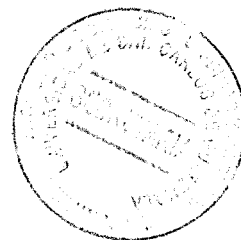


- a) Carga material de la prueba corresponde a la parte acusadora.
- b) Sólo tiene el carácter de prueba las practicadas en el juicio oral, bajo los principios de inmediación, contradicción, publicidad e igualdad.
- c) Las pruebas deben de haber sido obtenidas por medios lícitos.
- d) Las pruebas requieren de cierta entidad, no bastando las conjeturas o las meras sospechas.
- e) Existe libertad en los medios de prueba.
- f) Existe libre valoración de la prueba”²⁴

Al recibir la noticia criminal el fiscal correspondiente tiene el primer acercamiento a los hechos penalmente relevantes que se supone han ocurrido en el ámbito de su competencia en la sociedad y frente a los que, utilizando los medios de acreditación obtenidos a través de actos de investigación, tiene el deber de lograr el mayor conocimiento posible para tomar las decisiones que correspondan. Si decide ejercer la acción penal, esto es, someter la pretensión al juez de conocimiento mediante la acusación; tendrá que presentar al juez el conocimiento de los hechos.

La evidencia digital es única, cuando se la compara con otras formas de evidencia. A diferencia de la evidencia física, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único es su potencial de realizar copias no autorizadas de archivos, sin dejar rastro alguno. La evidencia digital posee, entre otras, las siguientes características:

²⁴ Bravo Barrera, Rolando. **La prueba en materia penal**. Pág. 8.



- a) Es volátil
- b) Es anónima
- c) Es duplicable
- d) Es alterable y modificable
- e) Es eliminable

Tales características sugieren la exigente labor requerida por los especialistas cuando tenga que llevarse adelante investigaciones sobre la delincuencia informática, en procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada en la escena del crimen.

Se requiere tratamiento especial a tiempo de manejar la evidencia digital durante el juicio, más allá del cumplimiento de las normas formales, pues estas deben estar articuladas con los esfuerzos de conservación y seguridad de los estándares internacionales.

De manera general a la evidencia digital también se le conoce como prueba electrónica, en su acepción general dentro del ámbito probatorio, puede ser considerada como cualquier información almacenada o transmitida en forma digital, la que una de las partes podrá utilizar en el juicio. La evidencia digital puede convertirse en un factor fundamental dentro de un proceso de investigación preparatoria, no obstante, no puede omitirse que ésta es frágil y volátil y que por lo tanto, puede tornarse en una desventaja para el sistema de justicia que no tenga los mecanismos adecuados para su efectivo

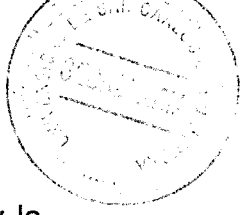


desarrollo, el Ministerio Público, en tal sentido necesitaría un laboratorio forense especializado en la recuperación de registros digitales.

Dentro del campo de la criminalista podemos identificar la informática forense, la que va adquiriendo inusitada importancia, debiéndose resaltar su carácter científico, por ello, tiene sus fundamentos en las leyes de la electricidad, de la física y el magnetismo, siendo importante puntualizar que es en base a fenómenos electromagnéticos que la información puede ser almacenada; por ello se afirma con certeza que la informática forense colabora en la investigación de delitos cometidos por organizaciones criminales, apoyándose en el método científico.

La evidencia digital permite acreditar hechos que conllevan efectos jurídicos. A título de ejemplo, éstos pueden ser: fugas de información confidencial, alteración de documentos electrónicos, empleo sin autorización de creaciones protegidas por la propiedad industrial o intelectual, actuaciones de competencia desleal, entre otros.

Los anteriores pueden desencadenar procesos judiciales de tipo mercantil, civil, laboral o social, administrativo y penal. Sin embargo, la evidencia digital también puede evitarlos, pues permite acreditar el cumplimiento de las obligaciones derivadas de un contrato. Las evidencias digitales se alojan en servidores de correo electrónico, teléfonos móviles, dispositivos USB, discos duros de ordenadores de puestos de trabajo, Internet, entre otros de especial importancia. Los delincuentes hoy están utilizando la tecnología para facilitar la comisión de infracciones y eludir a las autoridades. Este hecho ha logrado que las Tecnologías de la Información y la



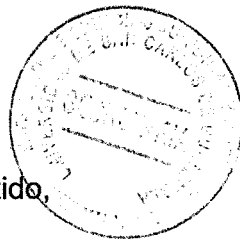
Comunicación se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

La obtención de Información demanda que los investigadores forenses encargados de la recolección preservación, análisis y presentación de las evidencias digitales hagan una labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal. Una forma segura de obtener evidencia digital cuando no se tiene una orden judicial es aislar el dispositivo en el cual se presume la existencia de evidencia digital en un compartimiento cerrado hasta tanto la corte determine autorizar el escrutinio y análisis de la información.

A fin de evitar la destrucción de evidencia digital es recomendable extraer una copia de seguridad íntegra del sistema mediante medios como imágenes de disco, backups en cintas o cdroms, entre otros. Todos estos elementos se conocerán detalladamente en el siguiente numeral donde se establece la clasificación correspondiente de los diferentes medios o dispositivos que pueden considerarse como evidencia digital.

3.4. Clasificación

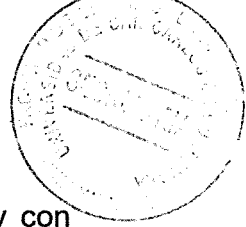
La importancia de la tecnología en las actividades judiciales en cualquier ámbito, ha ido cobrando notoriedad paulatinamente en virtud de la relevancia de la carga de la prueba y esencialmente en torno a la libertad de la prueba contenido en el Artículo 182 del Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, que resalta que se podrán probar todos los hechos y circunstancias de



interés para la correcta solución del caso por cualquier medio de prueba permitido, estimándose que dentro de estos aspectos se incluyen los elementos o dispositivos electrónicos o digitales, pues es un hecho notorio de que el paulatino incremento en el uso de las tecnologías y comunicaciones en el país, constituyen mecanismos óptimos y consecuentemente susceptibles de ofrecerse como medios probatorios.

La utilización de mecanismos digitales o electrónicos como medios de prueba dentro de un proceso penal en particular, ha delimitado una mayor brecha sobre los medios que oportunamente pueden incluirse como prueba para dirimir una controversia y que a la larga ha venido a beneficiar al sistema de justicia en general, básicamente porque estos elementos han implicado nuevos medios de investigación, mucho más útiles, versátiles y decisorios, en virtud que muchos de estos aspectos son considerados como medios de prueba científicos, minimizando con ello la subjetividad en la prueba que recurrentemente se generaba hasta hace una década.

En ese sentido, el uso de nuevos medios de investigación en el proceso penal, obliga a la adopción de una serie de reflexiones sobre el papel del Estado en el derecho en el moderno proceso penal, en virtud que al mismo le han correspondido una serie de cambios acorde con las nuevas tareas que se le han confiado en el campo de la seguridad interna del Estado y del combate del crimen organizado en la circunscripción geográfica de la República de Guatemala. Las nuevas herramientas tecnológicas, que se utilizan cotidianamente, permiten que se pueda reconstruir fácilmente donde se encontraba la víctima o el victimario, antes, durante y después de la comisión de un

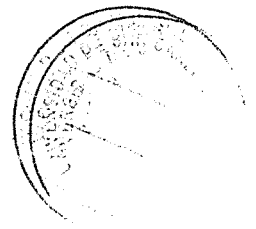


evento delictivo, reflejándose en tal sentido la serie de actividades que realiza y con quiénes se comunica, entre otros aspectos de relevancia.

Tanto teléfonos fijos y móviles, laptops, tarjetas de accesos a edificios, cámaras de seguridad, discos externos, Cd's, Dvd's, dispositivos extraíbles, impresoras, faxes, memorias de máquinas fotográficas, escáneres, memorias portátiles e inclusive los desplegados telefónicos que tanto han permitido la desarticulación de estructuras criminales, fundamentalmente porque en los mismos vienen incluidos las referencias geoposicionales de los objetivos y que en determinado momento permiten establecer su ubicación en el momento de suscitarse un evento delictivo en particular.

Este enorme abanico de posibilidades tecnológicas, son sólo algunos de los mecanismos que son susceptibles de utilizar diariamente en la vida personal y laboral; consecuentemente con ello, es necesario también hacer uso de los mismos dentro de los diversos diligenciamientos que deben atenderse en el proceso penal en general, resultando de ahí su importancia como mecanismos complementarios y necesarios para garantizar la eficiencia y eficacia de las actividades efectuadas en el marco de las actividades requeridas.

Algunos dispositivos tecnológicos que se encuentran estrechamente relacionados con el ámbito de la informática, en consecuencia, se considera que pueden volverse indicios o vestigios criminales que posteriormente se convertirán en evidencia digital, dentro de estos aspectos se señalan al respecto los siguientes:



a) Dispositivos de salida

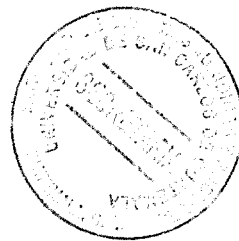
Se estima que son aquellos que permiten la comunicación entre la computadora y el usuario y la información sale en lugar de entrar, de entre esta gama de elementos se encuentran pantallas o terminales, impresoras y altavoces, plotters, visualizadores, tarjetas de sonido, altavoces y auriculares.

b) Dispositivos de entrada

Son aquellos que sirven para introducir datos a la computadora para su proceso. Los datos se leen de los dispositivos de entrada y se almacenan en la memoria central o interna. Los dispositivos de entrada convierten la información en señales eléctricas que se almacenan en la memoria central. Dentro de estos dispositivos se localizan por ejemplo teclados, dispositivos apuntadores, ratones (mouses), joystick (controles para videojuegos), escáneres, cámaras web (webcam), pantallas táctiles, teclados, lápices ópticos, gamepad, lectores de códigos de barras, lectores de códigos QR, sensores de huellas dactilares, cámaras digitales y micrófonos, entre otros.

c) Dispositivos mixtos

Son dispositivos mixtos, por ejemplo, la memoria RAM, un grabador de cds o dvds, el disco duro, un modem, principalmente porque todos pueden enviar o recibir datos de la Unidad Central de Procesos (CPU), de esta cuenta se considera que son susceptibles de localizar dentro de estos elementos, Fax-Módem, tarjeta de red, tarjeta de sonido.



d) Unidades o dispositivos de almacenamiento

Dentro de estos elementos, se destacan principalmente los discos duros internos y externos, debiéndose señalar que los discos duros tienen una gran capacidad de almacenamiento de información, pero al estar alojados normalmente dentro de la computadora (discos internos), no son extraíbles fácilmente.

Para intercambiar información con otros equipos (si no están conectados en red) se tienen que utilizar unidades de disco, como los disquetes, los discos ópticos (CD, DVD), los discos magneto-ópticos, memorias USB o las memorias flash, cintas magnéticas, memorias flash, entre otros.

El disco duro almacena casi toda la información que se maneja al trabajar con una computadora. En él se aloja, por ejemplo, el sistema operativo que permite arrancar la máquina, los programas, archivos de texto, imagen, vídeo, etc. Dicha unidad puede ser interna (fija) o externa (portátil), dependiendo del lugar que ocupe en el gabinete o caja de computadora.

Un disco duro está formado por varios discos apilados sobre los que se mueve una pequeña cabeza magnética que graba y lee la información. En ese sentido, se considera que este componente, al contrario que el micro o los módulos de memoria, no se pincha directamente en la placa, sino que se conecta a ella mediante un cable. También va conectado a la fuente de alimentación, pues, como cualquier otro componente, necesita energía para funcionar.



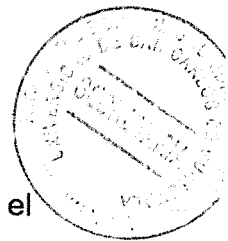
Las características principales de un disco duro son:

Capacidad: Esta se mide en gigabytes (Gb), estimándose que este es el espacio disponible para almacenar secuencias de un byte. La capacidad aumenta constantemente desde cientos de megabytes, decenas de gigabytes, cientos de gigabytes y hasta terabytes que no son más que disponer de más de 1000 gigabytes y así sucesivamente, hasta almacenar enormes cantidades de información.

Capacidad de transmisión de datos: Respecto a este apartado, se estima de utilidad destacar que de poco servirá un disco duro de gran capacidad si transmite los datos lentamente y este último aspecto influye determinadamente en los flujos de datos y por ende en cierta medida la fidelidad de la información. Los discos actuales pueden alcanzar transferencias de datos de 3 gigabytes por segundo.

3.5. Procedimientos para su recolección

Los aspectos relativos a la recolección y el embalaje de los indicios digitales, se encuentra a cargo de técnicos criminalistas de la Dirección de Investigaciones Criminalísticas del Ministerio Público, específicamente de la Unidad de Recolección de Evidencias, quienes con exclusividad efectúan la documentación y recolección de los vestigios que oportunamente son susceptibles de localizar en cualquier escenario criminal, desde luego que todo ello bajo las directrices y supervisión de un fiscal quien está a cargo del procedimiento en su totalidad.



El fin primordial de la Unidad de Recolección de Evidencias del Ministerio Público es el de recolectar y remitir las evidencias y otros medios de convicción que coadyuven al esclarecimiento de los hechos delictivos que investiguen los órganos del Ministerio Público y sus funciones se desarrollan bajo la conducción del Fiscal a cargo del caso. Está compuesta por el Gabinete Técnico, el cual a su vez se compone de las Unidades de Monitoreo y Unidad Recepción, Análisis, Control y como dependiente directo de esta unidad se encuentra el Archivo e Información.

Todas las diligencias que se realizan dentro de la Dirección de Investigaciones Criminalísticas, son llevadas a cabo por la existencia de solicitud por escrito que sea realizada por el agente o auxiliar fiscal que esté encargado del caso en el que solicite la investigación, peritaje o cualquier otra diligencia.

En torno a la recolección de la evidencia digital en la República de Guatemala, no se cuenta con un procedimiento en específico para efectuar la documentación de la totalidad de dispositivos que son susceptibles de localizar en los diversos escenarios que tienen a bien documentar.

Desarrolla el procesamiento de la escena del crimen y la recolección de indicios, bajo la dirección del fiscal responsable del caso y ejecutando las medidas dictadas para proteger y aislar indicios en los lugares en los que se esté investigando un delito, a fin de evitar contaminación o destrucción de rastros, evidencias u otros elementos materiales; elaborando los informes correspondientes, inmediatamente después de procesar la escena del crimen, de conformidad con disposiciones específicas;

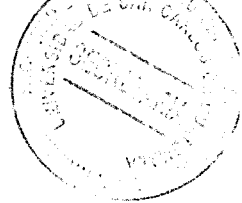


registrando y controlando las acciones realizadas por parte del personal en la escena del crimen o recolección de indicios, entregando de manera oportuna los informes de los casos asignados, por grupo e individual.

A pesar que se cuenta con la Instrucción del Ministerio Público 166-2013, Manual de Normas y Procedimientos para el Procesamiento de la Escena del Crimen, en el mismo no se localiza ningún apartado procedimental que permita efectuar con objetividad, precisión y efectividad, la documentación de indicios digitales en el país, estimándose en tal sentido que es en torno a estos preceptos que giran los aspectos medulares de la presente investigación, principalmente porque no se cuenta o detalla con precisión, los mecanismos a utilizar para la documentación de la evidencia digital que se localiza constantemente en plena era de la información, donde cada vez más es susceptible de localizar todo tipo de indicios de esta naturaleza y la importancia que tiene la misma para el esclarecimiento de la verdad en el país.

3.6. Diferencias entre indicio y evidencia digital

Las mismas fueron adoptadas en el Primer Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Celebrado en Ginebra, Suiza en 1955 y aprobadas por el Consejo Económico y Social de las Naciones Unidas en sus resoluciones 663C (XXIV) de 31 de julio de 1957 y 2076 (LXII) de 13 de mayo de 1977 y su objeto no es de describir en forma detallada un sistema penitenciario modelo, sino únicamente establecer, inspirándose en conceptos generalmente admitidos en nuestro tiempo y en los elementos esenciales de los sistemas contemporáneos más adecuados,

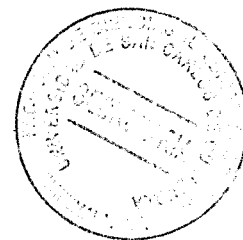


los principios y las reglas de una buena organización penitenciaria y de la práctica relativa al tratamiento de los reclusos.

Los criterios que se aplican a las materias a que se refieren estas reglas evolucionan constantemente. No tienden a excluir la posibilidad de experiencias y prácticas, siempre que éstas se ajusten a los principios y propósitos que se desprenden del texto de las reglas. Con ese espíritu, la administración penitenciaria central podrá siempre autorizar cualquier excepción a las reglas.

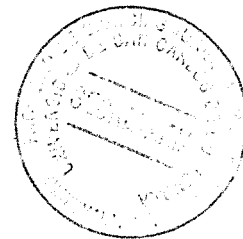
La primera parte de las reglas aborda lo relativo a la administración de los establecimientos penitenciarios y es aplicable a todas las categorías de reclusos en prisión preventiva o condenados, incluso a los que sean objeto de una medida de seguridad o de una medida de reeducación ordenada por el juez. En tanto que la segunda parte contiene las reglas que no son aplicables más que a las categorías de reclusos a que se refiere cada sección.

Sin embargo, las reglas de la sección A, aplicables a los reclusos condenados son igualmente aplicables a las categorías de reclusos a que se refieren las secciones B, C y D, siempre que no sean contradictorias con las reglas que las rigen y a condición de que sean provechosas para estos reclusos. Es de esta manera que estas reglas no están destinadas a determinar la organización de los establecimientos para delincuentes juveniles (establecimientos Borstal, instituciones de reeducación, etc.). No obstante, de un modo general, cabe considerar que la primera parte de las reglas mínimas es aplicable también a esos establecimientos.



Acorde con ello, la categoría de reclusos juveniles debe comprender, en todo caso, a los menores que dependen de las jurisdicciones de menores. Por lo general, no debería condenarse a los delincuentes juveniles a penas de prisión.

Las reglas en mención deben ser aplicadas imparcialmente. No se debe hacer diferencias de trato fundadas en prejuicios, principalmente de raza, color, sexo, lengua, religión, opinión política o cualquier otra opinión, de origen nacional o social, fortuna, nacimiento u otra situación cualquiera. Por el contrario, importa mucho respetar las creencias religiosas y los preceptos morales del grupo al que pertenezca el recluso.



CAPÍTULO IV

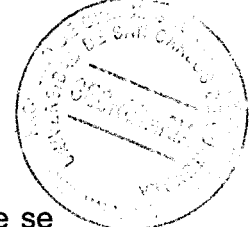
4. Incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos de origen cibernético

El presente capítulo se desglosa de forma breve y concisa los principales aspectos concernientes al incumplimiento del Estado ante la falta de protección y seguridad jurídica de la sociedad por delitos de origen cibernético, para lo cual se requiere abordar el propio concepto de protección y seguridad jurídica, los alcances y limitaciones de la investigación criminal en delitos cibernéticos, la vulnerabilidad de la sociedad por delitos de origen cibernético, las iniciativas del Estado para tipificar este tipo de delitos en el país y las perspectivas de la sociedad guatemalteca sobre estas conductas delictivas.

4.1. Conceptualización de la protección y seguridad jurídica

Sabido es que, a lo interno de los centros de privación de libertad, se localizan algunas estructuras de poder, que controlan los centros carcelarios del país, de esa cuenta múltiples son los factores que contribuyen a vulnerar los niveles de seguridad existentes, en ese contexto es necesario atender algunas consideraciones al respecto, para el efecto se presentan algunos planteamientos emitidos por autoridades internacionales que han experimentado con los diferentes niveles.

“El Buró Federal de Prisiones de Estados Unidos clasifica las prisiones de acuerdo a su nivel de seguridad, y la mayoría de las organizaciones penitenciarias estatales utilizan



las mismas categorías. Las seis categorías de seguridad reconocidas comúnmente se conocen como mínima, baja, media, alta, súper máxima seguridad y administrativa; cada tipo de prisión cuenta con prácticas de seguridad que están diseñadas para manejar de mejor manera al tipo de criminales encontrados dentro”.²⁵

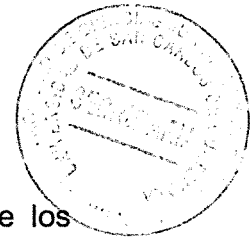
“Considerando que en la actualidad Guatemala se encuentra entre los 10 países con mayor hacinamiento a nivel mundial, el fenómeno de la sobrepoblación penitenciaria está presente en todo Centroamérica, pero no a niveles tan elevados como en Guatemala y en virtud que las características de la población reclusa en el país, tiende a mostrar un crecimiento rápido, resulta fundamental la implementación de un modelo que facilite y se adapte a los requerimientos de infraestructura encaminada a satisfacer los requerimientos de espacio físico.

En ese contexto y conociendo que el espacio utilizado para el efecto en el centro preventivo de la zona 18, como el de cumplimiento de condenas en Pavón Fraijanes, ya no dispone de capacidad para albergar a la población reclusa, bien puede pensarse en un tipo de construcción vertical que facilite el acceso a crear mayores espacios para la cantidad de reclusos y también porque el área donde se encuentra ha sido invadida por el crecimiento urbano de la población”.²⁶

Uno de los modelos de control que en la última década ha sido motivo de discusión es lo relativo a la implementación de brazaletes electrónicos, pues se estima que de

²⁵ http://www.ehowenespanol.com/tipos-seguridad-prisiones-info_463746/. (Consultado: 08 de enero de 2020).

²⁶ Centro de Investigaciones Económicas Nacionales (CIEN). **La prisión preventiva en Guatemala**. Pág. 3.

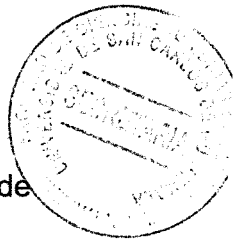


aplicarse en Guatemala, el Sistema Penitenciario y en todo caso cada uno de los centros de detención preventiva o de cumplimiento de condena debe identificar perfiles concretos, con bajo riesgo de reiteración en las actitudes criminales, en el entendido que este tipo de medidas de vigilancia evitan el ingreso en prisión, tanto de los internos en régimen ordinario como en régimen abierto y de infractores no peligrosos que no hayan cometido delitos graves.

Los brazaletes electrónicos se estiman que pueden facilitar también que se cumpla la condena en el entorno familiar y social, evitando la desestructuración familiar, de igual forma facilita, además, que el penado continúe su vida laboral y pueda atender así a la indemnización de la víctima.

El objetivo es evitar que la persona no sufra los efectos desocializadores del internamiento en prisión y en el caso de Guatemala, constituiría una buena alternativa, puesto que es de conocimiento popular los vejámenes que sufren los internos de nuevo ingreso por parte de los reclusos que llevan un periodo prolongado de tiempo en el lugar; esta circunstancia podría reducir los aspectos relativos al pago de la famosa talacha que se impone al recluso que recién ingresa tanto al preventivo de la zona 18, como al centro de cumplimiento de condenas en Pavón Fraijanes.

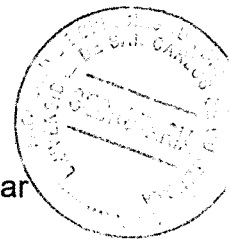
Ahora bien, es importante puntualizar sobre este apartado que para pensar en su aplicación, debe necesariamente contemplarse estos aspectos en una posible reforma no del Código Procesal Penal y tampoco del Decreto Número 33-2006 del Congreso de la República de Guatemala, Ley del Régimen Penitenciario, sino más bien al



reglamento de la ley, a pesar que el mismo se actualizó en el año 2017, a fin de readecuar el apartado correspondiente al régimen progresivo, a fin de impulsar la reeducación de los internos, siempre con respeto a la condena, efectuando por supuesto la salvedad que dicha concesión de las pulseras que funcionan a través de un sistema de posicionamiento global, está restringida y no debe realizarse en delitos dolosos o relacionados con violencia de género, toda vez que los mismos no son susceptibles de que puedan optar a una medida sustitutiva con facilidad.

La implementación de un sistema como tal, implicaría un costo bastante elevado, en virtud que son pocas las empresas que prestan el servicio de localización en el país, en ese sentido, sería más oneroso el costo de mantenimiento que el de adquisición, esto de acuerdo a información obtenida directamente de funcionarios del Sistema Penitenciario; de esta manera se pudo determinar de acuerdo a experiencia en el rubro de vehículos que el costo que presenta la empresa Lo Jack Detektor, es de un estimado en Q.800.00 mensuales por cada uno de los dispositivos activos.

Esta situación hace pensar que puede ser el propio Sistema Penitenciario quien disponga de los equipos de monitoreo, rastreo y ubicación de los dispositivos utilizados, tanto para evitar alguna posible fuga de información como la manipulación de los equipos tecnológicos al encontrarse en poder de empresas privadas; de esa cuenta puede minimizarse el costo de mantenimiento y se dispondría del control total de la información sensible que pertenezca y puede ser utilizada únicamente por personeros del Sistema Penitenciario del país; ante esta situación, los jueces o inspectores en todo



caso, encargados de verificar el cumplimiento de las penas, únicamente deben guardar el registro o monitoreo de estos dispositivos, pues su efectividad sería plena.

Otra de las debilidades que merecen destacarse, es lo concerniente a que la parte final del proceso penal guatemalteco se completa con una sentencia para que entre a la jurisdicción de un Juez de Ejecución Penal, debe necesariamente ser condenatoria, ya sea que imponga una pena de muerte, de prisión, de multa, aplicación de una medida de seguridad o las penas accesorias.

Este aspecto debe condenarse de alguna manera, excluyéndose de la jurisdicción del Juez de Ejecución Penal, lo relativo a la condena en costas procesales, pues de conformidad con el Artículo 45 del Código Procesal Penal, corresponde dicha función al Juez de Primera Instancia. Por otro lado, existen decisiones que el Juez de Ejecución Penal muchas veces desconoce, pues la Dirección General del Sistema Penitenciario, traslada de un reo de un centro preventivo a otro, o el traslado de un reo hacia un centro asistencial, sin el consentimiento del juez.

4.2. Alcances y limitaciones de la investigación criminal en delitos cibernéticos

Dentro de los principales aspectos que merecen destacarse en el presente apartado, se encuentra lo relativo a las deficiencias presupuestales y la falta de voluntad política de las autoridades y principalmente de las compañías telefónicas, en tal sentido se estima que las deficiencias jurídicas son las que por ende propician las deficiencias administrativas y desde entonces el fenómeno delictivo desde los centros de detención

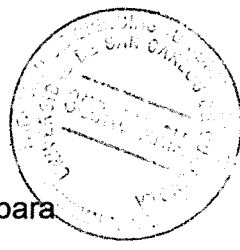


ha ido incrementándose gradualmente, sin que hasta la fecha se presenten soluciones de fondo, más que solo el ofrecimiento de los operadores de entregar los equipos bloqueadores a las autoridades para que estos se encarguen de su administración.

En ese sentido, aun cuando efectivamente se han hecho entrega de estos dispositivos al sistema penitenciario, incluso se tiene conocimiento a través de los medios de comunicación que son los propios agentes del sistema en mención, quienes sabotean las antenas y efectúan cortes de energía para interrumpir su funcionamiento, obedeciendo esto al fenómeno generalizado de la corrupción tan arraigado en las cárceles guatemaltecas.

Es de esta manera que se estima por consiguiente que las deficiencias administrativas, son de fondo pues aunque se cuente con una ley en la materia, tanto privados de libertad como los propios custodios y otras autoridades carcelarias, buscarán como evadir sus controles y por el pago de una cuota, buscarán como alterar los equipos y que los reclusos puedan efectuar sus comunicaciones desde los centros.

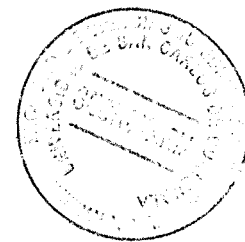
En ese sentido, es preciso señalar que otro de los aspectos a tomar en cuenta es el hecho de que a raíz de ese fenómeno de corrupción, si funcionaran con precisión estos bloqueadores, no se alentara por consiguiente el ingreso de todo tipo de terminales móviles a los centros de detención, pues al saber que no podrían comunicarse, que sentido tendría ingresar estos aparatos si se sabría que serían infructuosos los propósitos de entablar una comunicación efectiva.



Por lo tanto, estos aspectos son los que deben tomarse en consideración para comprender con precisión, por qué hasta la actualidad siguen generándose todo tipo de comunicaciones desde estos centros de detención y las autoridades parecen hacer poco por limitar, mitigar o contrarrestar este fenómeno, pues en ese proceso, muchos salen beneficiados, desde los propios reclusos, pasando por las autoridades carcelarias, hasta las empresas de telefonía, que saben de los ingresos considerables que perciben por la utilización de estos equipos en las cárceles del país.

Es de esta manera como en la Ley de Equipos Terminales Móviles se estableció que la Superintendencia de Telecomunicaciones, debe inscribir a los importadores, exportadores, distribuidores, vendedores y comercializadores de celulares detallando la actividad que realizan; sin embargo esta entidad no cuenta con la capacidad humana de administrar a los miles de comercializadores de terminales móviles en el país.

Todos estos aspectos influyen considerablemente para que en las requisas que esporádicamente se realizan en los 21 centros de privación de libertad del país, se han encontrado diversidad de objetos ilícitos, entre ellos teléfonos satelitales, los cuales les sirven a las organizaciones criminales, ya que no son susceptibles a las antenas bloqueadoras de celulares y con ello pueden mantener sus comunicaciones constantemente, con ello solo se refleja la serie de inconsistencias en materia institucional para contrarrestar la amplia recurrencia que se genera en torno a la utilización de equipos telefónicos en los recintos carcelarios del país.



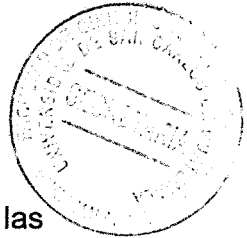
4.3. Vulnerabilidad de la sociedad por delitos de origen cibernético

Para lograr un mayor control adentro de los centros carcelarios hace falta reforzar las unidades de control interno, especialmente la Inspectoría. La misma debe contar con suficiente personal debidamente calificado, un reglamento y manual adecuado y suficiente seguridad al realizar sus inspecciones. Para garantizar la independencia de la Inspectoría se sugiere, entre otros, cambios en el proceso de nombramiento del Inspector. La reglamentación de los procedimientos operativos y la aplicación sistemática del régimen disciplinario para los privados de libertad serán claves para alcanzar mayor orden y control en los centros carcelarios.

Respecto a la rehabilitación social de los privados de libertad se necesita que la atención por parte de los profesionales sea integral y suficiente. Queda el desafío de proponer condiciones adecuadas para poder brindar esta ayuda a los privados de libertad. En el tema de los programas laborales es necesario una reorganización de dichos programas que permite mayor sistematización y control de las actividades, así como evaluar e implementar modelos novedosos y creativos mediante la tercerización de estos servicios.

a) “Ausencia de condiciones para la implementación de ley de régimen penitenciario

El sistema penitenciario no cuenta aún con las condiciones mínimas para poder desarrollar el régimen progresivo y de carrera establecidos en la ley, así mismo



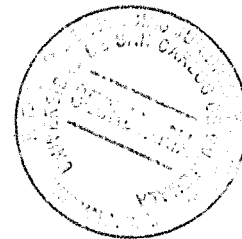
actualmente los centros requieren de una infraestructura acorde a desarrollar las actividades propias de las fases de tratamiento del régimen progresivo. Además, no hay coordinación entre los operadores de justicia para desarrollar el rol que le otorga la ley de régimen penitenciario a cada quien.

b) Hacinamiento

Los centros penales de cumplimiento de condena reflejan a un 54% de sobrepoblación y los centros de prisión preventiva a un 52%, esto tiene relación directa con la carencia de infraestructura y con uso irracional de la prisión preventiva por operadores del sistema de justicia y con captura ilegales y masivas de personas por presuntos delitos de posesión para el consumo y faltas.

c) Precariedad de servicios básicos

El 93% de los centros plantea escasez de agua potable, la disponibilidad de servicios de agua (chorros) por persona, tiene un promedio general de un servicio para 57.4 personas; en cuanto a servicios sanitarios, estos son escasos y limitada disponibilidad, en promedio hay disponible un servicio sanitario para 32.2 personas; la alimentación es de mala calidad e insuficiente; en el 56% de los centros no existe servicio telefónico. Existe escasa cobertura de los servicios médicos, el 56% de los centros no cuenta con médico ni paramédico; sólo hay disponible médico, 2 a 3 días a la semana su horario de trabajo nominal no supera las 4 horas a la semana.



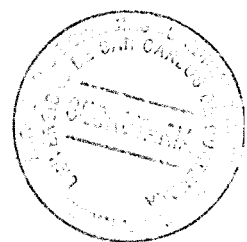
d) Malos tratos en contra de la población vulnerable

Principalmente de la de enfermos mentales, mujeres, indígenas, personas miembros de pandillas. En 2006 se documentaron 49 casos de tortura en 5 centros de prisión preventiva de hombres y mujeres y 42 casos de malos tratos en los mismos 5 centros de prisión preventiva.

El caso del mal trato a mujeres es grave, a las mujeres procesadas no se les permite ejercer su derecho a la visita conyugal, en las cárceles a cargo de la PNC, sufren de acoso sexual por parte de los agentes. No obstante que el 24% de la población privada de libertad es indígena, en las cárceles la mayoría de personal sólo habla español, asimismo la mayoría de personas indígenas son obligadas a realizar las labores de limpieza para sobrevivir.

La mayoría de integrantes de pandillas, está reclusa en un régimen más restrictivo y en condiciones más precarias, generalmente no se les permite el ingreso de comida, libros, periódicos; no se le proporciona camas, no se les proporciona atención médica adecuada, no obstante, la mayoría padece enfermedades de la piel (sarcopiosis) están hacinados la mayoría con un espacio para dormir de 0.32 metros cuadrados.

La situación de estos grupos se agrava considerablemente si se toma en cuenta que el acceso a mecanismos de solicitudes o quejas, es limitado y arbitrario, ya que son los mismos encargados quienes autorizan la presentación de solicitudes o queja ante las autoridades de la cárcel.



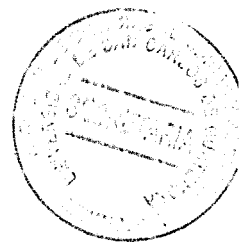
e) Corrupción

El principal instrumento de corrupción es la ubicación en sectores, éste es conforme el cupo y la capacidad económica de la persona que ingresa, el otro mecanismo es el cobro para ingreso de objetos y sustancias prohibidas.

En conclusión, las condiciones de las personas privadas de libertad continúan siendo precarias por la carencia de infraestructura y servicios básicos mínimos, son frecuentes los malos tratos y posibles hechos de tortura principalmente provenientes de las mismas personas privadas de libertad con aquiescencia de las autoridades y por parte de las mismas autoridades, principalmente en cárceles a cargo de la Policía Nacional Civil. Ante esta situación el control interno y externo de las cárceles es débil por la falta de recursos humanos y financieros”.²⁷

Como puede notarse, estos son los principales factores que inciden en las deficiencias del control operacional en las cárceles del país, aspecto que ha estado vigente hasta la actualidad y que de ninguna manera ha podido contrarrestarse, a pesar de los diversos intentos por mitigar la incidencia que tiene esta falta de control, sobre todo en la planificación de diversos delitos, tales como extorsiones, obstrucciones extorsivas de tránsito, exacciones intimidatorias, pasando hasta el asesinato, homicidio, femicidio, entre otros aspectos que merecen destacarse.

²⁷ Ibid.

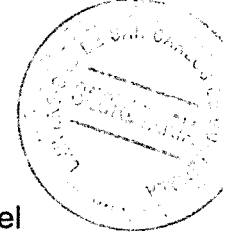


4.4. Iniciativas del Estado para tipificar los delitos cibernéticos en Guatemala

Históricamente las cárceles han funcionado como centros retributivos que lejos de reeducar y por ende resocializar al individuo, tal como lo preceptúa la Constitución Política de la República de Guatemala, se considera que en gran medida reproducen las injusticias de la estructura económica y en nada cumplen los estándares internacionales y nacionales de la buena práctica penitenciaria, por consiguiente se considera que en el caso de la República de Guatemala, existen evidentes dificultades para garantizar el espíritu del régimen progresivo vigente en el país.

Consciente de esta gama de limitaciones, debe sumarse también la violencia, la corrupción, el control disciplinario en poder de los reclusos en las cárceles, han generado arbitrariedades y, en el incumplimiento del fin constitucional de la readaptación social y la reeducación de los reclusos, pero sobre todo en nada han contribuido a la resolución de la conflictividad social. Pero existen otros problemas estructurales como la falta de aplicación de la ley ya existente, la poca asignación presupuestaria, la falta de una carrera penitenciaria y la falta de auditoria social.

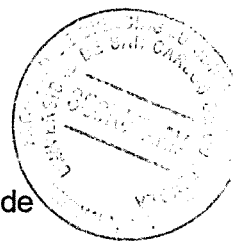
A pesar de que el Estado cuenta con suficiente información sobre el funcionamiento del Sistema Penitenciario proporcionada por las instituciones ya mencionadas, la situación actual de las cárceles públicas del sistema penitenciario no ha cambiado y lejos de ello, el margen de delitos que se siguen produciendo desde estos centros de detención, parece no detenerse.



De acuerdo con este planteamiento, puede complementarse con el hecho que, el Sistema Penitenciario guatemalteco, como conjunto de instituciones a cargo de la administración de los centros penales y la reinserción social de los internos, hasta el seis de octubre de 2006, careció durante décadas, de una ley específica que regulara su función, las normas aplicadas para el tratamiento de los reclusos, se encontraban dispersas en varias leyes penales y, las instituciones que lo conforman aún dependen fundamentalmente del Ministerio de Gobernación; el Decreto 33-2006 del Congreso de la República, Ley del Régimen Penitenciario agrupó las leyes dispersas y luego el Ministerio de Gobernación desarrolló el reglamento correspondiente en el año 2011 y que luego se actualizó con el Acuerdo Número 195-2017, precisamente en el 2017.

Como consecuencia de estas consideraciones, el sistema penitenciario depende administrativa, operativa y económicamente del Ministerio de Gobernación, existe una evidente ausencia de recursos suficientes que le permitan una mejor administración de los centros penales, la falta de recursos no permite la ampliación de la infraestructura en los espacios disponibles de los centros, observándose que los mismos internos paulatinamente han invadido estos espacios con construcciones anti-técnicas y caprichosas, que en nada benefician a los centros penales.

En ese sentido, es importante puntualizar que en esencia este fenómeno es fácilmente observable en centros de cumplimiento de condena como por ejemplo la Granja Modelo de Rehabilitación Pavón previo a la ocupación por parte de las autoridades, además la falta de recursos, tampoco permite la construcción de nuevas edificaciones, la compra de equipo tecnológico apropiado para la seguridad de los centros, la omisión de



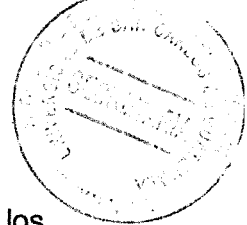
personal calificado que como equipo multidisciplinario determine el régimen de inserción aplicable acorde al tipo de reclusos de los centros penales.

Con todos estos aspectos se estima que existe una notable limitación para el desarrollo del régimen en mención en el país, dando pie a que el mismo no resulte ser efectivo, pero a criterio personal se estima que no es que el sistema progresivo sea fallido, sino que más bien son los mecanismos jurídicos y administrativos para su implementación, los que limitan su efectividad y es precisamente este aspecto el que se abordará en el siguiente numeral del presente trabajo de graduación.

La posibilidad de garantizar condiciones de seguridad que faciliten la convivencia, y la ejecución de un programa de tratamiento para la rehabilitación de la población reclusa, depende en gran medida de la disponibilidad y calidad de las instalaciones físicas con que se cuente y, del equipamiento que permita el cumplimiento de cada una de las competencias, que con ese propósito deban ejecutar los operadores del sistema.

Los agentes penitenciarios que realizan la revisión del ingreso de los visitantes no cuentan con supervisión continua y con procedimientos definidos con claridad, por lo que las autoridades no pueden establecer cómo realizan su trabajo. Además, la falta de control interno no permite identificar alguna desviación administrativa de las funciones de los agentes penitenciarios, que pueden constituir delitos.

Toda esta gama de dificultades, influye determinadamente en que los privados de libertad, operen abiertamente dentro de los recintos carcelarios, dedicándose con

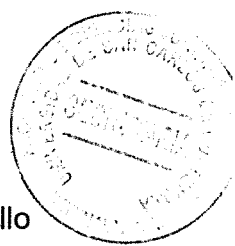


exclusividad a la planificación y logística para efectuar o cometer diversos delitos, en los cuales se utilizan equipos terminales móviles y como se señaló con anterioridad, es esta práctica recurrente y que parece no detenerse, la que afecta notoriamente el patrimonio de las personas, pues el sistema penitenciario guatemalteco, carece de mecanismos efectivos de control para contrarrestar el ingreso de estos equipos terminales a los diferentes centros de detención en la República de Guatemala.

4.5. Perspectivas de la sociedad guatemalteca sobre los delitos cibernéticos

La práctica común en los centros carcelarios es la comisión de diversos ilícitos, entre los que se destacan principalmente las extorsiones, obstrucción extorsiva de tránsito y exacciones intimidatorias, para lo cual se utilizan como mecanismo de comisión, los equipos terminales móviles, es decir toda clase de aparatos celulares que pese a la prohibición de ingreso a los mismos, continúan utilizando aberrantemente en los mismos, sin que hasta la fecha se disponga de un mecanismo de control efectivo para limitar la práctica recurrente de ingreso de estos equipos a los diferentes centros de detención del país, tal como lo preceptúa el Artículo 27 del Decreto Número 8-2013 del Congreso de la República de Guatemala, Ley de Equipos de Terminales Móviles, todo ello a pesar que como se indicó se contempla una pena de prisión de 6 a 10 años.

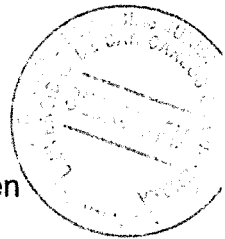
Acorde con ello, las autoridades del sistema penitenciario deben priorizar la implementación entre otros aspectos, de unidades caninas y cámaras de video que en conjunto a los arcos detectores de rayos x, todo ello con la finalidad específica de que se pueda detectar ampliamente el ingreso de estos equipos y efectuar las detenciones



correspondientes que desmotiven a las personas a ingresar estos dispositivos y con ello reducir la incidencia del fenómeno extorsivo desde los centros carcelarios del país.

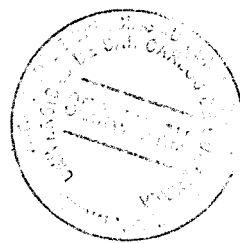
A raíz de la serie de limitaciones jurídicas e institucionales que prevalecen en los centros de detención de la República de Guatemala y de los que se ha hecho referencia en este capítulo, se estima que como un efecto inmediato del ingreso de estos equipos terminales móviles, se tiene el aumento paulatino e incidencia de las extorsiones y obstrucciones extorsivas efectuadas desde los centros carcelarios en el país; en ese contexto se estima que la problemática de fondo radica en las diversas argucias utilizadas por familiares y amistades de los detenidos para ingresar estos equipos a los centros de detención.

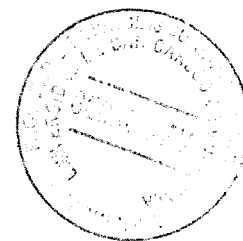
A esta serie de elementos debe sumarse la estrecha colaboración de funcionarios o agentes del sistema penitenciario que solicitan o aceptan a cambio de una retribución económica (cohecho pasivo o activo), el ingreso de todo tipo de dispositivos a los centros de detención, aun cuando dentro del Artículo 27 del Decreto Número 8-2013 del Congreso de la República de Guatemala, Ley de Equipos de Terminales Móviles, se tipifica con precisión el delito y la pena correspondiente para quienes ingresen equipos terminales móviles y/o sus componentes o cualquier equipo electrónico que sirva para comunicaciones, por algún motivo o por visita a un recluso o interno de un centro de privación de libertad o centro penitenciario, ya sean estos preventivos o de cumplimiento de condena.



Atendiendo estos preceptos, se considera que lejos ha quedado esta posibilidad, en virtud que constantemente las autoridades, principalmente de la Policía Nacional Civil, Ministerio Público y Sistema Penitenciario, a través de requisas e incautaciones efectuadas en estos recintos, localizan gran cantidad de dispositivos que evidentemente son utilizados para efectuar requerimientos extorsivos, amenazas e intimidaciones, pues así se ha demostrado en diversos casos o expedientes que la fiscalía correspondiente tiene a bien exponer y que son de conocimiento de la población a través de los medios de comunicación.

Estos factores vienen a generar la problemática, misma que parece no detenerse hasta que existe un marco normativo específico que permita contrarrestar el uso frecuente de todo tipo de dispositivos electrónicos que promueven las actividades delictivas en el país y que tienen como gran parte de las víctimas a la población trabajadora del país, sin que hasta la fecha se haya encontrado una salida viable y eficiente para limitar y/o contrarrestar todo tipo de actividades delictivas que se gestan desde las cárceles en el país y que únicamente dejan de manifiesto las limitaciones del aparato estatal para el cumplimiento de los verdaderos fines del régimen penitenciario, acorde con lo preceptuado en la propia Constitución Política de la República de Guatemala.



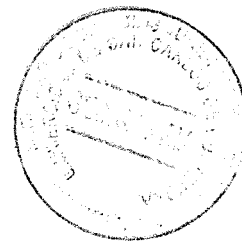


CONCLUSIÓN DISCURSIVA

El sistema penitenciario guatemalteco, durante décadas ha afrontado notables deficiencias para su administración eficiente y eficaz, circunstancia que se pensó que se revertiría con la aprobación del Decreto Número 33-2006 del Congreso de la República de Guatemala, Ley del Régimen Penitenciario y aunque fue un avance sustantivo en la materia, han aflorado nuevas formas delictivas que se originan precisamente desde los centros carcelarios del país, reflejando la carencia de una política integral para su gestión integral y que hasta el desarrollo de la investigación, continúa manifestando un alto grado de incidencia en cuanto a los delitos como extorsión y la conspiración extorsivas de tránsito que parecen no detenerse.

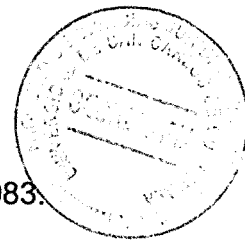
Derivado de esta serie de consideraciones, se estima que el incumplimiento pleno de la Ley y su respectivo reglamento, son los que han propiciado la falta de control administrativo y operacional en la totalidad de los centros carcelarios del país, circunstancia que paulatinamente ha ido agudizando la situación penitenciaria del país, de tal manera que continúa teniendo una alta incidencia criminal en la sociedad.

Es en este contexto que el Ministerio de Gobernación a través del Sistema Penitenciarios debe atender y llevar a cabo la ubicación y distribución de los reclusos o reclusas como lo establece la Ley en la materia, para una efectiva ejecución de las penas, debiendo ser uno de sus fines principales el de organizar a las personas reclusas bajo políticas objetivas que denoten el cumplimiento literal de dicha ley, efectuando una pre-evaluación para su ubicación y cumplimiento de la pena respectiva.



BIBLIOGRAFÍA

- AMBROCIO ABAC, Ana Victoria. **Efectos de la no clasificación de los reos en el centro preventivo.** Tesis Universidad Rafael Landívar de Guatemala. Facultad de Ciencias Jurídicas y Sociales. Quetzaltenango, Guatemala. 2014.
- BARROS LEAL, Cesar. **La prisión desde una perspectiva histórica y el desafío actual de los derechos humanos de los reclusos.** Instituto Interamericano de Derechos Humanos. Serie: Estudios de Derechos Humanos. Tomo II. San José, Costa Rica. 2007.
- BERDUGO, Ignacio y Laura Zuñiga. **Manual de derecho penitenciario.** Madrid. España. Ed. Colex. 2001.
- CABANELLAS, Guillermo. **Diccionario de derecho usual.** Tomo III. Buenos Aires, Argentina. Ed. Heliasta, 2001.
- Centro de Investigaciones Económicas Nacionales. **El sistema penitenciario guatemalteco, un diagnóstico.** Lineamientos de Política Económica, Social y de Seguridad 2012-2020. Guatemala 2011.
- CUELLO CALÓN, Eugenio. **Derecho penal. Parte general.** Tomo I. Barcelona, España. 18ª. ed. Ed. Bosch, 1989.
- CUELLO CALÓN, Eugenio. **La moderna penología: represión del delito y tratamiento de los delincuentes; penas y medidas, su ejecución.** Madrid, España. Ed. Bosch, 2001.
- DE LEÓN VELASCO, Héctor Aníbal y José Francisco De Mata Vela. **Derecho penal guatemalteco. Parte general y parte específica.** 22ª. ed. Ed. Magna Terra. Guatemala, 2010.
- DEL PONT, Luis Marco. **Derecho penitenciario.** 2ª. ed., México D.F. Ed. De Palma. 2005.
- FLORES GÓMEZ GONZÁLEZ, Fernando y Gustavo Carvajal Moreno. **Nociones de derecho positivo mexicano.** 25ª. ed. México D.F. Ed. Porrúa, 1986.
- GARCÍA VERDUGO, Alejandro. **El derecho penitenciario.** Tesis Universidad Rafael Landívar. Facultad de Ciencias Jurídicas y Sociales. Guatemala, 2016.
- GARCÍA VALDÉS, Carlos. **Historia de la prisión: teorías economicistas, crítica.** Ed. Edisofer. España. 1997.
- GARCÍA RAMÍREZ, Sergio. **La prisión.** México D.F. Ed. Instituto de Investigaciones Jurídicas de la universidad Nacional Autónoma de México, 1975.



GARRIDO, Luis. **Manual de ciencia penitenciaria**. Madrid, España. Ed. Edersa, 1983.

<http://hablemosdederechopenitenciario.blogspot.com/2014/11/historia-de-los-sistemas-penitenciarios.html>. (Consultado: 18 de enero de 2020).

http://www.ehowenespanol.com/tipos-seguridad-prisiones-info_463746/. (Consultado: 08 de enero de 2020).

LAHURA OLIVO, Marino. **Derecho penitenciario y ejecución penal en Perú**. Lima, Perú. Ed. La Cotera, 1982.

MENDOZA, BREMAUNTZ, Emma. **Derecho penitenciario**. México D.F. Ed. McGraw Hill, 1998.

OSSORIO Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. 28ª. ed. Buenos Aires, Argentina. Ed. Heliasta, 2001.

PEREZNIETO Y CASTRO Leonel, Abel Ledewsma Mondragón. **Introducción al estudio del derecho**. 2ª. ed. Madrid, España. Ed. Harla, 1992.

TÉLLEZ AGUILERA, Abel. **Revista de estudios penitenciarios: una aproximación a los orígenes y al concepto de derecho penitenciario**. Madrid, España. Ed. Secretaría General de Instituciones Penitenciarias, 2011.

VILLADIEGO GÓMEZ, Ángela Patricia. **Breviario histórico del derecho penitenciario y carcelario universal**. Revista virtual Legem. Barranquilla Colombia, 2013.

WELCH REYES, Yeiysson Roberto. **La reeducación y reinserción del recluso en Centroamérica**. Tesis Universidad Rafael Landívar. Facultad de Ciencias Jurídicas y Sociales. Quetzaltenango, Guatemala 2014.

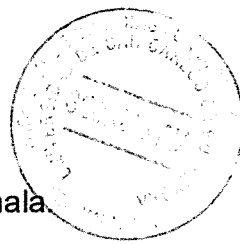
Legislación:

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

Declaración Universal de los Derechos Humanos. Organización de las Naciones Unidas. -ONU-. Nueva York, 1948.

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

Ley del Régimen Penitenciario. Congreso de la República de Guatemala. Decreto 33-2006.



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

Ley del Organismo Ejecutivo. Decreto Número 114-97 del Congreso de la República de Guatemala. Guatemala. 1994.

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