UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DEL NORTE
CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, ABOGADO Y NOTARIO

TRABAJO DE GRADUACIÓN

TESIS
ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA

ROSA IVONNE ESCOBEDO SOMOSA

COBÁN, ALTA VERAPAZ, MAYO DE 2 016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DEL NORTE
CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, ABOGADO Y NOTARIO

TRABAJO DE GRADUACIÓN

TESIS
ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA

PRESENTADA AL HONORABLE CONSEJO DIRECTIVO DEL CENTRO UNIVERSITARIO DEL NORTE

POR

ROSA IVONNE ESCOBEDO SOMOSA
CARNÉ 9316762

COMO REQUISITO PREVIO A OPTAR AL GRADO ACADÉMICO DE LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

COBÁN, ALTA VERAPAZ, MAYO DE 2 016

AUTORIDADES UNIVERSITARIAS

RECTOR MAGNÍFICO

Dr. Carlos Guillermo Alvarado Cerezo

CONSEJO DIRECTIVO

PRESIDENTE:	Lic. Zoot. Erwin Gonzalo Eskenasy Morales
SECRETARIA:	Licda.T.S. Floricelda Chiquin Yoj
REPRESENTANTE DOCENTES:	Ing. Geol. César Fernando Monterroso Rey
REPRESENTANTE EGRESADOS:	Lic. admón. Fredy Fernando Lemus Morales
REPRESENTANTE ESTUDIANTES:	Br. Fredy Enrique Gereda Milian
	PEM. César Oswaldo Bol Cú

COORDINADOR ACADÉMICO

Lic. Zoot. Erwin Fernando Monterroso Trujillo

COORDINADOR DE LA CARRERA

Lic. Jorge Gustavo Meza Ordoñez

COMISIÓN DE TRABAJOS DE GRADUACIÓN

COORDINADOR:	Msc. Mario de Jesús Estrada Iglesias
SECRETARIO:	Licda. Vasthi Alelí Reyes Laparra
VOCAL I:	Dr. Álvaro Enrique Sontay Ical
VOCAL II:	Msc. José Gerardo Molina Muñoz

REVISORA DE REDACCIÓN Y ESTILO

Licda. Aura Violeta Rey Yalibat

REVISOR DE TRABAJOS DE GRADUACIÓN

Lic. Oscar Roberto Rosales Gómez

ASESORA

Licda. Carla Liliana Chacón Monterrozo

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DEL NORTE

Cobán, Alta Verapaz, 30 de junio de 2 015.

SEÑORES:
MIEMBROS DE LA COMISIÓN DE TRABAJOS DE GRADUACIÓN
CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES
ABOGADO Y NOTARIO
CENTRO UNIVERSITARIO DEL NORTE -CUNOR-
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.

Respetable Comisión:

Atendiendo al nombramiento de fecha diecinueve de mayo del año dos mil quince, emitido por la honorable comisión en el cual se me nombra como Asesora del informe final de trabajo de graduación de la Bachiller Rosa Ivonne Escobedo Somosa, carné 9316762 y quien elaboró el trabajo de tesis intitulado **" ANALISIS JURIDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA"** me es grato informarles lo siguiente:

Luego del análisis realizado al trabajo de tesis, he podido determinar que cumple con los lineamientos, métodos y técnicas de investigación; así mismo, la secuencia de los capítulos conjuntamente con la redacción y estilo hace fácil la comprensión del tema. La contribución científica queda plasmada en las conclusiones y recomendaciones las cuales se enfocan desde un punto de vista doctrinario y legal; así mismo la bibliografía es acorde y se relaciona con el contenido de la tesis.

Después de reunirme con la bachiller Escobedo Somosa, le sugerí algunas correcciones a los capítulos, siempre bajo el respeto de su posición ideológica y la sustentante estuvo de acuerdo en llevar a cabo las modificaciones. Los objetivos se alcanzaron; las técnicas mayormente utilizadas fueron la bibliográfica, encuestas y la documental, las cuales contribuyeron a obtener el material suficiente y actual para el desarrollo de la tesis.

Por lo que al haber completado satisfactoriamente la etápa de Asesoría del trabajo de tesis, verificando que el mismo reúne los requisitos de carácter legal y los que exige esa casa de estudios, me permito emitir DICTAMEN FAVORABLE, para su posterior evaluación por el tribunal examinador, previo a optar al grado académico de Licenciatura en Ciencias Jurídicas y Sociales.

Sin otro particular me suscribo de ustedes,

Deferentemente:

Licda. Carla Liliana Chacón Monterrozo
Colegiado NO. 3338

Carla Liliana Chacón Monterrozo
ABOGADO Y NOTARIO

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DEL NORTE

Cobán, Alta Verapaz, 6 de Octubre de 2015.

SEÑORES:
MIEMBROS DE LA COMISIÓN DE TRABAJOS DE GRADUACIÓN
CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES
ABOGADO Y NOTARIO
CENTRO UNIVERSITARIO DEL NORTE -CUNOR-
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.

Respetable Comisión:

Atendiendo al nombramiento de fecha 28 de julio del año dos mil quince, emitido por la honorable comisión en el cual se me nombra como **Revisor** del informe final de trabajo de graduación de la bachiller Rosa Ivonne Escobedo Somosa, carné 9316762 y quien elaboró el trabajo de tesis intitulado **"ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA"** me es grato informarles lo siguiente:

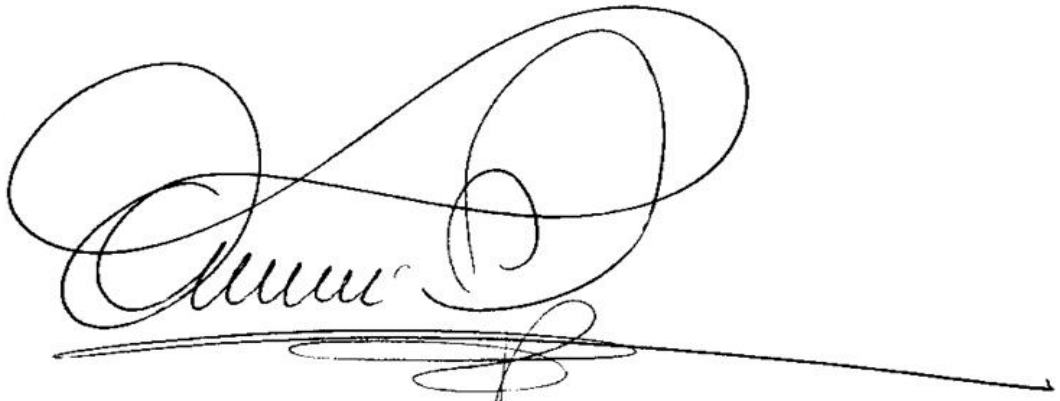
Luego de las modificaciones pertinentes realizadas al trabajo de tesis, he podido determinar que cumple con los lineamientos, métodos y técnicas de investigaciones; así mismo, la secuencia de los capítulos conjuntamente con la redacción y estilo hace fácil la comprensión del tema. La contribución científica queda plasmada en las respectivas conclusiones y recomendaciones, las cuales se enfocan desde un punto de vista doctrinario y legal; así mismo, la bibliografía es acorde y se relaciona con el contenido de la tesis.

Después de reunirme con la bachiller Escobedo Somosa, le sugerí algunas correcciones a los capítulos, siempre bajo el respeto de su posición ideológica y la sustentante estuvo de acuerdo en llevar a cabo las modificaciones. Los objetivos se alcanzaron.

Por lo que al haber completado satisfactoriamente la etapa de Revisión del trabajo de tesis, verificando que el mismo reúne los requisitos de carácter legal y los que exige esa casa de estudios, me permito emitir **DICTAMEN FAVORABLE**, para su posterior evaluación por el tribunal examinador, previo a optar al grado académico de Licenciatura en Ciencias Jurídicas y Sociales.

Sin otro particular me suscribo de ustedes,

Deferentemente:



Licenciado Oscar Roberto Rosales Gómez
Colegiado No. 7,369

Oscar Roberto Rosales Gómez
ABOGADO Y NOTARIO

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DEL NORTE

ENCARGADA DE REDACCIÓN Y ESTILO DE LA COMISIÓN DE TRABAJOS DE GRADUACIÓN DE LA CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, ABOGADO Y NOTARIO, DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, CENTRO UNIVERSITARIO DEL NORTE (CUNOR). Cobán, Alta Verapaz, uno de Abril del dos mil dieciséis.----------

I) Con fundamento en las atribuciones que me fueron otorgadas en sesión ordinaria del Honorable Consejo Directivo del Centro Universitario del Norte –CUNOR- de la Universidad de San Carlos de Guatemala, nombrándome como titular, encargada de la Redacción y Estilo, se ha procedido a la revisión del formato de impresión, bibliografía, redacción y ortografía del Trabajo de Graduación titulado: **"ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA"** de la estudiante **ROSA IVONNE ESCOBEDO SOMOSA** con carné número 9316762; **II)** CONSIDERANDO: Que después del análisis y revisión pertinente, se ha cumplido con los requisitos establecidos en el Normativo General de Trabajos de Graduación para las carreras a nivel de grado del Centro Universitario del Norte – CUNOR - y demás disposiciones aplicables, a mi juicio y a las normas de redacción y estilo, el trabajo de graduación es satisfactorio. En virtud de lo anterior, se emite **DICTAMEN FAVORABLE** del trabajo de graduación relacionado.----------

Id y Enseñad a Todos

Licda. Aura Violeta Rey Yalibat
Encargada de Redacción y Estilo

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DEL NORTE

COMISIÓN DE TRABAJOS DE GRADUACIÓN DE LA CARRERA DE LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, ABOGADO Y NOTARIO, DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, CENTRO UNIVERSITARIO DEL NORTE (CUNOR). Cobán, Alta Verapaz, veinticinco de abril del año dos mil dieciséis. **I)** Se tiene como analizado el expediente de la estudiante ROSA IVONNE ESCOBEDO SOMOSA, con carné número 9316762 y por recibidos los dictámenes favorables de asesor, revisor y encargado de redacción y estilo del trabajo de graduación intitulado **"ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA"** y comprobándose haber cumplido con los requerimientos establecidos en el Normativo General de Trabajos de Graduación para las carreras a nivel de grado del Centro Universitario del Norte –CUNOR- y demás disposiciones aplicables, esta Comisión en forma colegiada, **DA VISTO BUENO** al trabajo de graduación referido; **II)** Remítase a la Dirección del Centro Universitario del Norte para que se emita la orden de impresión respectiva; **III)** Notifíquese.

Msc. Mario de Jesús Estrada Iglesias
Coordinador

Licda. Vasthi Aleli Reyes Laparra
Secretaria

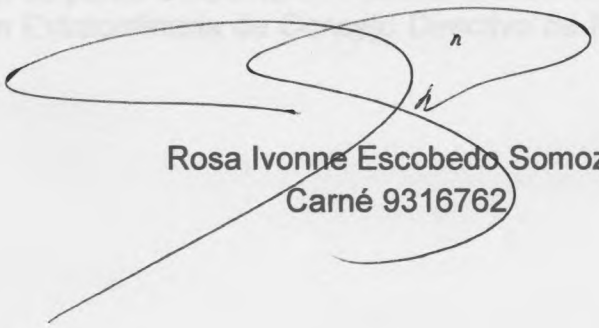
Dr. Álvaro Enrique Sontay Ical
Vocal I

Msc. José Gerardo Molina Muñoz
Vocal II

Comisión Trabajos de Graduación
USAC - CUNOR
Ciencias Jurídicas y Sociales

HONORABLE COMITÉ EXAMINADOR

En cumplimiento a lo establecido por los estatutos de la Universidad de San Carlos de Guatemala, presento a consideración de ustedes el trabajo de graduación titulado: "**Análisis Jurídico del Fraude Cibernético en Guatemala**", como requisito previo a optar al grado académico de Licenciada en Ciencias Jurídicas y Sociales.



Rosa Ivonne Escobedo Somoza
Carné 9316762

RESPONSABILIDAD

“La responsabilidad del contenido de los trabajos de graduación es: Del estudiante que opta al título, del asesor y del revisor; la Comisión de Redacción y Estilo de cada carrera, es la responsable de la estructura y la forma”.

Aprobado en su punto SEGUNDO, inciso 2.4, subinciso 2.4.1 del Acta No. 17-2 012 de Sesión Extraordinaria de Consejo Directivo de fecha 18 de julio del año 2 012.

DEDICATORIA
A:

Dios:

Por ser parte esencial en mi vida, y por todas las bendiciones recibidas, infinitas gracias.

Mis padres:

María Luz y Oscar Rolando Morales.

Mis hijas:

Ligia y Diana, por el ánimo inyectado a mi vida y ser los motores que impulsan mis sueños e ilusiones.

A mis sobrinos:

Nohelia, Víctor Hugo y Alexander por s u cariño, comprensión y apoyo en los momentos difíciles.

Mis hermanos:

Alexanders, que desde el cielo seguro se alegra por mí, a Byron, y Oscar David, quien a sus diecisiete añitos, me dio el tema a investigar.

A mis tíos:

Héctor y Aníbal, por acompañar estos sueños e ilusiones.

AGRADECIMIENTO A:

Los Licenciados:

Miembros de la Honorable Comisión de Trabajos de Graduación, Vasthi Alelí Reyes Laparra, Luis Augusto Macz Choc, Álvaro Enrique Sontay Ical, y Wilmer Martín Quim Cuc. (Asesora) Carla Liliana Chacón Monterrozo, (Revisor) Oscar Roberto Rosales Gómez, Vilma Aracely de León Miranda; y (Redacción y Estilo) Aura Violeta Rey Yalibat por su colaboración y profesionalismo con los estudiantes. Doctora Thelma Patricia Cortez Bendfeldt, un agradecimiento especial como profesional e investigadora.

A mis amigos:

Flor de María Avilés Chacón, María del Rosario Morales, Eunice Álvarez, Sergio Dardón, Sandra Maribel Ramírez Sierra, David Winter, Helmooth Morán Herrera y Víctor Méndez. Por su solidaridad y amistad incondicional.

La Tricentenaria Universidad de San Carlos de Guatemala:

Alma Máter Central, por formarme en mis años de estudiante, y al Centro Universitario del Norte, por admitirme y ser parte fundamental en mi desarrollo y formación profesional.

ÍNDICE GENERAL

Pág.

RESUMEN ix
INTRODUCCIÓN 1
OBJETIVOS 5

CAPÍTULO 1
EL DERECHO INFORMÁTICO

1.1 Derecho informático e informática jurídica 7
1.2 Antecedentes 9
1.2.1 Derecho informático 13
a. Concepto 14
b. Elementos personales 15
c. Bien jurídico tutelado 16
d. Derecho informático y sus límites 17
1.2.2 Informática jurídica 19
a. Concepto 20
b. Elementos personales 21
c. Bien jurídico tutelado 21
1.3 Diferencia entre derecho informático e informática jurídica 24
1.3.1 Documentación informática-jurisprudencial 25

CAPÍTULO 2
MARCO JURÍDICO RELACIONADO CON DERECHO INFORMÁTICO

2.1 Antecedentes
2.2 Constitución Política de la República de Guatemala y la protección de los datos personales 31
2.2.1 La inviolabilidad de la correspondencia, documentos y libros 33
2.2.2 El acceso a registro y archivos del Estado 36
2.2.3 Publicidad de los actos de la administración pública 38
2.2.4 Derecho a la privacidad, hábeas data o exhibición de datos 39
a. Consentimiento expreso 42
b. Violación al hábeas data 44
2.3 Derecho penal relacionado con la informática jurídica 49
2.2.5 Características de los delitos cibernéticos

(Delitos de cuello blanco) 57
2.2.6 Delitos contra los datos personales y delitos Informáticos 60
2.2.7 Conceptos 63
2.3 Convenio de Budapest 70
2.3.1 Antecedentes y alcances normativos 74
2.3.2 Países que se han suscrito al convenio de Budapest 75

CAPÍTULO 3

FRAUDE CIBERNÉTICO

3.1 Antecedentes 79
3.2 Fraude cibernético 85
3.2.1 Concepto 90
3.3 Competencia jurisdiccional para diligencias novedosas en Guatemala 90
3.3.1 Diligencias novedosas 91
3.3.2 Competencia jurisdiccional 96
3.4 Juzgados especializados 99
3.4.1 Cibernética forense 101
3.4.2 Importancia de la cooperación internacional contra la cibercriminalidad 103
3.5 Amplitud en la admisión de pruebas de cibernética forense 105
3.5.1 Alcance normativo 108

CAPÍTULO 4
ANÁLISIS DE LA PROPUESTA DE LA LEY 4055 CONTRA EL FRAUDE CIBERNÉTICO EN GUATEMALA Y TRABAJO DE CAMPO

4.1 Análisis de la iniciativa 111
4.2 Presentación, análisis y discusión de resultados 129
4.3 Desarrollo de la investigación 144
CONCLUSIONES 147
RECOMENDACIONES 151
BIBLIOGRAFÍA 155
ANEXOS 161

ÍNDICE DE GRÁFICAS

		Pág.
Gráfica 1	Cibercriminalidad según Convenio de Budapest 2011	71
Gráfica 2	Cibercriminalidad según Convenio de Budapest 2012	72
Gráfica 3	Cibercriminalidad según Convenio de Budapest 2013	73
Gráfica 4	Seguridad cibernética en América Latina y El Caribe: Del 2010 al 2013	78
Gráfica 5	¿Ha escuchado en medios de comunicación sobre los peligros del uso indebido del internet?	131
Gráfica 6	¿Conoce qué es el fraude cibernético?	132
Gráfica 7	Señale cuál de los siguientes datos ha proporcionado por internet, teléfonos celulares, correo electrónico u otro medio tecnológico:	133
Gráfica 8	¿Por qué considera que las personas no denuncian ser víctimas de delitos cibernéticos?	135
Gráfica 9	Considera que alguna vez ha sido víctima de los siguientes delitos cibernéticos? • Acoso • Amenaza • Calumnia • Difamación	

- Engaño
- Falsificación de datos
- Fraude
- Intimidación 137

Gráfica 10 ¿Alguna vez ha denunciado ser víctima de delitos cometidos por internet? 139

Gráfica 11 ¿Sabe si los delitos informáticos están regulados en Leyes actuales? 141

Gráfica 12 ¿Sabe que actualmente se encuentra pendiente de aprobación la propuesta de iniciativa de Ley 4055 sobre Delitos Informáticos? 142

Gráfica 13 ¿Tiene interés en conocer el contenido de la iniciativa de Ley 4055, sobre Delitos Informáticos? 143

ÍNDICE DE CUADROS

		Pág.
Cuadro 1	Delitos tradicionales y sus equivalencias	22
Cuadro 2	Tipos penales de mayor incidencia identificados en la red social	146

LISTA DE SIGLAS Y ABREVIATURAS

CEJA: Centro de Estudios Jurídicos de las Américas

CEPAL: Comisión Económica Para América Latina

CERIGUA: Centro de Reportes Informáticos Sobre Guatemala

CICIG: Comisión Internacional Contra la Impunidad en Guatemala

CIPREVI: Centro de Investigación para la Prevención de la Violencia

DICAT: Departamento de Investigación de Crímenes y Delitos de Alta Tecnología

EG: Encuentro por Guatemala

FBI: Buró Federal de Investigación

GPS: *Global Positioning Sistem*, Sistema de Posicionamiento Global

OEA: Organización De Estados Americanos

ONU: Organización de Naciones Unidas

REMJA: Reunión de Ministros de Justicia de las Américas

SCIRT: Equipo de Respuesta a Incidentes de Seguridad Cibernética

SIC: Proviene de la frase latina ***sic erat scriptum***, 'así fue escrito'

UNFPA: Fondeo de Población de las Naciones Unidas

UNODC: Oficina de Naciones Unidas Contra la Droga y el Delito

RESUMEN

El presente trabajo de investigación, se pretende realizar un análisis jurídico del fraude cibernético en Guatemala, para ello se utilizó como base legal, la Constitución Política de la República de Guatemala, así como las Leyes vigentes que regulan lo referente a delitos relacionados con la tecnología, como: la *Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas*, Decreto 47-2008; *Ley de Derechos de Autor y Derechos Conexos*, Decreto 33-98; *Ley de Acceso a la Información Pública*, Decreto 57-2008; así como, herramientas jurídicas de derecho comparado, Acuerdos y Convenios Internacionales de protección contra delitos de alta tecnología.

Se realizó un estudio de las Memorias del Estado, de los períodos comprendidos del 2010 al 2013, en virtud de ser fuente de datos estadísticos de delitos denunciados y sancionados por el Estado a nivel nacional, sin embargo, en ningún registro se encontraron datos referentes a denuncias o delitos claramente relacionados con la tecnología. La Procuraduría General de la Nación reportó 259 denuncias en el año 2012, relacionadas con transgresiones a derechos vinculados con tecnología; no obstante, no constan como tales en los registro estatales. Por lo que se procedió a realizar una encuesta utilizando la página social de Facebook, como medio tecnológico de comunicación e interacción social, por medio de la cual se determinó que el 66.67% de los encuestados no denuncia ser víctima de éste tipo de delitos, pues

no existe regulación al respecto. Mientras que un 33.33 %, refirió no efectuar las denuncias por temor a represalias. Se utilizaron los métodos de investigación de tipo jurídico-descriptiva y analítica, en virtud de formularse el análisis de casos concretos, con el objetivo de establecer si existe transgresión de los derechos constitucionales como garantías mínimas e irrenunciables para los ciudadanos, observando e interpretando en el marco legal que se regula en la Constitución Política de la República de Guatemala, asimismo el desarrollo de la presente investigación se fundamentó en el análisis de tipo jurídico propositivo, porque se plantea el problema y la posible solución viable para la aplicación de la Ley contenida en nuestro actual ordenamiento jurídico en relación al fraude cibernético.

La justificación para llevar a cabo el presente análisis, deriva precisamente de la necesidad de legislar en cuanto a los delitos tecnológicos que constantemente vulneran los derechos fundamentales de los ciberciudadanos en general. Para el desarrollo de la presente investigación se utilizaron las técnicas siguientes: Investigación de campo a través de fichas bibliográficas, encuestas. En especial se realizó el análisis jurídico de la propuesta de *Ley 4055 de Delitos Informáticos*, que ofrece la protección contra algunos delitos; no obstante, son insuficientes para ejercer una verdadera protección por parte del Estado, pues existe una diversidad de hechos delictivos que no encuadran en esas figuras punibles, por lo que es necesario crear una Ley especial de delitos Informáticos proyectada de acuerdo a nuestra realidad nacional.

Por tanto, con la presente investigación se pretende contribuir al avance de la justicia penal en Guatemala, para alcanzar las garantías que la *Constitución Política de la República de Guatemala* resguarda.

INTRODUCCIÓN

Los delitos informáticos representan una grave infracción a las normas constitucionales, establecidas para la prevalencia del bien común y para la prevención de esta modalidad delictiva, sin embargo, Guatemala no cuenta con un plan de respuesta a la crisis que puedan ocasionar los delitos cibernéticos. Es por ello que en el siguiente análisis se exponen las diferentes propuestas legales en cuanto a delitos cibernéticos, mediante el uso del derecho comparado como herramienta legal, así como la postura ideológica de diferentes autores en el marco de los derechos fundamentales, en especial lo referente al derecho a la autodeterminación informativa o hábeas data. Las teorías que orientaron el desarrollo del presente contenido, son las que informan a la dogmática penal moderna, en especial a la teoría finalista que establece de forma más adecuada la persecución del delito.

Sobre la base del principio de legalidad, el objetivo principal de la presente investigación es identificar cuáles son los derechos constitucionales que se vulneran al cometer fraude cibernético, mismos que deben protegerse en la investigación de la prueba cibernética y la aplicación de la norma de asistencia entre países, en especial la protección de la información de datos contenidos en archivos, y al uso de instrumentos de derecho internacional que coadyuven en beneficio de la aplicación del derecho.

Las constituciones evolucionan para brindar seguridad jurídica a sus ciudadanos como consecuencia a los cambios que sufren las sociedades. Sin embargo, se complica la aplicación de las actuales normas del *Código Penal*, al no existir suficientes figuras punibles, lo que se traduce en lagunas legales que permiten al delincuente realizar actos ilícitos, haciendo uso de las nuevas tecnologías de la información. En ese sentido, es obligación del Estado el alcanzar ese grado de sofisticación al adecuarse a las tendencias tecnológicas modernas, para contrarrestar los efectos negativos del uso de tecnología, tanto del delincuente común, como del crimen organizado, utilizando herramientas jurídicas eficaces de asistencia mutua entre naciones y poder así en alguna forma, encuadrar los actos ilícitos con figuras jurídicas acordes al avance tecnológico.

El derecho comparado es de suma importancia para el desarrollo de la presente investigación, por lo que el análisis se centró en el estudio de los elementos fundamentales comunes al fraude cibernético, considerando las diferencias en las esferas sustantivas y cotejando algunas legislaciones de derecho internacional en beneficio de la modificación del derecho adjetivo guatemalteco, para que se adecúe a nuestra realidad nacional; no obstante, para la legalidad de los distintos elementos probatorios que se implementen en coherencia con el resto de las acciones procesales, y que coadyuven en la búsqueda de la aplicación de la justicia penal, se debe determinar la eficacia de la prueba cibernética.

Se hace del conocimiento del lector que, considerando que la inmersión de la tecnología en nuestra sociedad es una realidad que no podemos ignorar, en el presente trabajo de investigación se revisan los conceptos y visiones tradicionales del mundo físico, para adaptarlos al actual contexto del mundo tecnológico. El presente trabajo, consta de cuatro capítulos a saber**,** distribuidos de la siguiente forma:

En el capítulo uno, se preceptúa lo relativo a: Aspectos generales, derecho Informático e Informática jurídica y sus diferencias, así como lo referente a documentación informática jurisprudencial, es decir, sentencias o procesos y otros documentos de acceso público;

En el capítulo dos, contiene lo respectivo a: Marco jurídico relacionado con el derecho informático, especialmente referencias conceptuales y en especial, la relación de la *Constitución Política de la República de Guatemala* y la protección de los datos personales;

En el capítulo tres, se incluye lo concerniente a: Antecedentes del fraude cibernético, lo referente a competencia jurisdiccional para diligencias novedosas en Guatemala; diligencia novedosas, competencia jurisdiccional, juzgados especializados, cibernética forense, importancia de la cooperación internacional contra la cibercriminalidad, en especial la amplitud en la admisión de pruebas de cibernética forense, alcance normativo; y

En el capítulo cuatro, se expone lo referente a: Análisis de la propuesta de Ley 4055 *Ley de Delitos Informáticos*, presentación, análisis y discusión de resultados y desarrollo de la investigación.

La importancia de la investigación efectuada se debe a que, los derechos fundamentales tradicionales protegidos por la *Constitución Política de la República de Guatemala,* han evolucionado con la introducción de la informática en el mundo de lo jurídico, por lo que es necesario identificar los derechos Constitucionales que se vulneran al cometer fraude cibernético y

establecer si los vacío legales y esa protección que ofrece el Estado, es subsanada con las Leyes vigentes.

OBJETIVOS

GENERAL

a. Identificar cuáles son los derechos constitucionales que se vulneran al cometer fraude cibernético.

ESPECÍFICOS

a. Analizar si los bienes jurídicos tutelados por la *Constitución Política de la República de Guatemala*, en el marco de la prevención del fraude cibernético, son congruentes con la propuesta de Ley 4055 de Delitos Informáticos.

b. Identificar los delitos que no están tipificados en la propuesta de Ley 4055 de Delitos Informáticos.

c. Determinar si la violación del hábeas data o violación de los datos personales constituye un delito que puede ser penalizado.

d. Identificar los vacíos legales que pueden ser subsanados a través de leyes existentes.

CAPÍTULO 1
EL DERECHO INFORMÁTICO

1.1 Derecho informático e informática jurídica

Entre el derecho y la informática, existen dos tipos de enfoques: El primero, hace referencia a lo instrumental, es decir, lo referente a la informática jurídica como instrumento. El segundo, hace referencia a la informática como objeto del derecho. Al hacer un breve análisis relativo al derecho y la informática, en sus inicios existía una simple relación como herramienta instrumental para facilitar la vida cotidiana, en la actualidad su uso se va haciendo cada vez más indispensable en el desarrollo de los países y sistemas económicos, que con la evolución tecnológica, se van haciendo de uso cotidiano. Sin embargo, al considerar la informática como objeto del derecho se hace alusión al derecho informático en sí mismo, haciéndose imperante establecer la diferencia que existen para su mejor comprensión.

> "Según ***Héctor Ramón, Peñaranda***[1], la interrelación entre el Derecho y la Informática, se crean unas relaciones intersubjetivas entre las personas naturales o jurídicas y de entes morales del Estado, y surgen entonces, un conjunto de reglas técnicas conectadas con el derecho, que vienen a construir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la ciencia informática con autonomía propia."

[1] Héctor Ramón, Peñaranda Quinteros. *Iuscibernética. Interrelación entre el Derecho y la Informática*. https://www.Monografías.com (14 de mayo de 2 015).

La informática, surge de la inquietud del ser humano para desarrollar métodos y técnicas efectivas de comunicación. Por definición, el procesamiento de datos o cibernética se conoce como: la ciencia encargada del estudio de la automatización, procesamiento, almacenamiento y clasificación de datos; para accesar a los mismos, es necesario utilizar sistemas computacionales de tecnología que comprenden un sistemático y complejo mundo cibernético. El avance tecnológico que experimentan las sociedades, se debe a que las nuevas generaciones manejan esos instrumentos especializados en su qué hacer cotidiano; y al constante flujo de programas, sistemas, redes y formas de interacción que crean una evolución tecnológica.

La sistematización de los programas tecnológicos ha permitido simplificar, organizar y agilizar, una gran variedad de actividades en el mundo moderno, lo que también ha propiciado un desarrollo significativo en distintas ciencias. Esta herramienta tecnológica, es imprescindible para la implementación de nuevos métodos de investigación, coadyuva en la búsqueda del desarrollo social y económico de las naciones, en pro de sus habitantes. Como herramienta innovadora, favorece el tratamiento de la información y su correspondiente sistema de archivo; así como, el uso de los programas específicos, que permiten y facilitan cambios esenciales en la labor judicial, accediendo a una mejor aplicación de los recursos del Estado, proporcionando un ambiente de estabilidad. Corresponde al Estado el observar que se cumplan los principios procesales.

1.2 Antecedentes

El desarrollo de la sociedad ha tenido su mayor avance desde el surgimiento de la tecnología, como eje vital para impulsar el desarrollo económico-social a nivel mundial. El enfoque abierto de los estudiosos de las ciencias tecnológicas, ha permitido que dicha evolución especializada, trascienda y alimente otras ciencias que en conjunción, sean la base de herramientas eficaces y fundamentales para el desarrollo en general. No obstante los beneficios, también son plataforma para la comisión de nuevas formas de contravención a las normas establecidas por las entidades Estatales y que por el medio utilizado, trasciende barreras fronterizas, lo que se ha transformado en células especializadas de crimen organizado. Es así que, con el avance tecnológico, surgen nuevas formas de contravención a los derechos inherentes a la persona humana, tanto individual como en forma colectiva.

Informática, tecnología de la información, cibernética son algunas denominaciones que reciben los sistemas organizados de la tecnología. André Marie- Ampere (1775-1836) utilizó por primera vez el término cibernética. Algunas definiciones de autores establecen diversas posturas respecto a la definición de la informática; sin embargo, se colegia en cuanto a que son **sistemas operativos tecnológicos**. Es obligación del Estado, proporcionar un ambiente de seguridad jurídica; no obstante, por medio de las disposiciones legales actuales, no se dispone de normas especiales.

Wiener[2], matemático, estadounidense, es conocido como el fundador de la cibernética, quien acuño el término científico en su libro "*Cibernética o el Control y Comunicación en Animales y Máquinas*", publicado en 1947. Utilizó sus modelos matemáticos para reproducir el sistema automático de las redes neuronales que gobiernan el automatismo respiratorio, lo que sirvió de base para la creación de la primera computadora.

Stafford Beer. Filósofo de la teoría organizacional y gerencial, citado por Wiener como "*El padre de la Cibernética de Gestión*", respecto de la Teoría Cibernética, define la cibernética como:

> *"*Ciencia que estudia los flujos de información que rodean un sistema y la forma en que ésta información es usada por el sistema como un valor y la define como la ciencia de la organización efectiva*".*[3]

Se suele confundir la cibernética con la informática en virtud de la utilización de la tecnología, sin embargo a diferencia de la informática, la cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas. La unión de diferentes ciencias como la mecánica electrónica, medicina, física, química y computación han dado surgimiento de una nueva doctrina denominada *biónica*, la cual busca imitar y curar enfermedades y, deficiencias físicas a través de la cibernética. La informática por otra parte, es la ciencia que se ocupa específicamente de los sistemas operativos de comunicación con el uso de tecnología de la información que surgen como nuevas

[2]Norbert, Wiener. http://www.biografiasyvidas.com./biografia/w/wienwr.htm. (15 de mayo de 2 015).

[3] Publicado por Camilo, Gonzales Serrano. *Teorías de la comunicación, teoría cibernética.* https:// www.teoriadela.blospot.com/2013/02/teoria-cibernetica.html. (martes 26 de febrero de 2 013).

herramientas jurídicas de trabajo en beneficio de la simplificación en la investigación de las ciencias en general.

> (Del Fr. Informatique) **La Real Academia Española,** define la informática jurídica como: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*".*[4]

En la *Convención de Palermo*, en la actualidad se han observado problemas originados por la transgresión al derecho de las personas individuales y/o colectivas, que tienen relación directa o indirecta con la tecnología de la información y el derecho en general, lo que ha generado la necesidad de analizar lo referente al denominado Derecho Informático en virtud del creciente avance de la delincuencia transnacional. Aunque existen muchos países que han incluido dentro de sus disposiciones legales, lo referente a la protección del derecho informático individual y colectivo, han surgido nuevas formas de comisión de hechos delictivos, utilizando novedosos medios tecnológicos como plataforma para hacerlos ineficaces.

Han surgido de igual forma, figuras de defensa de esos derechos protegidos tanto por el Estado a través del Ministerio público, como de organismos internacionales de asistencia y cooperación internaciones, por ejemplo la Comisión Internacional Contra la Impunidad en Guatemala (CICIG).

[4]Diccionario de la Real Academia Española versión digital. Https:/lema.rae.es/drae/svr/search%3Fkey%3Dinfor%25C3%25C3%25°1tica.(6 de junio de 2 015)

La integración tecnológica, ha evolucionado el mundo en diferentes facetas, transformando la visión del mundo cibernético y evolucionando de simple herramienta opcional a elemento fundamental en varias esferas, siendo como característica principal y especial los efectos transnacionales. En ese sentido, el proyecto de Ley Peruana establece en la Guía para los Países en Desarrollo y la Unión Internacional de Telecomunicaciones, que el uso del internet y la TIC ha permitido desarrollar un conjunto de aplicaciones informáticas para el desarrollo del cibergobierno, cibercomercio, la cibereducación, la cibersalud y el ciberentorno entre otros, lo cual ha permitido mejorar la calidad de los servicios brindados a la sociedad y, en especial, ha facilitado la integración progresiva de poblaciones en zonas remotas, lo cual es un factor importante de inclusión social.

Los derechos fundamentales instituidos en la *Carta Magna* son preceptuados más allá de la percepción del futuro inmediato. De los Artículos 1, 2, 3, 4, 5, 24, 29, 30, 31, 35, 39, 41, 42, 44, 46, relativos a los derechos fundamentales relacionados con la privacidad, sin desmerecer los derechos sociales y el derecho a no ser discriminado; se precisa la importancia que surge en virtud de los avances informáticos y la vulnerabilidad de nuevos derechos así como de nuevas figuras delictivas, que forman parte del fenómeno tecnológico a nivel mundial. El aporte de doctrinas aplicables al derecho, debe ser congruente con las herramientas jurídicas de derecho comparado, para coadyuvar en aquellos casos en que el delito trascienda fronteras. No obstante, existen limitaciones en la administración de justicia, debido a las lagunas legales en cuanto a delitos relacionados con alta tecnología.

> Según el ***Dr. Vladimir, Guerra***[5]***, "***la enumeración constitucional de los derechos fundamentales no constituye un numerus clausus, porque ello sería tanto como admitir la desprotección en cierto ámbitos; la tipificación no significa que la personalidad sea la suma de estos concretos derechos fundamentales, sino que los tipificados son la concreción positiva de la personalidad y por ello pueden los Tribunales interpretar las normas constitucionales, para ofrecer una protección lo más amplia posible."

Considerado como derecho fundamental y natural[6] que es materia de protección de los derechos humanos de las personas, el derecho a la privacidad de los datos es inherente a la condición humana. En tal virtud, se define derecho natural como:

> "Es el ordenamiento jurídico que nace y se funda en la naturaleza humana, debiendo su origen, por tanto, a la voluntad normativa de ninguna autoridad, como ocurre con el derecho positivo. Es un conjunto de preceptos que se imponen al derecho positivo y que éste debe respetar…El derecho natural es un derecho, tanto por la estructura de sus normas (Enunciados prescriptivos relativos a comportamientos) como por su obligatoriedad. (El derecho natural es aceptado como objetivamente obligatorio*)".*[7]

1.2.1 Derecho informático

> "El término Derecho Informático (Rechtsinformatik) fue utilizado por el Dr. Wilhelm Steinmüller, académico de la Universidad de Ratisbona de Alemania en 1970".[8]

---

[5] Vladimir Osman, Aguilar Guerra. *Derechos fundamentales*. (Guatemala: Serviprensa, 2 005.) 77.

[6] Diccionario Jurídico Espasa. *Derecho natural*. (Madrid, España: Calpe, 1 999.) 322.

[7] Ibíd.

[8] Definiciones.*DerechoInformático*.https://www.es.wikipedia.org/wiki/Derecho_informático. (14 de mayo de 2 015).

El Derecho Informático, surge a partir de 1942, del uso generalizado de sistemas cibernéticos, especialmente, con la implementación de los diferentes medios sociales de comunicación masiva, que por lo complejo de su estructura son difíciles de rastrear; sobre todo, en aquellos casos en que se transgredan o violen derechos individuales o colectivos.

Según el tratadista ***Carlos A. Peña***, respecto al Derecho y las técnicas de la información, en especial a la injerencia de la tecnología en el entorno social, se denomina derecho informático:

> *"*Es la universalidad de problemas que surgen de las transformaciones que el derecho ha ido realizando, como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social, y que requieren nuevas regulaciones o una interpretación de las regulaciones ya existentes a fin de dar respuestas en el sentido de la justicia".[9]

a. Concepto

Derivado del análisis de las ideas conceptuales, puede concluirse entonces que el Derecho Informático es la ciencia que se encarga del estudio y análisis del conjunto de principios, innovaciones tecnológicas y disposiciones normativas dirigidas a la regulación de las nuevas tendencias especializadas y la comunicación en general, que surge como consecuencia de la evolución tecnológica en las sociedades actuales; así también, en virtud del uso de nuevas herramientas científicas especializadas e impuestas a la sociedad, por las continuas diligencias novedosas que se

[9] Carlos Alberto, Peña. *Derecho y las tecnologías de la información*. (Buenos Aires Argentina: Universidad de Palermo, 1 998). 23.

desarrollan en beneficio social, cultural, individual, colectivo y comercial.

Es importante tomar en consideración, el regular lo referente a delitos tecnológicos en una *Ley Especial de Tratamiento de Datos*, sean éstos contenidos de carácter público y privado; y en consecuencia, analizar el impacto social generado por las nuevas plataformas científicas, tecnológicas, comerciales e individuales inmersas en el mundo cotidiano cuya interacción trascienden al mundo de lo jurídico.

b. Elementos personales

1. Sujeto Activo: (Hacker) El que comete el delito.

Es la persona que tiene habilidades especiales relacionadas con la cibernética, la tecnología y todas las herramientas tecnológicas novedosas utilizadas en la comisión de una conducta delictiva, antijurídica y culpable a cuya intervención, ya sea activa o intelectual, debe adjudicarse una pena. También son denominados delitos de cuello blanco. Pues son cometidos por medios tecnológicos, en donde una persona con conocimientos en cibernética, y en virtud de un trabajo estratégico o no, y sobre todo al conocimiento de los sistemas operativos informáticos específicos y con características sensibles, por lo que: sustrae, modifica o utiliza información o documentos en general, sin el consentimiento del titular del derecho. Son delitos con características no

violentas que cometen las personas, normalmente por motivos financieros.

2. **Sujeto Pasivo**: (Usuario) Víctima del delito.

   Es cualquier ente sobre el cual recae la conducta antijurídica que realiza el sujeto activo. Pueden ser[10]:

- Personas Individuales
- Personas Jurídicas
- Instituciones Bancarias
- El Gobierno

c. Bien jurídico tutelado

Del contenido de los conceptos de los juristas, se puede determinar que el bien que ha sido lesionado directa o indirectamente o puesto en peligro por la comisión de una conducta delictiva, antijurídica, típica y culpable, y que es constitutiva de sanción penal, es en esencia *la información*; y que, por ser sustraída sin el consentimiento y la acción ejecutada por medios tecnológicos como herramienta para la comisión de hechos delictivos continuados, puede y debe ser tipificado, regulado y sancionado como delitos contra los derechos fundamentales del ciber ciudadano.

[10]Santiago, Acurio del pino. *Delitos informáticos, generalidades*. (Quito, Ecuador: Editorial Cep, 2 009.) 21.

d. Derecho informático y sus límites

La *Constitución Política de la República de Guatemala*, establece por un lado, en el Artículo 35 respecto de la libertad de emisión del pensamiento, que es un derecho esencial a la condición de ciudadano, utilizando para ellos los distintos medios de difusión; por otro lado, en el Artículo 80 en cuanto a la Promoción de la Ciencia y la Tecnología, lo referente a las herramientas jurídicas especializadas anticipándose a los acontecimientos futuros, se entiende que las nuevas predisposiciones tecnológicas coadyuvan en la persecución de posibles hechos delictivos. Herramientas jurídicas, como la implementación del sistema de cámaras **Gessel** que con el objeto de utilizar los nuevos avances tecnológicos al servicio del sistema jurídico nacional penal en beneficio de la población.

En el uso del derecho de expresión, la plataforma de las redes sociales proporciona un medio por el cual los usuarios utilizan herramientas electrónicas, en las que se intercambia información diversa, no necesariamente fidedigna. En su gran mayoría, algunos usuarios utilizan estas redes para difamar, amenazar, coaccionar e incluso acosar a otros usuarios. En ocasiones, éstos medios son utilizados para la comisión de hechos delictivos que trascienden la relación tecnológica indirecta, como medio generador y fundamental de un hecho punible; sean estos sobre hurto de información en general para beneficios económicos o simplemente, como medio que utilizan los grupos de delincuencia organizada o personas con

interés directo en la comisión del hecho punible, para efectuar otro delito.

Sin embargo, también se establece que en el uso de esa libertad de expresión, no debe alterarse el orden público o faltar el respeto a la vida o a la moral. En general se prevé, el establecimiento del orden público en todo momento, como garantía de seguridad al ciudadano en beneficio preferentemente colectivo, sin excluir el derecho individual que posee cada ciudadano.

Asimismo, en la *Ley de Emisión del Pensamiento*, Decreto Número 9, se estable que son responsables ante la Ley quienes falten al respeto, a la vida privada o a la moral, o incurran en los delitos de faltas sancionados por la norma. El Estado de Guatemala, debe garantizar a los habitantes los derechos naturales y comunes inherentes a la persona humana. Los derechos específicos y claramente vulnerables al ser víctima de delitos cibernéticos, cometidos utilizando medios tecnológicos al ser expuestos a los diferentes medios de comunicación social son: el derecho a la privacidad, el honor, derecho de propiedad informática e intelectual, derecho de autodeterminación o hábeas data y protección a los datos personales, entre otros.

1.2.2 Informática jurídica

Algunos tratadistas, refieren acerca de la informática en cuanto a su juicio y la conceptualizan de la siguiente manera: ***Di Giorgi***,[11] ***"****L'informatica giuridica"*, citado por Hernández Díaz, Leyre, al respecto de la informática, relaciona "el uso de las nuevas tecnologías de la información al derecho, sobre todo a los sectores que integran éste ámbito jurídico".

> "Según ***Carlos A. Peña*** esta concepción de la informática como herramienta utilizada por los operadores del derecho se le llama usualmente con el nombre de Informática jurídica. Herramienta jurídica, actualmente de uso cotidiano".[12]

> ***"Julio Téllez,*** en su definición y clasificación de la informática-jurídica expresa que es la técnica disciplinaria que tiene por objeto el estudio e investigación de los conocimientos aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamientos de información jurídica necesaria para lograr dicha recuperación".[13]

[11] Di Giorgi, R. M./Ragona, M. *L´informatica del diritto. Citado por Hernández Días Leyre. (Milano, Italia: Edito da Giuffré, 2 004). 227.*

[12] Ibíd., 243.

[13] *Informática jurídica*. https://wwwes.slideshare.net/. (18 de mayo de 2 015).

> *"**Emilio, Suñé LIinas***, en su visión de la informática la define como la aplicación de los ordenadores electrónicos orientada a la reducción de problemas jurídicos".[14]

a. Concepto:

Es la ciencia que encargada del estudio, investigación, análisis y aplicación de la tecnología de la información al mundo de lo jurídico." Tiene trascendencia en las distintas ramas con las que el derecho tiene relación directa o indirecta, es decir, que la informática en virtud de haberse fusionado en el marco de las actuaciones judiciales, beneficios sociales, económicos, individuales y jurídicos; también tiene relación con la comunicación, telemática, ingeniería, etcétera, que en un momento dado pueden coadyuvar en el peritaje de procesos jurídicos a través de las nuevas formas de reproducción de los procesos legales, en las audiencias.

Se logra entonces unificar la informática jurídica como herramienta fundamental, para cumplir con el principio de celeridad procesal. En consecuencia, es la relación que existe entre el derecho y el uso de tecnología de la información, siendo ésta un medio eficaz en la interpretación de documentos que utilizan los profesionales del derecho como instrumentos o herramientas cotidianas, y medios eficaces en el desarrollo y aplicación de procedimientos que se

[14]Emilio, Suñé Llinas. *Informática jurídica y derecho informático*. (Distrito Federal, México: Editorial Porrúa, 2 006.) 20.

ejecutan en sus actuaciones judiciales. Entonces, trata de documentos, y no de normas.

b. Elementos personales

Sujeto Activo: Juristas en general.
Profesionales del derecho en el desarrollo de sus actividades profesionales.
Sujeto Pasivo: Usuario o dueño del derecho que se protege. En el uso de la defensa de sus derechos en cada proceso judicial**.**

c. Bien jurídico tutelado

El bien jurídico protegido en general es la *información*[15]; sin embargo, es considerada de diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico y finalmente por los sistemas que la procesan o automatizan.

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

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

[15]Santiago, Acurio del Pino. *Delitos informáticos, generalidades*. (Quito, Ecuador: Editorial Cep, 2 009.) 20.

CUADRO 1
DELITOS TRADICIONALES Y SUS EQUIVALENCIAS[16]

Delitos tradicionales	Ciberdelito equivalente
Hurtos menores/ daño malicioso	Hackeos, ataques software malicioso, degeneración de servicios.
Ofensas contra menores	Sitios web pornográficos, creación de perfiles falsos con fines pedófilos.
Lavado de dinero	Sistemas fraudulentos de pago en línea, mulas, engaño nigeriano (Nigerian Scam)
	Robo de identidad, phishing, *spoofing*, piratería software, películas y música, robo de Propiedad Intelectual en soporte electrónico, sustracción de equipos informáticos y celulares.
Acoso *coacción** *Amenazas** *difamación** *engaño**, intimidación*, *calumnias**	Ciberacoso, *coacción** etcétera, a adultos y menores.
Fraude	Fraude en línea, subasta fraudulenta, estafa por solicitud de fondos a través de internet.

Fuente: investigación de campo, 2015 *

La Constitución Política de la República de Guatemala, establece en cuanto a los derechos de los ciudadanos en la parte introductoria la primacía de la persona humana como sujeto y fin del orden social; reconociendo a la familia como génesis primario y fundamental de los valores espirituales y morales de la sociedad y, al Estado, como responsable de la promoción del bien común, de la consolidación del régimen de legalidad, seguridad, justica, igualdad, libertad y paz.

[16]*Ciberdelito en América Latina y El Caribe*. http://www.proyecto amparo. net/files/Ciberdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf./y/ht tps://www.crimecommission.govau/publications/crime. (22 de julio de 2 015).

En los *Acuerdo de Paz*, en el numeral 12, se establece que las reformas constitucionales contenidas en los acuerdos de paz, constituyen la base sustantiva y fundamental para la conciliación de la sociedad guatemalteca en el marco de un Estado de Derecho, la convivencia democrática, la plena observancia y el estricto respeto de los derechos humanos. Respecto a los principios y valores establecidos en los *Acuerdos de Paz*, *Convenios internacionales sobre Derechos Humanos*, Acuerdos de Cooperación Mutua y contenidos de investigación que surgen sobre delitos de alta tecnología, en los que los derechos protegidos por las constituciones políticas de los países.

Al igual que sucede en la República de Guatemala aunque no figuren como tales, como lo es el derecho a la autodeterminación informativa.

Algunos países integrantes de tratados internacionales contra el crimen organizado, en sus legislaciones tienen tipificados los delitos informáticos, como: Alemania, Austria, Italia, entre otros, por lo que presentan índices de criminalidad cibernética controlada, pese a esto, se modifican y aumentan día con día. Al no tener una regulación que norme la conducta de sus ciudadanos, existe anarquía o ausencia del poder del Estado o a la criminalidad. En relación a temas informáticos, en México a través de la *Revista Artículos Electrónicos*, respecto a las legislaciones en diferentes países, sobre temas de delitos cibernéticos se refiere que, la información y la privacidad de sus datos personales contenidos en archivos cibernéticos, existen,

aunque de hecho no estén tipificados en un ordenamiento jurídico, deben ser protegidos o sancionados por cada Estado.

Lo relativo a la integridad y disponibilidad de los datos contenidos en sistemas automatizados, archivo de datos o banco de datos que se sirvan del uso de tecnología, ya sea, con fines de archivo o almacenamiento de datos, acuerdos comerciales, secretos societarios, transacciones en general, archivos de uso y contenido privado o público que consten como archivos confidenciales; son todos bienes jurídicos que también son y deben ser protegidos por cada Estado.

1.3 Diferencia entre derecho informático e informática jurídica

- El **derecho informático** (esencial u objeto del derecho)

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

- En contraste, la **informática jurídica** (especial o instrumental)

Es de relación *especial,* porque surge de esa necesidad de protección a esos derechos inherentes del cual el Estado es garante. Como herramienta tecnológica de uso cotidiano, en la aplicación del ejercicio técnico de los juristas en el desarrollo de sus actividades profesionales, en especial, en la defensa procesal de los derechos vulnerados como representantes del Estado, a través de sus órganos jurisdiccionales. Es el sector normativo de los sistemas dirigidos a la regulación de las nuevas tendencias tecnológicas de la información, y la comunicación; es decir, se refiere a las propuestas normativas, teorías, análisis, investigaciones, estudios específicos, razonamientos jurídicos, etc. Trata de la norma en sí.

En resumen, es todo lo que tiene por objeto el analizar, interpretar, exponer y sistematizar esas normas fuente o documentos que se relacionan directa o indirectamente con el *derecho*.

1.3.1 Documentación informática-jurisprudencial

La documentación informática, trata precisamente de documentos jurídicos, leyes, sentencias, jurisprudencia entre otras, que se encuentran en documentos digitales. En cuanto a lo referente a la jurisprudencia, en la actualidad se encuentran a disposición resoluciones de interés y acceso público a los profesionales del derecho en las diferentes plataformas virtuales que proporciona la Corte de Constitucionalidad, a través de la Unidad de Gaceta y Jurisprudencia para beneficio público y administrativo, en el complejo mundo de la cibernética aplicada al mundo de lo jurídico a través de las páginas: *informática@cc.gob.gt* / *gacetas@cc.gob.gt*.

En cuanto al reconocimiento jurídico de las comunicaciones electrónicas, como documentos con efectos jurídicos, según se deduce de las disposiciones de la *Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas*, Decreto 47-2008, se enuncia en el Artículo 10, tienen validez o fuerza obligatoria por el simple hecho del consentimiento de las partes. Asimismo, establece que no se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica. Es decir, que las comunicaciones electrónicas son admisibles como medios de prueba, conforme los criterios reconocidos por la legislación para la apreciación de la prueba.

Países que cuentan con publicación informática jurisprudencial en América Latina y el Caribe:

- Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Paraguay, Panamá, Perú, República Dominicana y Venezuela.

Es importante dar algunos ejemplos sobre documentación informática, es decir, "Sentencias, Procesos o Expedientes**"** contenidas en páginas digitales o páginas web, para consulta pública relativas a delitos informáticos, utilizando medios tecnológicos para investigar el tipo de sanción que se emitió por la comisión del hecho punible, para el combate regional de los delitos informáticos, investigadores, policías y fiscales de Centroamérica y República Dominicana, participaron en un seminario taller sobre delitos informáticos. Algunos ejemplos de documentación Informática:

Proceso 34564, Corte Suprema de Justicia, **República de Colombia**. Sala de casación Penal, Acta 267. Transacción bancaria realizada desde la ciudad de Barranquilla de manera ilícita y superando barreras electrónicas. **Leyes Violentadas**: Se imputó hurto calificado, por haberse cometido superando seguridades electrónicas, según lo establecido en el Artículo 240.4 del código penal…afectación del **Bien Jurídico Tutelado**: patrimonio económico particular y determinación de la jurisdicción. Competencia / Transferencia de Activos. Magistrado ponente José Leonidas Bustos Martínez.

Expediente 1356-2006[17], Corte de Constitucionalidad. Juzgado Sexto de Primera Instancia del Ramo Civil del Departamento de **Guatemala**. Tribunal de Amparo. Promovido por el Procurador de los Derechos Humanos Jorge de León Duque.

En la resolución se establece que la comercialización de datos de una persona debe encontrarse sujeta a que esta sea proporcionada voluntariamente por la persona, cuyos datos serán objeto de comercialización**. Leyes Violentadas**: Artículos. 44, 46, 49 Constitución Política de la República de Guatemala; 10, 15, 197 Ley del Organismo Judicial; 25, 26 Ley de Amparo, Exhibición Personal y de Constitucionalidad; 17 Acuerdo 4-89 Corte de Constitucionalidad. **Bien Jurídico Tutelado:** Violación de datos personales a través de la página web denominada “informaciónpública.net” atentando contra la dignidad, intimidad, privacidad, honor y protección de datos

[17]Organismo judicial. *Sentencia 1356-2006*.https://www.informática@cc.gob.gt/ gaceta@cc.gob.gt. (22 julio de 2 015).

personales que figuran en programas informáticos. Divulgación de información. Guatemala 11 de octubre de 2006.

Sentencia, Corte Constitucional de **Colombia**[18]. C-1011/2008. Revisión de Constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado -221/07 Cámara (Acum. 05/06 Senado) "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."

Sentencia 21-7-03 (**Colombia**) en una acción tutelar por la violación al derecho constitucional de **Hábeas Data**, "autodeterminación informática y la intimidad mediante spam."

[18]*Revisión de constitucionalidad del proyecto de Ley Estatutaria*. https://Oiprodat.com/jurisdicción-relacionada/jurisdicción-sudamericana/ juris dicción-Colombia. (2 de junio de 2 015).

CAPÍTULO 2
MARCO JURÍDICO RELACIONADO CON DERECHO INFORMÁTICO

2.1 Antecedentes

La globalización como proceso de integración económica, social, política, ideológica, cultural y en general de desarrollo social, conlleva dispositivos tecnológicos que generalmente suelen proporcionar plataformas para el desarrollo de los países. En tal virtud, el Derecho Informático no sólo representa esa plataforma de desarrollo en sentido amplio, sino también, en el sentido estricto, crea nuevas fuentes y amplias esferas de desarrollo para los países considerados subdesarrollados. En el marco de las nuevas tendencias de negociaciones tecnológicas en pro del desarrollo de las naciones, también se generan nuevas figuras relacionadas con la contravención de éstas, en virtud de no existir cuerpos legales que las normen.

Creándose un vacío legal, que puede llegar a ocasionar, en algunos casos de relevancia nacional, innumerables violaciones a los derechos humanos. En consecuencia, se han creado normas de aplicación y cooperación transfronteriza en virtud de que este tipo de delitos suelen ser de carácter transnacional. El Artículo 44 de nuestra Carta Magna, establece lo referente a los derechos inherentes a la persona humana:

*"*Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana".[19]

Si se considera que con el surgimiento de la informática se ha trascendido no sólo la barrera de lo social, tecnológico, y jurídico; sino que, en realidad la informática representa el avance necesario de las naciones sean éstas desarrolladas o subdesarrolladas y, tomando en consideración que la tecnología es fundamental en el ámbito cotidiano, en consecuencia, es utilizado como plataforma para el progreso de las naciones; se colegia entonces, que tiene especial relevancia en el mundo comercial, en virtud de las nuevas formas de contratación, como: redes sociales, páginas web y nuevos medios de comunicación. Son los inicios de las nuevas tendencias de negociación tecnológica, contratos atípicos mercantiles, que dejan vulnerable también *nuevos* derechos contractuales.

La ausencia de elementos para juzgar transgresiones, facilita la comisión de delitos de carácter cibernético y muchos son producto del uso clandestino de las redes sociales, lo que ha generado propuestas concretas para posibles soluciones internas en algunos países latinos, como lo es la creación del *Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT*), contenido en la Ley 53-07 Sobre Crímenes y Delitos de Alta Tecnología que coadyuva como entidad subordinada a la Dirección Central de Investigaciones Criminales de la Policía Nacional de la República Dominicana; sin embargo, en Guatemala no se ha legislado al respecto.

[19] Asamblea Nacional Constituyente. *Constitución Política dela República de Guatemala*. Guatemala: Serviprensa, 1 985.

La población más vulnerable es la que se encuentra en un constante uso de la información digital, generalmente son los niños y adolescentes, quienes hacen uso continuo o cotidiano de las telecomunicaciones y tecnologías de la información, como lo son las redes sociales, juegos electrónicos, etcétera, siendo en muchos casos víctimas de personas con perfiles falsos con fines delictivos.

2.2 Constitución Política de la República de Guatemala y la protección de los datos personales.

Nuestra *Carta Magna*, establece en el Artículo 44 que esos derechos y garantías que otorga, no excluyen otros que, aunque no figuren expresamente en la ley, son inherentes a la persona humana. Asimismo que serán nulas *ipso jure* o de pleno derecho las normas y las disposiciones gubernativas o de cualquier otro orden que disminuyan, restrinjan o tergiversen los derechos que la constitución garantiza.

Del análisis de los Artículos 1 y 2 de la *Constitución Política de la República de Guatemala*, se deduce que esa protección de la cual el Estado es garante, abarca eventos futuros. En éste contexto, según el Artículo 44, la aplicación del derecho no es excluyente de los derechos emergentes en eventos futuros, que constituyan o se encuadren en nuevos derechos inherentes a la persona humana susceptibles a la protección Estatal. Es decir, que en la prevención de un evento o presupuesto futuro en el que el Estado debe anticipar sus acciones legales, como sucede con los que por disposición de la Ley deban ser subsanadas sin tener un trámite específico, los delitos de carácter

cibernético no pueden ser encuadrados pues no existe una figura punible, aunque se refieran a eventos futuros.

Dentro de los deberes del Estado, se establece el garantizar la protección de la ciudadanía, la vida, la libertad, la justicia, la paz y el desarrollo integral de las personas en todos los ámbitos en que éstos desarrollen sus actividades diarias, encaminadas a un bien común, como ley imprescindible; respetando la ley matriz en el uso de esos derechos fundamentales, ya sea que figuren expresamente o no, como sucede con las surgidas en épocas posteriores a la aplicación de las normas constitucionales en virtud del surgimiento de la evolución tecnológica, siempre existe una laguna legal. Nuestra constitución, en el Artículo 31 sobre derecho al acceso a archivos y registros estatales**:**

> *"*Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información y actualización*"*.[20]

Considerando el Artículo anterior como fundamento constitucional de la protección de datos personales, en donde se establece el derecho inherente de toda persona de conocer el contenido de los datos que de ellas consten, se deduce que se refiere a todo tipo de registros en donde figuren datos personales, que es en sí, el espíritu que fundamenta el *Hábeas Data*. Esa protección garantiza los eventos futuros, incluyendo los avances tecnológicos como presupuestos, es decir, en aquellos casos del uso inadecuado de tecnología al sustraer, modificar o alterar datos personales en general; Derechos garantizados por el Estado puesto que

[20] Ibíd.,

los valores, la justicia y el desarrollo integral de la persona son derechos inherentes a la condición de ciudadano.

Para lo cual debe adoptar las medidas legales que a juicio del Estado sean convenientes, según lo demanden las necesidades y condiciones del momento, que pueden ser individuales, sociales o colectivas. Requiere de un análisis profesional y acucioso, el evaluar los riesgos que puede ocasionar esa transgresión del derecho de propiedad informática y la inclusión del derecho de habeas data, así como el derecho de hábeas data financiero como bienes jurídicos tutelados en Guatemala.

La Ley 53-07, de la *República Dominicana*, en el Artículo 1 instituye que la Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se lleva a cabo por sus medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

2.2.1 La inviolabilidad de la correspondencia, documentos y libros

El *Código Penal guatemalteco*, respecto a los delitos contra la libertad y seguridad de la persona (Artículos 217-223) establece que:

> "Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despacho telegráfico, telefónico o de otra naturaleza, que no le estén dirigidos a quien sin abrirlos, se impusiere de su contenido será sancionado con multa de cien a mil quetzales".[21]

Las medidas técnicas, investigaciones, medios instrumentales y de administración de justicia que debe otorgar el Estado a través de sus órganos jurisdiccionales, que son necesarias para garantizar la seguridad y confidencialidad de datos personales vertidos en registros, ya sean estatales o de alguna institución no gubernamental, deben garantizar el resguardo de la privacidad de esos datos, que los usuarios proporcionen, evitando que el contenido sea adulterado o modificado; se debe impedir así mismo, la transmisión, pérdida, consulta o tratamiento de datos no autorizados. Es necesario entonces, implementar medidas eficaces que permitan evitar y detectar violaciones a los datos proporcionados por usuarios, que son susceptibles de ser expuestos a medios tecnológicos.

> "La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna…los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen plena prueba en juicio".[22]

---

[21] Congreso de la República de Guatemala. *Código penal guatemalteco*. (Decreto 17-73). *Delitos contra la libertad individual y seguridad de la persona.* (Guatemala: Librería jurídica, 1 992.) Artículo 217.

[22] Congreso de la República de Guatemala. *Código procesal penal*. (Decreto 51-92). *Libertad de la prueba*. (Guatemala: Librería jurídica, 1 992.) Artículo 182.

La *Ley Sobre Crímenes de Alta Tecnología de la República Dominicana,* establece en su primer considerando que los derechos y deberes fundamentales de los ciudadanos entre los que se encuentra la libertad de expresión, integridad e inviolabilidad de la correspondencia y demás documentos privados, incluyendo el correo electrónico. *El Código Tributario*, sobre la confidencialidad regula:

> "Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas. Los documentos o informaciones obtenidas con violación de este artículo, no producen fe, ni hacen prueba en juicio. Los funcionarios y empleados públicos que intervengan en la aplicación, recaudación, fiscalización y control de tributos sólo pueden revelar dichas informaciones a sus superiores jerárquicos o a requerimientos de los tribunales de justicia siempre que en ambos casos se trate de problemas vinculadas con la administración, fiscalización y percepción de los tributos".[23]

De igual forma la correspondencia, documentos, fotografías, videos, slideshares y libros, entre otros, contenidos en archivos digitales son susceptibles de protección, pues forman parte del patrimonio informático, que debe ser protegido y garantizado por el Estado. En la actualidad se observa la violación a éste derecho, a través de programas maliciosos o malwares, que contienen una diversidad de formas para la comisión delictiva, entre ellos: el infeccioso, el oculto y para obtener beneficios, utilizados para el hurto, modificación, clonación, transmisión y transformación de

[23]Congreso de la República de Guatemala. Código Tributario. (Decreto Número 6-91) Artículo 101.

contenido digital, que causa daños irreparables, por lo que debe ser regulado en una ley especial.

2.2.2 El acceso a registros y archivos del Estado

Como derecho otorgado por el Estado, el derecho de **reserva o confidencialidad de datos personales** conforme lo establece la *Constitución Política de la República de Guatemala*, es un derecho inviolable. Sin embargo, el dato o información a que se refiere, ya sea proporcionado por el usuario en virtud de un registro estatal o de una contratación, debe contener el pleno consentimiento del que tiene el derecho a esa intimidad, en cuanto a la información en sí y no debe transgredir ninguna norma, aún en virtud del mismo consentimiento.

En el Artículo 31 de la *Constitución*, se preceptúa que toda persona tiene el derecho fundamental de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, de igual forma en la actualidad existen archivos digitales que deben ser de fácil acceso para los usuarios de los medios tecnológicos; y siendo que la finalidad a que se dedica esta información, es de carácter público, debe proteger el derecho individual, así como el derecho de que corrija, rectifique y actualice la información, para evitar abusos de derechos, como en el caso de cobros abusivos por algunos bancos del sistema, al publicar listas de clientes morosos, que no han sido actualizadas.

Considerando que la inmersión de la tecnología para nuestra sociedad es una realidad que no se puede ni debe ignorar, es

necesario actualizar los conceptos y visiones tradicionales del mundo e incorporarlos al mundo digital e incluirlos en nuestro ordenamiento jurídico. En virtud de éste tipo de registros, se ha observado el incremento a la invasión de la privacidad, sobre todo de los datos contenidos en archivos y cuyo contenido no son de uso público. Ya sea, con el uso directo o indirecto de instrumentos tecnológicos, el acceso a la información no autorizada de esos datos considerados confidenciales, debe ser regulada y sancionada.

Debe establecerse la diferencia entre acceso lícito e ilícito de archivos informáticos. El tema de la seguridad[24] no sólo interesa a la tecnología aplicada a la seguridad jurídica, sino también, al negocio jurídico y comercio en general, en virtud del nuevo sistema de contrataciones electrónicas y al tratamiento de datos privado, semi-privado y público. Es así que, según la norma se preceptúa como:

- **Acceso ilícito** en la *Ley Peruana de Represión de la Cibercriminalidad se instituye que*:

> 'El que accede a todo o en parte de un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privada de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días de multa…'.[25]

[24]Cámara Internacional de Comercio. *Principios sobre la personalidad informática*.https//www.Velascocalle.co (25 de mayo de 2 015).

[25]Ley Peruana de Represión de la Cibercriminalidad. T*ítulo V-A sobre Delitos Contra Datos y Sistemas Informáticos*. (Lima, Perú: 2 013) Artículo 208.

2.2.3 Publicidad de los actos de la administración pública

Todos los actos administrativos son públicos, y se puede acceder a ellos en cualquier momento que se requiera, como un derecho esencial a la condición de ciudadano. Al respecto, nuestra Carta Magna establece:

> "Los interesados a obtener, en cualquier momento, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar…o de datos suministrados por particulares bajo garantía de confidencia".[26]

La plataforma de carácter tecnológico estatal, es decir vía internet, páginas de acceso público, proporcionadas por la unidad de ***Gaceta y Jurisprudencia de la Corte de Constitucionalidad*** figura como nuevo sistema de consulta de jurisprudencia constitucional, cuyo objeto es precisamente hacer públicos los actos de la administración del Estado a través de las actuaciones jurisprudenciales digitales.

Países que cuentan con sistemas de publicación y actualización de datos de Sentencias Vía Internet según el Panorama del Derecho Informático en América Latina y el Caribe (CEPAL) Número 39: Argentina, Bolivia, (Estado Plurinacional de), Brasil, Chile, Colombia, Costa Rica, Ecuador, EL Salvador, Guatemala, Paraguay, Panamá, Perú, República Dominicana y Venezuela (República Bolivariana de). Guatemala, cuenta con plataformas especializadas de acceso a la información pública

[26]Asamblea Nacional Constituyente. *Constitución Política dela República de Guatemala*. (Guatemala: Serviprensa, 1 985). Artículo 30.

facilitadas por Corte de Constitucionalidad, en la que la unidad de Gaceta y Jurisprudencia, suministra información referente a expedientes conocidos por la Corte, conforme a lo dispuesto en el Artículo 10 de la ley 57-2008 de *Acceso a la Información Pública*, también a través de los portales o páginas 'informáticac.gob.gt y gacetac.gob.gt'.

2.2.4 Derecho a la privacidad, hábeas data o exhibición de datos

"Decisión de los pobladores de una unidad territorial acerca de su futuro estatuto político".[27]

Conocido en muchos países y desconocido por muchos otros el *hábeas data*, es el derecho que se protege en virtud de ese avance tecnológico. Es en primer lugar, el derecho emergente del uso de alta tecnología, en el que se ve vulnerada la privacidad ante la constante evolución tecnológica. Inició a reglamentarse en algunas legislaciones tanto por leyes especiales de hábeas data, como por leyes de protección de los delitos de alta tecnología, para normar lo referente al contenido de los datos personales que en algunos países, suelen tener un capítulo procesal, en donde se describe el objeto de la acción del hábeas data per se. Dicha legitimación, sea ésta de carácter pasivo o activo, debe incluir la investigación, la prueba y la sentencia respectiva, como en todo delito.

A través de diversos medios de comunicación, los usuarios tienen conocimiento de violación de derechos de contenido

[27]Real Académica Española. RAE. *Hábeas data*. (Madrid, España: Espasa, 2 014.) Consulta electrónica (31 de mayo de 2015).

personal, sin embargo, en Guatemala no existe un programa de capacitación nacional para educar a la ciudadanía sobre lo relativo a la prevención de este tipo de delitos, sobre todo para proteger a las nuevas generaciones; pese a que, son éstos los vulnerables por el desmedido uso y descontrol de las redes sociales. El glosario del departamento de derecho internacional, de la Organización de Estados Americanos, conceptualiza el derecho a la autodeterminación o protección de datos personales como:

Las Propuestas de Declaraciones de Derechos del Ciberespacio y Constituciones, a través de la concepción iusnaturalista de los derechos innatos o derechos naturales, establecen ese pensamiento jurídico moderno ha venido destacando sucesivamente algunos derechos que constituyen la primera y esencial manifestación de la personalidad, a los que denominara precisamente derechos de la personalidad, tratando de construir doctrinariamente, ante la parquedad de los textos jurídicos de Derecho privado, como teoría de la protección básica de la persona, por sí misma y como tal, frente a las invasiones o inmisiones procedentes de la actividad social, ya sean imputables a otros particulares o a los poderes públicos. [28]

Es decir, que aunque no expresa específicamente como un derecho protegido por la constitución, se deduce del contenido en la *Declaración de Derechos del Ciberespacio*, que el derecho de hábeas data, como derecho derivado de la personalidad, es *garantía* que todo ciudadano tiene y debe protegerse ***erga omnes***.

[28]Cfr. ***Beltrán, De Heredia***. C*onstitución jurídica de los derechos de la personalidad*, Madrid, España. 1 976; Citado por Aguilar Guerra, Vladimir. *El significado de la idea persona*. (Guatemala: Serviprensa, 2 005.) 47.

En cuanto al derecho de autodeterminación, los datos que consten en archivos estatales o en el sistema cibernético, según lo contenido en el Artículo 9 de la Declaración de Derechos del Ciberespacio, garantiza que:

1. Todo orden político legítimo en la sociedad de la información, ha de garantizar el hábeas data; es decir, por parte de los ciber-ciudadanos sobre sus datos personales.
2. Para la efectividad del derecho al hábeas data, son ineludibles dos requisitos:
   a. La existencia de una ley formal que contemple ésta cuestión, como objeto directo, más allá de la posible presencia de leyes sectoriales y,
   b. La existencia de unos órganos de control específicos, con potestades de investigación inmediata, que deberán tener garantías de independencia e imparcialidad equivalentes a las del poder judicial.

Así también, se establece que al igual que otro derecho, no es de carácter absoluto. Refiriéndose a que no se debe limitar otros derechos y libertades dignos de protección, y que también tiene ese carácter de derecho fundamental, como lo es el hábeas corpus, como un derecho de todo ciudadano, detenido o preso a comparecer inmediata y públicamente ante un juez o tribunal para que, oyéndolo, resuelva si su arresto fue o no legal, y si debe alzarse o mantenerse, como lo son entre otros: la libertad de la información, libertad de empresa y el bien común. Aunque también es importante, analizar respecto a los derechos que limitan el hábeas data como lo es el derecho individual.

Constituido el Tribunal de Amparo, respecto a los derechos que se tutelan ante la utilización indebida de datos contenidos en archivos o bases de datos. *Expediente* 1356-2006. IV Considerando:

> "Es sabido que en la legislación comparada, y de acuerdo con la doctrina procesal constitucional moderna, la tutela de tales derechos se hace por medio de la acción denominada "Hábeas Data", misma que en Guatemala no ha sido objeto de regulación legal. Ante ese vacío legal, y mientras el mismo concurra en este país, esta Corte sostiene que por la amplitud con la que está estableciendo el ámbito de conocimiento del amparo, este último resulta ser la acción constitucional idónea para garantizar el derecho que a toda asiste de acceder a su información personal recabada en banco de datos o registros particulares y oficiales (observándose, respecto de este último, las situaciones de excepcionalidad contenidas en el artículo 30 constitucional)".[29]

a. Consentimiento expreso

> "Acción y efecto de consentir,…manifestación expresa o tácita por la cual, un sujeto se vincula jurídicamente".[30]

El consentimiento expreso, no es más que la manifestación de voluntad expuesta libremente y habitualmente orientada a determinados actos, contratos o acciones que representan la

[29]Corte de Constitucionalidad. *Amparo*. *Considerando IV. Expediente 1356-2006*.Https:www.rediph.org/documentación/jurídica/common/Guatemala/EXPEDIENTE_1356_2006.pdf. (31 de mayo de 2 015).

[30]Real Academia Española. RAE. *Consentimiento*. (Madrid, España: Espasa, 2 014.) Consulta electrónica (31 de mayo de 2015).

voluntad, mediante la cual el titular del derecho, autoriza el tratamiento de sus datos personales, ya sea en todo o en parte y, para los usos que a éste convengan sean éstos, por medios escritos o tecnológicos.

Auto determinación: Es el derecho o poder que tiene toda persona de decidir sobre el contenido de la información que proporciona en virtud de las diferentes formas de contratación que surgen, limitando lo relativo a aspectos determinados de su intimidad. Comprende además, entre otros derechos básicos:

- El conocer el contenido de la información que de ellas conste en los registros o bancos de datos;
- La forma en que esos registros van a utilizar esos datos;
- La potestad de exigir la actualización del contenido;
- Solicitar la corrección del contenido de los datos en cualquier momento;
- Derecho a la intimidad del contenido de la información proporcionada bajo las condiciones legales, claras, pactadas por las partes respetando los derechos inherentes a cada persona.

En Sentencia del **21.7.03** (Colombia) se ejerció una acción de tutela por la violación al derecho constitucional de hábeas data, autodeterminación informática y la intimidad mediante *spam*, consideradas como unidades básicas de información, cuyos datos almacenados son susceptibles de ser modificados por el titular o parte afectada y, que pasan a formar parte de un archivo especial

como fuente de información de cualquier tipo, sean éstas de carácter individual o natural, colectivas o jurídicas identificables o identificadas, pueden resultar alteradas por programas maliciosos, por lo que deben ser protegidos por el Estado.

b. Violación al hábeas data

La Ley 53-07 *Sobre Crímenes de Alta Tecnología, del Congreso Nacional de la República Dominicana*, establece en su constitución que los derechos y deberes fundamentales de los ciudadanos entre los que se encuentran la libertad de expresión, la integridad e inviolabilidad de la correspondencia y demás documentos privados. Así mismo, que la *Ley General de las Telecomunicaciones* N°. 153-98, del 27 de mayo de 1998, estatuye la obligación de respetar la inviolabilidad de las telecomunicaciones.

En éste sentido, en el segundo considerando, prohíbe el uso de las telecomunicaciones contrario a las leyes o que tenga por objeto cometer delitos o entorpecer la acción de la justicia. Como una forma de limitar el derecho individual sobre el bien común o social, pese a que en la *Ley de Emisión del Pensamiento* en el Artículo 1 se conceptualiza esa libre la emisión del pensamiento en cualquier forma, no obstante, también se regula en la constitución, en el Artículo 35 que quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la Ley. La contravención de los derechos contenidos en el hábeas data, incluyen además de la autodeterminación, el

derecho a la privacidad de los datos contenidos, y al buen uso del tratamiento de los datos, como derecho fundamental del ciudadano.

Asimismo, la Ley Dominicana preceptúa en su tercer considerando, que las tecnologías de la información y de la comunicación han experimentado un desarrollo impresionante, con lo que brindan un nuevo soporte para la comisión de delitos tradicionales y crean nuevas modalidades de infracciones y hechos no incriminados, afectando los intereses patrimoniales y extra patrimoniales de las personas físicas y morales, así como del Estado y las instituciones que lo representan.

El contenido del hábeas data se refiere al ejercicio de una acción derivada de un *Derecho Constitucional*, que tiene cualquier persona cuyos datos figuren en un registro ya sea privado o estatal que figuren en bancos de datos y acceder a tal registro para conocer información vertida sobre su persona y de solicitar la corrección o eliminación de información desactualizada. Así también, puede aplicarse al derecho de solicitar la eliminación de la información considerada obsoleta por el transcurso del tiempo e irrelevancia de su existencia en los registros en que constan. Puede aplicarse al derecho al olvido, es decir, derecho a eliminar información obsoleta, por el transcurso del tiempo o porque ha perdido su efectividad, de conformidad con la Ley y los tratados internacionales.

> "La Ley no amparará el abuso de derecho ni el ejercicio antisocial del mismo, ni el que puedan ejercer los usuarios de la información, sobre todo para obtener un lucro indebido,

> ni el de los titulares de los derechos de propiedad intelectual o industrial, cuando obstaculicen más allá de intereses legítimos el libre flujo de la misma por el ciberespacio*".*[31]

Los derechos de autor, protegidos como derechos patrimoniales, confieren a sus titulares la facultad de disponer sobre sus derechos de transferir total o parcialmente, así como la utilización y aprovechamiento de sus obras en beneficio de terceros. Aún con los avances tecnológicos, éstos derechos son imprescriptibles y protegen la obra durante toda la vida del autor y setenta y cinco años después de su muerte, siendo únicamente transmisibles a sus herederos, sin límite de tiempo y a falta de éstos, al Estado. Así también, el Convenio de Berna, respecto a la protección de obras literarias y artísticas establece lo referente a los derechos protegidos y todo lo referente al uso de ese derecho patrimonial.

Como parte de la 'Convención Jurisdiccional', sobre protección de los derechos de autor y derechos conexos, adoptados en Ginebra el 29 de octubre de 1971, se estableció, por medio de los considerandos, los mecanismos necesarios para tutelar adecuadamente los derechos de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión. Por tal motivo, se hace indispensable el uso de herramientas jurídicas globales, en beneficio de la población vulnerable a la comisión de éste tipo de delitos cibernéticos, que son de impacto social y muchas veces con efectos jurídicos transnacionales.

[31]Congreso de la República de Guatemala. *Ley de derechos de autor y derechos conexos*. *Dto. 33-98*. (Guatemala: Librería Jurídica, 1 998.) Artículo 8.

En la *Ley Electoral Y De Partidos Políticos*, así como el Acuerdo 1-2015 se prohíbe el cambio de dirección, el *Tribunal Supremo Electoral*, no permite cambios o modificaciones en los registros, si no es con seis meses de anticipación a las elecciones electorales, lo que violenta el derecho a la autodeterminación de las personas, al impedir el cambio de dirección contradice la norma constitucional que establece el derecho que toda persona tiene de conocer lo que de ellas conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica ésta información, específicamente la corrección, rectificación y actualización...puesto que la primacía en el orden de aplicación de la Ley, es en éstos casos, lo que en las convenciones respecto a éstas, sin contradecir la de la Constitución, y ésta no fija plazos.

La Constitución Política de la República de Guatemala, establece en caso de la inconstitucionalidad de las Leyes en casos concretos, a través del Artículo 116 que en todo proceso de cualquier competencia, jurisdicción, instancia y en casación, hasta antes de dictarse sentencia, las partes podrán plantear como acción, excepción o incidente, la inconstitucionalidad total o parcial de una ley a efecto de que se declare su inaplicabilidad, el tribunal deberá pronunciarse al respecto.

Nuestro país actualmente cuenta con herramientas jurídicas que han previsto la plataforma electrónica según establece la *Ley de Acceso a la Información Pública*, Decreto Número 57-2008, por lo que, el recurso legal que se encuentra a disposición de todo individuo y que es ignorado es el derecho de *hábeas data,* acción constitucional que puede ejercer cualquier persona que esté

incluida en un registro o banco de datos. Para acceder a tales registros, la persona puede solicitar que le sea suministrada la información existente sobre su persona, así como la eliminación o corrección si los datos tienen información errónea, falsa o desactualizada.

En 2004 la *República de El Salvador* reconoció por primera vez en sentencia emitida por la Corte Suprema de Justicia, como parte de los derechos fundamentales de los ciudadanos salvadoreños. La protección de datos o autodeterminación informativa, derivado de un proceso de amparo constitucional en contra de una empresa que recopilaba y comercializaba información denominada DICOM.

Actualmente la figura del hábeas data sólo puede ser analizada por la misma Corte Suprema de Justicia, al no existir una Ley especial que regule la protección de datos en el Salvador, según el Centro de Documentación Judicial. Según **sentencia 1356- 2006**, el 24 de junio de 2014, el Juzgado Décimo Primero de Primera Instancia Civil, condenó por delitos contra la privacidad, que utilizan los datos de las personas sin previa autorización de los usuarios a las empresas: *Infonet, Digidata y Trans Unión Guatemala S.A*. La acción de amparo fue promovida por el procurador de los derechos humanos, Jorge de León Duque, en contra de tres empresas anónimas dedicadas a la compra y venta de datos personales.

Además de tomar en cuenta los fallos emitidos por la corte, como fuente de derecho para los delitos cometidos contra la privacidad de las personas individuales, se debe tomar en

consideración lo relativo al tratamiento de datos financieros y el apartado especial para referente al hábeas data financiero tomando como referencia el derecho comparado, como la *Ley Colombiana, Decreto 1777*, la Ley 1266-2008 que regulan lo relativo a la seguridad de la información y hábeas data, así como sentencias en este sentido como a manera de ejemplo la sentencia colombiana 1011-2008, y sus aplicaciones tanto en el área pública como en el área privada.

2.3 Derecho penal relacionado con la informática jurídica

En virtud del avance tecnológico que se ha experimentado a nivel mundial, se ha hecho necesario el regular respecto a las nuevas tendencias tecnológicas que directa o indirectamente influyen en la comisión de delitos utilizando medios tecnológicos. En ese sentido, la República del Perú en su *Ley de Delitos Informáticos*, modificó el *Código Penal Peruano* vigente hasta el 12 de septiembre de 2013, con el fin de modernizarlo e integrar a la legislación lo referente a medios tecnológicos como herramientas para la comisión de infracciones a la Ley, para ser tipificados y sancionados. Así mismo, con la implementación de disposiciones legales generalmente se pretende frenar los impulsos criminales, en alguna medida coadyuvar en el marco de la lucha eficaz contra la cibercriminalidad en general.

En éste sentido, *La República Dominicana*, Ley No. 53-07 *Sobre Crímenes y Delitos de Alta Tecnología*, contempla lo relacionado a la propiedad intelectual y afines, refiriéndose también a la propiedad industrial, (ver Ley N° 20-00 del 8 de mayo de 2000) estableciendo

que cuando cometan delitos a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones se establece sanción con penas que se determinen específicas para actos delictivos específicos contemplados en esa Ley, respetos de delitos relacionados con la propiedad intelectual y afines, contenidos en el capítulo III, en el Artículo 25.

Es por ello que en el marco jurídico es indispensable incorporar en Guatemala nuevas herramientas legislativas para ejercer una función coercitiva clara y eficaz, con el fin de evitar en lo posible la comisión de delitos de carácter cibernético en general. Es importancia hacer mención de la necesidad de complementar nuestras leyes con las disposiciones legales extranjeras que han adoptado países con éxito en la aplicación de leyes especiales, para lograr minimizar el impacto de los delitos de carácter cibernético. Así también, en virtud de esa protección de la cual el Estado está obligado, también establece que se debe procurar la seguridad en las nuevas tendencias de contratación, en especial las que se refieren a las que se hacen con el uso de tecnología.

Es importante analizar las actuales disposiciones legales con relación al tratamiento de datos y el apartado especial que se refiere al hábeas data, en las diferentes formas de aplicación del derecho. Además de tomarse en cuenta, las sentencias emitidas por la *Corte de Constitucionalidad* al respecto, como fuente de derecho.

La transgresión al hábeas data es además de un delito penal, un delito de carácter constitucional, al violar los derechos fundamentales de las personas, delito que debe ser tomado en consideración, analizado y tipificado en leyes penales; en virtud del

vacío legal y la necesidad de la creación de un cuerpo legal especializado en ésta materia, no puede ser sancionada en las Leyes existentes, pues son insuficientes para la prevención de fraudes de carácter cibernético. Se debe ampliar en cuanto a la inclusión de nuevas figuras delictivas en relación a los delitos de carácter cibernético, así como lo concerniente a la ampliación de dicha temática tomando en cuenta lo que al respecto se derive del derecho comparado.

El *Estado de Guatemala*, debe favorecer la investigación para que a través de herramientas jurídicas, los legisladores aprueben leyes de urgencia nacional en un término que no violente el debido proceso, debiendo de igual forma, analizar la creación de una legislación especial de aplicación transterritorial sobre delitos informáticos, y realizar un estudio comparativo con personal colegiado idóneo, respecto a los diferentes cuerpos legales, tanto de los contenidos en los países latinoamericanos, como en las disposiciones normativas del bloque de países europeos; para que las herramientas jurídicas que entren en vigencia tengan concordancia con esos cuerpos legales, se debe comparar en especial, los contenidos en países adscritos a los convenios relativos a delitos informáticos.

Algunos cuerpos legales en relación a la protección de éstos derechos cibernéticos son: *Ley Orgánica de Bancos de Guatemala*, Decreto Número 16-2002; *Ley de Derechos de Autor y Derechos Conexos* y sus reformas, Decreto Número 33-98; *Ley de Propiedad Industrial* (rama de la propiedad intelectual) Decreto 57-2000; *Ley de Protección al Consumidor y Usuario*, Decreto Número 473; *Ley de*

Organizaciones No Gubernamentales para el Desarrollo, Decreto 02-2003, no obstante, son insuficientes para contrarrestar los daños informáticos.

En cuanto a la conectividad mundial y al delito cibernético, según la Oficina de Naciones Unidas contra la Droga y el Delito (@UNODC), el consejo de Medellín, Colombia, aprobó la política pública de seguridad como expertos en el estudio y combate del delito cibernético, como por ejemplo: el combate de la corrupción a través de aplicaciones para celular, lucha contra la trata de personas, etcétera.

> "*Cuando de ello dependa el éxito en la colaboración transnacional. Se estima que para el 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70 % de la población mundial. Para 2020 el número de dispositivos interconectados por la red (Internet de las cosas) será seis veces mayor al número de personas, lo que transformará la concepción actual de Internet. En el mundo híperconectado del futuro será difícil imaginar un <delito informático>, o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo internet*".[32]

Respecto a la base de Derecho Comparado, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, en el cuarto considerando establece que la integración al comercio electrónico global requiere que sean adoptados instrumentos técnicos y legales basados en los modelos de legislación

[32]*Organización de las Naciones Unidas. La conectividad mundial y el delito cibernético.* http://www.unodc.org/doments/organizedcrime/UNODC_ CCPCJ_EG.4_2013/2_S.pdf. (25 de mayo de 2 013).

internacional que buscan la uniformización de esta rama del derecho tan especializada, y que debe dársele seguridad jurídica y técnica a las contrataciones, comunicaciones y firmas electrónicas mediante el señalamiento de la equivalencia funcional a estas últimas con respecto a los documentos en papel y a las firmas manuscritas.

Las reformas en materia penal de delitos informáticos contenidas en las legislaciones de cada país, son necesarias y se deben confrontar como urgencia nacional. En cuanto a la necesidad de integrar los diferentes cuerpos legales, en beneficio del uso de herramientas transnacionales en América Latina y El Caribe, según se menciona en el Panorama del Derecho Informático en América Latina y EL Caribe, en la colección de documentos y proyectos número 39, éstos son algunos países que han legislado al respecto:

- **Guatemala**:

  Código Penal- Capítulo VII. De los Delitos Contra el Derecho de Autor, La Propiedad Industrial y Delitos Informáticos

  Código de 1973, reformado en éste capítulo en 1996 y 2000.

  Figuras previstas:

- Tutela derechos de autores (robo, uso y gestión de obras sin la autorización del autor)
- Destrucción de registros informáticos
- Violación a los derechos de la propiedad industrial

  Publicación y Actualización de sentencias por internet

  0%

  Acceso a la información en internet de los tribunales de justicia

  26 %

- **Venezuela (República Bolivariana de)**:

  Decreto 48/2001 Ley Especial Contra Delitos Informáticos.

  Hasta entonces se extendían las tipologías del Código Penal de 1964.

  Figuras previstas:

- Sabotaje
- Daño de Sistemas
- Falsificación de documentos
- Acceso indebido
- Espionaje informático
- Violación de privacidad o de Datos Personales
- Revelación indebida de información personal
- Difusión o Exhibición de material pornográfico adulto o de niños/adolescentes
- Apropiación de propiedad intelectual
- Publicaciones y Actualizaciones de Sentencias en internet[33]

  16,7%

  Acceso a la información en internet de los tribunales de justicia[34]

  62,1%

- **Chile**:

  Ley 19.223 / 1993 Sobre Delitos Informáticos. Ley Especial.

  Figuras previstas:

- Acceso indebido a información contenida en un sistema de tratamiento de la misma
- Destrucción de un sistema informático o alteración del funcionamiento del mismo
- Daño, alteración y divulgación indebida de datos informáticos

[33] Ibíd., 31.
[34] Ibídem., 32.

Nuevo Proyecto de Ley (mensaje del Ejecutivo. Boletín No. 3083-07)

- Falsificación de documentos electrónicos y tarjetas de crédito
- Fraude Informático
- Obtención indebida de servicios de telecomunicaciones
- Publicación y actualización de Sentencias en Internet
  5,5%
- Acceso a la Información en Internet de los Tribunales de Justicia
  77,8%

- **Ecuador**:
  Ley No. 2002-67, de Comercio Electrónico, Firmas y Mensajes de Datos. Ningún instrumento legal específico hace referencia a la tipificación del código.
- Publicación y actualización de Sentencias en Internet
  11,1%
- Acceso a la Información en internet de los Tribunales de Justicia
  35,9%

- **Colombia**:
  Ley 679 de 2001 Sobre pornografía infantil en redes sociales.
  Ley Especial (El Código Penal Colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos informáticos como tales).
  Figuras previstas:
- La explotación
- Pornografía
- Turismo sexual
- Y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio
- Publicación y actualización de Sentencias en Internet

12,5%

- Acceso a la Información en Internet de los Tribunales de Justicia
  46,4%

- **Brasil**:

  Ley 8137(27/12/90), sobre “Crímenes contra el orden económico y las relaciones de consumo”. Ley especial.

  Figuras previstas:

  - Uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la hacienda pública.
  - Publicidad y actualización de Sentencias en Internet
    16,7%
  - Acceso a la Información en Internet de los Tribunales de Justicia
    73,9%

- **México**:

  El Código Penal de México fue reformado con la Ley el 17 de mayo de 1999. El título décimo del *Código Penal*, en la sección sobre “Delitos Contra el Patrimonio”, prevé en el Artículo 217 del referido texto legal al delito informático.

  Figuras previstas:

  - Delito Informático
  - Publicidad y actualización de Sentencias en Internet
    0,0%
  - Acceso a la Información en Internet de los Tribunales de Justicia
    42,2%

2.3.1 Características de los delitos cibernéticos (*delitos de cuello blanco*)

Para tener claro la trascendencia del delito cibernético, es indispensable comprender en primera línea lo concerniente al origen del surgimiento de los delitos conocidos como delitos de cuello blanco. Desde los comienzos de la creación y uso de los registros, se ha evidenciado como consecuencia que el delito *per se*, ha sido cometido por personas de todos los estratos sociales. En 1939 el término '*delito de cuello blanco*'[35] fue acuñado oficialmente para referirse a delitos cometidos por profesionales o empleados del gobierno en el curso de sus trabajos. Se denomina así a los hechos delictivos cometidos por un grupo limitado de personas, con amplios conocimientos informáticos. En estos delitos se tiene como perfil sociológico a personas con un alto nivel académico, sociológico y económico.

La *Ley de Derechos de Autor y Sus Derechos Conexos,* establece en su Artículo 30 que la protección de obras literarias, sin embargo, ésta se amplía tanto en la aplicación de los programas operativos, como en los programas aplicativos, ya sea en forma de códigos fuente o códigos objeto.

Son delitos de características no violentas, generalmente cometidos por personas con amplios conocimientos sobre cibernética, tecnología y en general al uso de los diferentes sistemas cibernéticos y, en virtud del fácil acceso a elementos tecnológicos,

[35] *Delitos de cuello blanco*. https///abogados.lawinfo.com/recursos/ley-criminal/crimen-de-cuello-blanco/delitos-de cuello-blanco.html. (15 de mayo de 2 015).

principalmente en el área laboral en la que se desarrolle o no. Por tal motivo, son considerados delitos de cuello blanco, porque generalmente son delitos cometidos por profesionales en el desarrollo de sus funciones corporativas. De igual manera que otro tipo de delitos, pueden actuar de forma separada o conjunta, es decir puede ser parte de una red de delincuencia considerada como crimen organizado o en forma aislada es decir, individual.

El segundo considerando de la *Ley Contra la Delincuencia Organizada*, Decreto 21-2006 establece que la delincuencia organizada es un flagelo que actualmente ha colocado a los habitantes de la República en un estado de indefensión, por su funcionamiento organizacional, lo que hace necesario la creación de un instrumento legal para perseguir, procesar y erradicar a la delincuencia organizada.

En general, éste tipo de delitos tienen como objetivo principal el uso de esta información que ha sido principalmente sustraída por medios tecnológicos con pleno conocimiento de sistemas operativos y que, tienden a ser plataforma para ser manipulada en la comisión de otro tipo de delitos. Es decir, que la característica de éstos delitos es precisamente el concurso de delitos cibernéticos que necesariamente deben ser analizados. El convenio del Consejo de Europa ha definido cuatro categorías de delitos informáticos, entiéndase cualquier acto cometido dentro del uso de las tecnologías de la información y comunicación, siendo éstas, según el contenido en el proyecto de iniciativa de Ley 4055, sobre delitos informáticos las siguientes:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informativos.
2. Delitos estrictamente informáticos.
3. Delitos relativos al contenido.
4. Delitos relativos a la violación de los derechos de autor y derechos afines.

Es importante hacer una distinción entre las referencias conceptuales de algunos autores respecto a los delitos informáticos, y los delitos cometidos contra la informática en sí, es así que, ***Choclan Montalvo***, respecto de las infracciones patrimoniales de los procesos de transferencia de datos, establece que sigue siendo frecuente, con todo, la distinción de muchos autores entre los delitos relacionados con la informática en cuanto ésta constituye medio idóneo para la realización de los mismos y delitos en los que la informática es objeto del delito o la infracción. Lo que representa nuevos retos jurídico-penales, y nuevas respuestas político criminales.

> Según ***De La Mata Barranco***[36], "en ocasiones nos encontramos con delitos cometidos contra y a través de los sistemas informáticos e incluso un cuarto tipo de delitos en el que podrían incluirse los delitos contra la propiedad intelectual de nuevos bienes de naturaleza informáticos (propiedad intelectual e industrial de programas, nombres de dominio, topografías de productos semiconductores, etc.)."

[36]Norberto Javier, De la Mata Barranco. Los delitos vinculados a las tecnologías de la información y la comunicación en el código penal. Panorámica general, en el delito e informática. Bilbao, España: (Tirant Lo Blanch, 2 007). 49

El autor expone además, lo referente a la clasificación utilizada a fin de poder ofrecer una sistemática visión lo más completa y adecuada posible de los delitos relacionados a las Tecnologías de la Información y la Comunicación (TIC), delitos que deben ser vinculados en disposiciones penales guatemaltecas, como medios persuasivo, para minimizar los efectos jurídicos de la trasgresión al derecho informatico patrimonial en general.

> ***Carrasco Andrino, M. M***[37]., "al describir lo referente a los delitos vinculados a las Tecnologías de la Información y Comunicaciones (TIC), contenidas en el código penal español, establece que ésta expansión y dependencia social de las TIC, las que hacen que un ataque a ellas, deba ser considerado en sí mismo como un ataque a un nuevo bien jurídico colectivo. Cuando se daña un sistema informático concreto, no solo se daña un bien jurídico individual, sino que se generan riesgos para toda la comunidad de usuarios".

2.3.2 Delitos contra los datos personales y delitos informáticos

Muchos países, han analizados y categorizado los diferentes tipos de delitos cibernéticos, pese a que es difícil reconocerlos e identificarlos por el complicado mundo de la cibernética y sus diferentes aplicaciones en: sistemas, programas, redes sociales y aparatos tecnológicos entre otros. Con respecto a la protección de los datos personales, y considerando la inmersión de la tecnología en la vida

[37]M.M, Carrasco Andrino. *El acceso ilícito a un sistema informático*. https://www.Pcbjuridico.com/docs/libros/la-adecuación.pdf. (21 de mayo de 2 015).

cotidiana, en la sociedad cada vez cambiante y más inclinada al uso de herramientas tecnológicas, es necesario ampliar los conceptos legales contenidos en leyes existentes para adaptarlos al actual contexto del mundo digital. En virtud de que, en nuestro país ya existe regulación en cuanto a la contratación electrónica; es decir, comercio electrónico, se hace necesario ampliar el contenido de la ley penal.

En el segundo considerando del *Proyecto de Iniciativa de Ley de Delitos Informáticos*, 4055, se manifiesta que por la naturaleza de los actos de Cibercrimen y que son delitos transfronterizos, se complica la aplicación de las actuales normas del código penal.

Así también, es necesario analizar métodos de detección de delitos informáticos y crear una ley especial para prevenir y sancionar delitos de naturaleza informática que puedan afectar el objeto o materia de la normativa de comercio electrónico y todos aquellos ilícitos de naturaleza informática. El delito informático implica actividades criminales que, en un primer momento, los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como: robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera; sin embargo, debe destacarse que el uso indebido de los aparatos tecnológicos, es lo que ha propiciado esa creciente necesidad de regular al respecto.

- **Delitos contra datos personales:** El simple hecho de sustraer, modificar, destruir, eliminar, compartir, desclasificar, manipular, difundir o dar otro uso, a la base de datos o registro de datos, contenidos en un equipo de cómputo o la acción de modificar la firma electrónica, archivos, documentos, fotografías, y todo contenido en un sistema computacional, sea éste de uso privado o público o de los derechos contenidos en archivos de redes sociales, sin el consentimiento del titular del derecho, encuadra en la comisión de delitos contra datos personales.

Por ejemplo*: el* ***Phishing Symantec***[38] puso en funcionamiento un grupo de equipos conocidos como ***"Honeypots",*** que constituyen una red de sistemas que se han hecho vulnerables a fin de capturar y estudiar ataques reales. La información obtenida se utiliza en actividades de investigación y para mejorar los productos de Symantec. Dicho sistema capturó un ataque de phishing estereotipado dirigido a **eBay,** el servicio de subastas en internet. El sitio web fraudulento, fue eliminado antes de que ningún usuario pudiera visitar el sitio y resultara víctima de la estafa, pues el portal de internet tenía gran similitud con la versión auténtica.

- **Delitos informáticos:** Se pueden mencionar: acceso no autorizado a servicios informáticos, amenazas y difamación, fraudes financieros o phishing, fraudes y abusos

[38] *Por el combate regional de los delitos informáticos*. http://www.prensalibre.com/internacional/CrecedelitocibernéticoOEA_0_913108723.html.Subido el 30 de marzo de 2012. (25 mayo de 2015).

de confianza, pornografía infantil, robo de secretos industriales, robo de servicios, robo o hurto de software, sabotaje informático entre muchos otros.

> "En cuanto a la legislación relativa al delito cibernético, en comparación con la legislación vigente, la legislación nueva o prevista en esta materia trata principalmente de las medidas de investigación, la jurisdicción, las pruebas electrónicas y la cooperación internacional".[39]

El Artículo 30 de la *Ley de Derechos de Autor y sus Derechos Conexos*, establece que los "programas de ordenador se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos, como a los programas aplicativos, ya sea en forma de código fuente o código objeto, y cualquiera que sea su forma o modo de expresión. La documentación técnica y los manuales de uso de un programa gozan de la misma protección prevista para los programas de ordenador".

2.3.3 Conceptos

De las definiciones contenidas en diccionarios jurídicos, *Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas*, decreto 47-2008, las contenidas en la

[39]La conectividad mundial y el delito cibernético. http://www.unodc.org/doments /organizedcrime/UNODC_CCPCJ_EG.4_2013/2_S.pdf. (25 de mayo de 2 015).

Ley 53-07 *Sobre Delitos de Alta Tecnología, y Ley de Derechos de Autor y Derechos Conexos*, Decreto Número 33-98; los conceptos más significativos relacionados con lo referente a la terminología informática y necesarios para la comprensión de los derechos personales que se protegen, cabe destacar los siguientes:

Acceso ilícito: El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él.

Clonación: Duplicación o reproducción exacta de una serie electrónica, un número o sistema.

Código de identificación: Información clave o mecanismo similar, que identifica a un sistema de información que permite el acceso privado y protegido por dicho sistema.

Códigos fuente o código objeto: Los programas de ordenador se protegen en los mismos términos que las obras literarias.

Computadora: Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y /o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole,

incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma. Las computadoras también pueden llegar a efectuar falsificación de documentos de uso comercial y no comercial.

Datos: Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, video, voz, sonido, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil con tales fines.

Delito de alta tecnología: Aquellas conductas que atenten a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

Derechos humanos: Se le conoce como derechos humanos individuales, y tiene tres características: a) Imponen al Estado la obligación de respetarlos; b) los titulares son, en el caso de los derechos civiles, los ciudadanos en general y en el caso de los derechos

políticos el ciudadano en ejercicio, como violación al derecho de autodeterminación informativa; y c) son reclamables en todo momento y lugar y no está sujeto a variación de factores sociales o políticos.[40]

Desvío de servicios: Se produce cada vez que se conectan irregularmente las facilidades internacionales a la red pública conmutada para terminar tráfico.

Dispositivo: Objeto, artículo, pieza, código, utilizado para cometer delitos de alta tecnología.

Emisión: La difusión directa o indirecta por medio de ondas hertzianas, cable, fibra óptica, o cualquier otro medio de sonidos o sonidos sincronizados con imágenes para su recepción por el público.

Falsificaciones informáticas*:* Cuando se alteran datos de documentos almacenados en forma computarizada y sin el consentimiento del titular.

Firma electrónica: Los datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica.

[40]***Zenteno Barillas***, Citado por Carlos Larios Ochaita***.*** *Derecho internacional público*. Instituto de investigaciones jurídicas y sociales. (Universidad de San Carlos de Guatemala. Guatemala: F&G Editores, 2 001.) 34.

Firma electrónica avanzada: la firma electrónica que cumple los requisitos siguientes:

a. Estar vinculada al firmante de manera única;

b. Permitir la identificación del firmante;

c. Haber sido creada utilizando los medios que el firmante puede mantener bajo su exclusivo control;

d. Estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable.

Firmante: Es la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Iniciador: Toda parte que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar una comunicación electrónica antes de ser archivada, si ese es el caso, pero que no haya actuado a título de intermediario con respecto a esa comunicación electrónica.

Intercambio electrónica de datos (IED): La transmisión electrónica de una información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.

Fuente de la información: Es la persona, entidad u organización que recibe, conoce datos personales de los titulares de la información en virtud de una relación comercial, servicio, banco de datos o de cualquier otra índole que, en razón de previa autorización legal o emergida

directamente del titular del derecho, suministra esos datos a un operador de información, que a su vez, entregará al usuario final. *Ejemplo: Los bancos*.

Hábeas data: Acción constitucional que puede ejercer cualquier persona que estuviera incluida en un registro o banco de datos, para acceder a tal registro y que le sea suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad. La frase legal se utiliza en latín, cuya traducción más literal es <tener datos presentes> siendo "hábeas" la segunda persona singular del presente de subjuntivo del verbo latino "habére" (en este caso entendido como <tener>).

Hábeas data financiero: Acción constitucional que puede ejercer cualquier persona jurídica incluida en un registro o banco de datos.[41]

Herramienta jurídica: Término que hace referencia a las normas jurídicas en general, acuerdos, decretos o documentos jurídicos que utilizan los operadores de justicia en el desempeño de sus funciones.

[41] **Ley Colombiana** Dto. 1777. *Seguridad de la información y hábeas data*. Constitución Política de la República de Colombia. Hábeas data financiero. (Sentencia 1011-2008; Ley 1266-2009). https//*www.Velascocalle.co.* (25 mayo 2 015). Artículo 15.

Operador de la información: Es la persona, entidad u organización que recibe la fuente de datos personales, sobre varios titulares de la información, los administra y los pone a disposición o en conocimiento de los usuarios, bajo los parámetros establecidos en la norma jurídica; por ejemplo: El uso de la información de las tarjetas de crédito.

Sistema operativo: Programa especial que se carga en un computador luego de ser encendido y cuya función es gestionar los demás programas o aplicaciones, que se ejecutaran en dicho computador como, por ejemplo, un procesador de texto, hoja de cálculo, la impresión de un texto en una impresión o una conexión a internet.

Titular de la información: Es la persona natural o jurídica a quien se refiere la información que se confiere en un banco de datos y que se encuentra sujeto al derecho de *Habeas Data.*

Usuario: Es la persona natural o jurídica, que puede acceder a información personal suministrada por el operador, la fuente o directamente por el titular de la información.

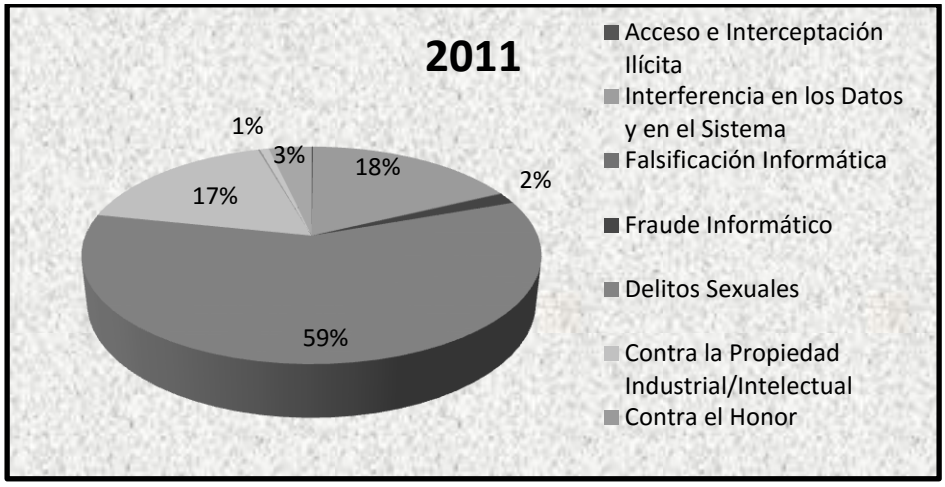
2.4 Convenio de Budapest

El *Convenio de Budapest*,[42] entró en vigencia el 1° de julio de 2004 y en su redacción participaron los 41 países miembros del consejo Europeo, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica. Es considerado como el primer instrumento supranacional sobre la materia y herramienta internacional contra la cibercriminalidad; determinado a coadyuvar en forma conjunta con los países firmantes a garantizar la prevalencia de las garantías mínimas para la protección de los derechos fundamentales de privacidad y lo referente al derecho de autodeterminación ya sea individual o colectiva, contenida en la Constitución de cada nación. Por medio del convenio se pretende la protección del derecho al *hábeas data* o derecho autodeterminación informativa de la privacidad de los datos personales.

La prevención a las transgresiones de los derechos humanos fundamentales, cometidos por medios tecnológicos sean éstos directos o indirectos deben ser tipificados y constar en herramientas legales específicas, para establecer medios coercitivos eficaces, efectivos y congruentes con las disposiciones legales, tanto en los países desde donde se realice el acto delictivo, como en el país en donde tenga sus efectos. Debe ser analizado y discutido el impacto social de éste tipo de delitos para determinar los tipos o figuras delictivas que sea necesario establecer, y evitar la comisión de delitos cibernéticos en el futuro.

[42] *Convenio sobre cibercriminalidad Budapest*. https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf. (23 de mayo de 2 015).

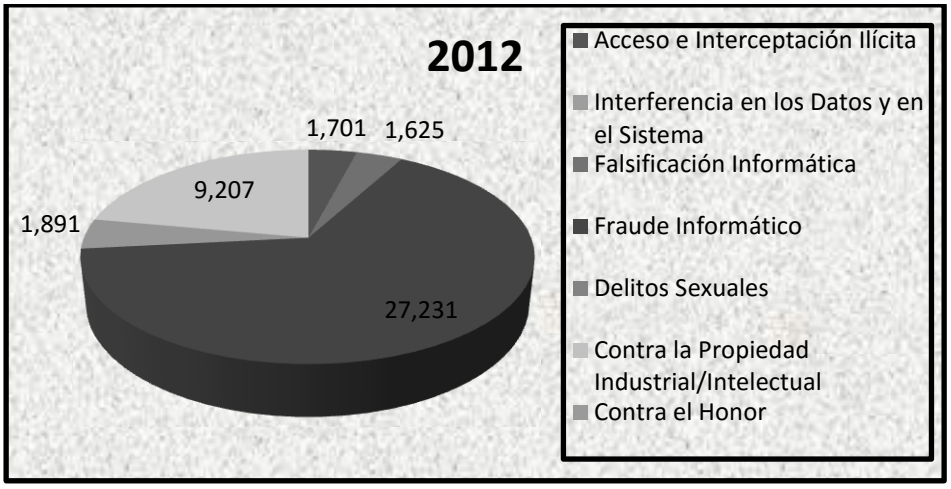
GRÁFICA 1
CIBERCRIMINALIDAD
SEGÚN CONVENIO DE BUDAPEST



Fuente: Cibercriminalidad Ministerio del Interior. Disponible en la siguiente dirección:http://www.interior.gob.es/prensa/noticias//asset_publisher/GHU8Ap6ztgsg/content/id/2037736. (25 de mayo de 2 015).

En los inicios del año 2011, según los datos estadísticos obtenidos del reporte presentado en el convenio, se observaron importantes transgresiones a los derechos fundamentales generados a través de ordenadores, lo que provocó cierto escepticismo en cuanto al uso de los aparatos tecnológicos. Según lo reportado por el *Convenio de Budapest*, hubieron **37, 458** denuncias. Entre las más relevantes cabe destacar que el 59 % de las denuncias se refiere a delitos sexuales, el 18% relacionados a interferencia en los datos y en el sisma operativo, el 17% delitos contra la Propiedad Industrial e Intelectual. Debido a su alcance, los crímenes cibernéticos deben ser categorizados como prioridad en la persecución penal y, en especial debido al constante avance e innovaciones en cuanto a las formas de comisión de los delitos cibernéticos.

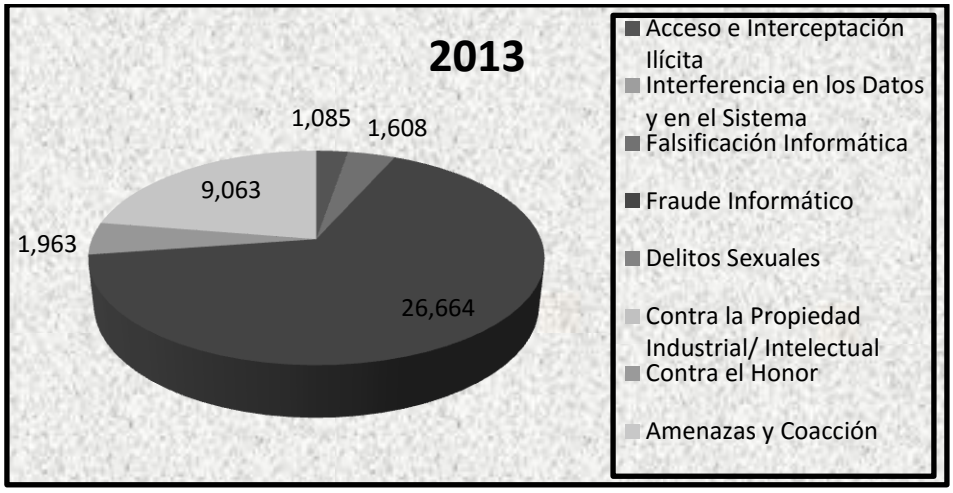
GRÁFICA 2
CIBERCRIMINALIDAD
SEGÚN CONVENIO DE BUDAPEST



Fuente: Cibercriminalidad Ministerio del Interior. Disponible en la siguiente dirección:http://www.interior.gob.es/prensa/noticias//asset_publisher/GHU8Ap6ztgsg/content/id/2037736. (25 de mayo de 2 015).

Estos comprenden los datos sobre el número de infracciones penales reportadas o denunciadas, cabe destacar que constituyen un 65% es decir representan **42, 855** denuncias, de las conocidas por las naciones participantes, hasta el 2012. El problema de la ciberdelincuencia es que al no estar regulado se va haciendo más frecuente y un daño directo a los derechos ciudadanos a nivel mundial, pues como se indica en el gráfico se reportaron 27, 231 denuncias de delitos sexuales; 9,207 denuncias sobre interferencia de datos y en el sistema; así también, 1,625 denuncias relacionadas con falsificaciones informáticas; 1,891 sobre delitos contra el honor; mientras que 1,701 de las reportadas son delitos contra la propiedad industrial/intelectual. Es preciso hacer mención que no todos los usuarios denuncian ante las autoridades, lo que podría elevar las cifras a un número considerable.

GRÁFICA 3
CIBERCRIMINALIDAD
SEGÚN CONVENIO DE BUDAPEST



Fuente: Cibercriminalidad Ministerio del Interior. Disponible en la siguiente dirección:http://www.interior.gob.es/prensa/noticias//asset_publisher/GHU8Ap6ztgsg/content/id/2037736.(25 de mayo de 2 015).

De los delitos reportados, como violaciones a los derechos fundamentales, en 2013 las denuncias se elevaron a **42.437**, de las que fueron reportadas 26, 664 conciernen en especial al de fraude informático; 9, 063 de las denuncias fueron de amenazas y coacción; 1,963 denuncias contra el honor; 1,608 se refieren a falsificación informática; y 1, 085 denuncias sobre acceso e interceptación ilícita. A pesar que en los países europeos existe una cultura de denuncia y leyes en contra de delitos cibernéticos, entre los años comprendidos de 2010 al 2013, se reportaron **122,785** denuncias relacionadas a delitos informáticos. Siendo que en América latina no ha habido un estudio específico al respecto, existe expectativa en cuanto a las cifras a reportase.

2.4.1 Antecedentes y alcances normativos

En virtud de que en nuestro país ya existe regulación sobre el comercio electrónico, según el contenido de la *Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas*, se hace necesario emitir una Ley especial para prevenir y sancionar los delitos de naturaleza informática, que puedan afectar el objeto o materia de la normativa de comercio electrónico y todos aquellos actos ilícitos de naturaleza informática. El *Código Penal*, en cuanto a la reforma del Capítulo VI, de los *Delitos Contra El Derecho de Autor, La Propiedad Industrial y Delitos Informáticos*, reformado por el Artículo 12 del Decreto 33-96, es insuficiente para proteger los derechos de los ciudadanos, ante los delitos de carácter cibernético.

Los delitos cibernéticos, frecuentemente tienen implicaciones de seguridad nacional y de procedimientos de inteligencia, lo cual implica la colaboración nacional e internacional en algunos casos. El uso de instituciones que coadyuven en la colaboración de la búsqueda de mecanismos para erradicar los efectos de la comisión de los delitos cibernéticos, es prioridad en cada nación, para ello es necesario crear una red de investigación con el apoyo de normas especializadas que regulen lo referente a dicha materia.

> "Cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada".[43]

[43]Organización de las Naciones Unidas. *Manual para la prevención y control de delitos informáticos*. (Washington, USA: ONU, 2 012.) 3.

El *informe global*[44] de la corrupción realizada en 2007 de *Transparency International*, reveló que América Latina mostraba los niveles más altos de desconfianza en el poder judicial. Esa incapacidad de los sistemas judiciales para sancionar a quienes cometen delitos, en algunos países fomenta la percepción de impunidad de los sectores poderosos, la sensación de inseguridad entre los ciudadanos comunes y un menor interés por parte de los inversionistas extranjeros, lo que genera una clara inestabilidad económica y caos eventual en cuanto a las contrataciones en general. Guatemala tiene una percepción de índice de corrupción de 115 %.

2.4.2 Países que se han suscrito al convenio de Budapest

Actualmente el **Convenio de Budapest** no se encuentra vigente en ningún país de América Latina y el Caribe, aunque no se ha limitado la participación a los miembros del consejo de Europa, aún no se ha aprobado para Latinoamérica, en virtud del silencio y a que ningún país se ha adherido al protocolo. Sin embargo, América Latina ha desarrollado estrategias para prevención frente a la delincuencia cibernética, con la Estrategia Iberoamericana Integral para combatir amenazas a la "**Seguridad Cibernética**" adaptada por la Asamblea General de la Organización de Estados Americanos (OEA) en 2 004.

[44] *Informe global*. www.Transparency.org. (23 de mayo de 2 015).

> "La Organización de Estados Americanos, tiene por finalidad coadyuvar al cumplimiento de las obligaciones internacionales de los Estados americanos en lo concerniente a la protección de los derechos humanos, así como al cumplimiento de las funciones que en este ámbito tiene atribuidas los distintos órganos de la OEA ("otros tratados objeto de la función consultiva de la Corte, artículo 64 Convención americana de Derechos Humanos.)".[45]

Las nuevas formas de cooperación internacional incluyen la extradición, la asistencia jurídica recíproca, el reconocimiento recíproco de la sentencia extranjera y la cooperación oficiosa entre policía y policía; no obstante, debido a que algunos países no se adhieren a los convenios contra problemas específicos que la comunidad mundial observa en beneficio de las naciones, muchos delitos con carácter transfronterizo no son perseguidos adecuadamente y es motivo de contravención a normas de países que generalmente se ven afectados por la comisión de un hecho delictivo.[46]

El Convenio de Budapest fue oficialmente redactado por los 43 (*ha sido ratificado por 20*) países miembros del Consejo de Europa, junto con Estados Unidos de América, Canadá, Japón y otros que participaron como observadores. Se propone fundamentalmente:

[45]Corte Interamericana de Derechos Humanos. (Washington, USA: OEA, 1 982.) 82.

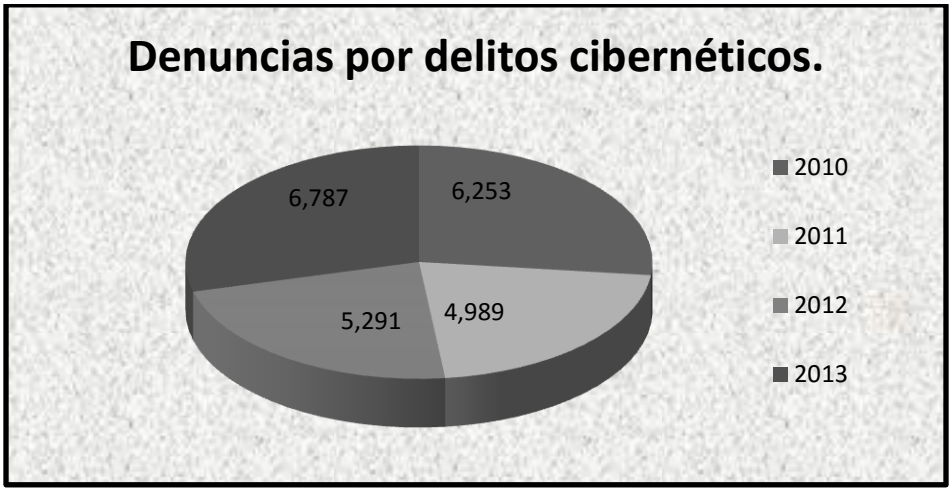
[46]*La conectividad mundial y el delito cibernético*. http://www.unodc.org/doments/ organizedcrime/UNODC_CCPCJ_EG.4_2013/2_S.pdf. (25 de mayo de 2 015).

1. Incluir una relación de delitos que cada Estado miembro debe considerar como tales. El tratado tipifica como delitos a las infracciones de piratería, la producción, venta o distribución de herramientas de piratería, la pornografía infantil y una lista amplia de infracciones de la propiedad intelectual (Artículos 2-11).

2. Requiere que todos los Estados signatarios concedan nuevos poderes de búsqueda e intervención a las autoridades policiales, incluida la facultad de exigir a los servidores de internet que preserven los registros de uso de internet de cada ciudadano u otros datos, y la facultad de controlar en tiempo real las actividades en línea de los ciudadanos. (Artículos 16-22).

3. Requiere también el cumplimiento de la ley en todos los países participantes de manera que estos cooperen con los cuerpos de policía de otros países participantes ante una "*solicitud de asistencia mutua*" de la policía de otro país "*en la mayor medida de lo posible*" (Artículos 23-35).

GRÁFICA 4
SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE



Fuente: Tendencias de seguridad cibernética en América Lanita y el Caribe. Disponibleen:http://www.symantec.com/content/es/mx/Enterprise/other_resources/b-cybersecurity-trends-report-lamc.pdf. (25 de mayo de 2 015).

En América Latina, se observa una creciente en los índices de Ciberdelincuencia, las tendencias en cuanto al avance de éste tipo de delitos son preocupantes, en total se ha reportado la cantidad de vulnerabilidad global de **23,320** usuarios, por medio de denuncias efectuadas entre los años comprendidos del 2010 al 2013, pero no existe una regulación integral o norma que prevenga, no sólo los delitos cibernéticos en las naciones, sino, las que se creen como herramienta legal de asistencia mutua entre naciones, para evitar la incidencia de aquellos delitos que, por la facilidad de su comisión, como lo son los delitos de carácter cibernético, son difíciles de detectar y favorecen al crimen organizado.

CAPÍTULO 3
FRAUDE CIBERNÉTICO

3.1 Antecedentes

Guatemala no cuenta con un plan de respuesta a una crisis cibernética que afecte a la ciudadanía. Tan solo en 2012, la Procuraduría General de la Nación conoció 259 denuncias, violentándose derechos como: la intimidad, libertad de acción, autodeterminación y comercialización de datos sensibles. Así también, fraudes realizados por hackers a bancos afectando a usuarios tanto dentro como fuera de nuestras fronteras. En Guatemala, empresas señaladas de vulnerar este tipo de garantías son: Infonet, Digidata y Trans Unión Guatemala, S.A. utilizando datos personales, sin previa autorización del usuario afectado, la acción de amparo fue promovida por el procurador, siendo emitida la sentencia el 24 de junio de 2014 en el Juzgado Décimo Primero de Primera Instancia Civil.[47]

En América Latina, “se está experimentando una expansión de la cooperación internacional centrada en la seguridad y el desarrollo, incluyendo la seguridad ciudadana”.[48]

---

[47]Corte de Constitucionalidad, *Amparo. Expediente 1356-2006. Considerando IV*.https//www.redipd.org/documentación/jurídica/common/Guatemala/EXPEDIENTE_1356_2006.pdf. (15 mayo 2 015).

[48]*Revisión de la cooperación de seguridad ciudadana en América Latina*. https//www.Ciprevica.Org. (15 de mayo de 2 015).

Aquellos delitos aún no tipificados como tales como los cibernéticos, en cualquier ordenamiento jurídico producen inestabilidad social, económica, jurídica además de anarquía y se tiende a facilitar el crimen organizado haciendo evidente un problema de protección a la seguridad ciudadana en virtud de una laguna legal.

> "Por la naturaleza de los actos de Cibercrimen y que son delitos transfronterizos, se complica la aplicación de las actuales normas del código penal, lo que se traduce en lagunas legales que permiten al delincuente realizar actos ilícitos por medio de las nuevas tecnologías de la información".[49]

Los casos más comunes registrados en países que utilizan tecnología de información o internet, son esencialmente a través de los correos electrónicos, ya que al momento de ingresar a sitios web o páginas no seguras, la simple descarga de programas, música o juegos de video on line, los hace vulnerables de ser víctimas de delitos cibernético. Estos delitos se cometen a través de programas invasivos denominados Malware, que infectan los sistemas operativos de cómputo, causando daños a los usuarios que habitualmente acceden a éstos sitios. También pueden ser cometidos a través de páginas web que simulan ser banca virtual de bancos reconocidos en el país, utilizando falsas entradas de apariencia segura, en la que solicitan a los usuarios el cambio de códigos o información específica.

---

[49] Hugo, Morán. *Proyecto de ley de delitos informáticos. Decreto 4055*. (Guatemala: Editorial jurídica, 2 010.) 17.

La *Constitución Española,* (Artículos 197-201) sobre la libertad de los ciudadanos y el delito informático, que el ataque se produce contra la intimidad e infracciones a la propiedad intelectual (Artos 270-287). ***Rafael Calvo***, define el delito informático como:

> "La realización de una acción que reuniendo la características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra derechos y libertades de los ciudadanos*".*[50]

Es necesario tomar en cuenta, la utilización de las nuevas plataformas tecnológicas como lo son las redes sociales, el automatismo de nuevas tendencias especializadas en los usos cotidianos, y en general, al surgimiento de nuevas formas de comercio y contratación en la aplicación de éstos medios tecnológicos a las instituciones profesionales. Es necesario implementar herramientas jurídicas técnicas, en consecuencia de ese constante flujo tecnológico, tendencias e instrumentos jurídicos aplicables en beneficio de mutua cooperación internacional; que eventualmente puedan ser de fácil acceso y en beneficio de los ciudadanos para la aplicación del derecho, sea éste de carácter público o privado, nacional o internacional.

Pajuelo Bertrán[51], en su "Ensayo *Crítico de la Gestión Dogmática del Bien Jurídico Tutelado en los Delitos Cibernéticos"*, establece que estos nuevos delitos tecnológicos evolucionan, poniendo en riesgo a las

---

[50] Rafael, Fernández Calvo. Constitución española. *Libertades de los ciudadanos, delito informático*. *Instauración de un marco legal en internet.* https://books.google.com.gt. (Madrid, España: 1 978). 283

[51] Carlos Alberto, Pajuelo Bertrán. *Ensayo crítico de la gestión dogmática del bien jurídico tutelado en los delitos informáticos en el Perú*. (Lima, Perú: Sunat, 2 012). 325.

infraestructuras gubernamentales, por lo que se buscan la colaboración mutua entre gobiernos para la lucha y prevención del crimen organizado y en especial el tecnológico.

Asimismo, esa dogmática penal establece que para que un acto realizado por el hombre, sea considerado un hecho delictivo, debe llevar inmerso el proceso o fases de la criminalización, utilizando esa terminología coloquial de alarma social, en la que se observa las fases de criminalidad primaria y secundaria en prevención de actividades tecnológicas ilícitas. En éste sentido, enuncia ***Claus Roxin*** citado por Pajuelo Bertrán:

> "No se debe perder a la solución social de conflictos como el eje de la función político criminal de la antijuricidad, para lo cual el legislador debe ceñirse a un número limitado de principios ordenadores".[52]

El *Código Penal,* establece lo referente a los delitos contra el patrimonio, los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos.[53] En consecuencia, las disposiciones penales normativas, han tipificado algunas figuras delictivas relacionadas con los delitos tecnológicos, entre ellos los cometidos sin autorización:

- Destruir, borrar o inutilizar registros informáticos;
- Alterar, borrar o inutilizar las instrucciones o programas que utilizan las computadoras;

---

[52] Ibíd.,

[53]Congreso de la República de Guatemala. Código penal guatemalteco. *De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos. .Decreto número 17-73, incisos A-G. Reformado por el artículo 12 del decreto 33-96*. (Guatemala: Librería jurídica, 1 998.) Artículo 274.

- Copiar o reproducir instrucciones o programas de computación sin consentimiento;
- Crear bancos de datos o un registro informático, con datos que puedan afectar la intimidad de las personas;
- Utilizar 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 o alterar los estados contables o la situación patrimonial de una persona física o jurídica;
- Utilizar los registros informáticos de otro o ingresar por cualquier medio a su banco de datos o archivos electrónicos;
- Destruir o poner en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

Con penas de prisión que van desde los 6 meses a 5 años y multas que van desde 200 a 3000 quetzales. Siendo la sanción un medio de coerción, las penas deben ser mayores para éste tipo de delitos; no obstante, lo preceptuado en el último párrafo del Artículo 274 literal “A”, en los casos en que la prestación de servicios fueren de carácter público o se trate de un registro oficial, se eleva la pena en un tercio, sin embargo, se debe analizar al respecto y evaluar la creación de un estatuto especial, que regule lo referente a los delitos informáticos, pues las leyes existentes son insuficientes para los delitos cibernéticos actuales, en virtud de ser la tecnología un elemento cambiante, es necesario también evolucionar en la creación de herramientas jurídicas.

Según la Concepción Finalista, la acción es esa conducta humana dirigida por la voluntad hacia un resultado concreto, es decir, la norma castiga la manifestación de la acción como rasgo secundario de una

contravención. Pero existe también, el castigo a la simple manifestación de la acción, como rasgo primario, por ejemplo: la tentativa. Sin embargo ese efecto no se da en todos los delitos. El sujeto de la acción, siempre es el ser humano, no existe otro ser sujeto de la acción, entonces, si no es ser humano, no puede ser considerado como delito. El delito evoluciona utilizando medios tecnológicos programados para la comisión de hechos delictivos, que no encuadran en la concepción de la acción, según ésta teoría entonces, los fraudes cibernéticos programados mediante malwares, al no estar tipificados, no son delitos.

El *Código Procesal Penal Italiano*, preceptúa lo referente al fraude procesal, pero para que exista ésta figura, debe constar una actuación judicial o administrativa ante los correspondientes funcionarios, dentro de los cuales debe resolverse algún asunto jurídico. Aunque no se encuentra regulada en nuestro ordenamiento jurídico, es importante hacer notar la necesidad de regular al respecto, para evitar fallas en la administración de justicia, respecto a la creación de la Ley contra el fraude cibernético, regulando lo referente al manejo de datos y la prueba cibernética. En dicha norma se define el fraude procesal de la siguiente manera:

> "EL perito que, en la ejecución de un dictamen pericial, o el que, en el curso de un proceso civil, administrativo o penal, o anterior a éste último, cambien artificiosamente el estado de lugares, de personas o de cosas, con el fin de engañar al juez en una diligencia de inspección o reconstrucción judiciales, serán castigados, si el hecho no tuviere previsto como infracción por alguna disposición legal especial, con reclusión de 6 meses a 3 años".[54]

[54] Código penal italiano. Fraude procesal. https://www.juareztavares.com /textos/codigoitaliano.pdf. (11 de junio de 2 015) Artículo 374.

3.2 Fraude cibernético

A diferencia de lo tipificado en el *Código Penal*, respecto a los delitos tradicionales contra el patrimonio, los diferentes tipos de fraude cibernéticos que se pueden ejecutar, no se encuentran regulados en nuestro ordenamiento jurídico, no obstante, a las reformas contenidas por el Decreto 48-95 del Artículo 274, reformado por el Artículo 3. Si bien es cierto, se hallan regulados en otros cuerpos legales de derecho comparado, es necesario que integren una ley especial. Los presupuestos ilícitos que se encuentran regulados tienen la misma apariencia que la estafa o el fraude, es por ello que, el juez penal se ve en la necesidad de aplicar sanciones relativas a la estafa, hurto o fraude para emitir su fallo, aunque el daño cometido merezca una sanción mayor. Es usual observar fraudes a cajeros automáticos, bancarios, a usuarios sean éstos de carácter público o privado, entre otros, cometidos utilizando medios científicos para realizar el delito.

La informática, como ciencia o técnica ha permitido facilitar la aplicación de sistemas tecnológicos en beneficio de otras ciencias, a través del uso de medios especializados. Cabe destacar que no obstante, los numerosos beneficios generados con el uso de medios técnico científicos y los beneficios sociales que han experimentado las sociedades, los índices de Ciberdelincuencia van en constante aumento. Por lo tanto, el derecho debe enfrentarse a estos cambios generados por el uso constante de la tecnología y por consiguiente debe regular lo concerniente a los límites del derecho del uso de esa tecnología, en beneficio del derecho social. Es importante el realizar un análisis entre los efectos de los delitos que se cometen utilizando medios tecnológicos, de los que no, y establecer la dimensión del daño causado.

Para su comprensión y clasificación, es necesario definirlos:

- **Fraude**[55]: (D.P.) “Equivale a engaño, que consiste en cualquier falta de verdad debida a simulación entre lo que se piensa o se dice o se hace creer, instigando o induciendo a otra persona actuar en la forma que interesa, o en la falta de verdad en lo que se dice o se hace”.

- **Fraude de Ley**: (D.CI.) Vulneración de la norma jurídica al amparo, aparente, de otra norma o disposición diversa.

- **Definición Legal***:* El que engañando a uno o aprovechándose del error en que este se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido. Al igual comete delito de fraude genérico al que engañando a uno o aprovechándose en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro.

> ***Camacho Losa***, (1987) define el fraude cibernético como: “Toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito.”[56]

De esta manera, expresa el autor que esa acción dolosa, que provoca un perjuicio a personas o entidades, no necesariamente conlleva un beneficio material para su autor, o que, al contrario, produzca un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen de forma activa dispositivos habitualmente utilizados en las actividades informáticas.

---

[55] Diccionario Jurídico Espasa. *Fraude*. (Madrid, España: Escalpe, 1 999.) 434.

[56] Congreso de la República de Colombia. *Delitos informáticos y entorno jurídico en Colombia (ISSN 0123-1472, Vol. 11 No. 28)*. (Bogotá, Colombia: Editorial jurídica, 2 010.) 12.

> "***Casanoba, Romeo***[57], detalla que el fraude informático es la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero".

Los elementos constitutivos de fraude según ***Camacho, Losa***[58] son:

- **Sujeto activo**: Quien comete el fraude.
- **Medio**: Se refiere al sistema informático.
- **Objeto**: Es el bien que produce el beneficio ilícito.
- **Sujeto pasivo**: La víctima.

Según lo que refiere el autor, es evidente que lo que caracteriza al fraude informático, es el medio a través del cual se comete, la computadora. En la actualidad, se están utilizando otros medios tecnológicos para cometer delitos, como lo son: los teléfonos inteligentes, sistemas de *GPS*, localizadores, drónes, sistemas de cómputo y rastreo de impulsos electromagnéticos, etc. Estos medios científico-tecnológicos para beneficios sociales, como lo son los denominados drónes, y pese a los beneficios, en cuanto al recabo de información catastral o mapeo, también genera la invasión al derecho de privacidad en algunos casos, lo que genera cierto escepticismo en cuanto al uso de estos novedosos instrumentos especializados.

Choclán, Montalvo, (1997) refiriéndose a la especificidad del delito informático establece dos factores: "1. Las acciones se vinculan al

---

[57] Carlos María, Romeo Casanova. *Poder informático y seguridad jurídica*. *Citado por el Dr. Santiago Acurio del Pino*. (Madrid, España: Internacional, 1 988) 14.

[58] Ibíd. 17.

funcionamiento de una máquina y, 2. En buena parte de los supuestos, recae sobre un objeto intangible o inmaterial".[59]

Es importante hacer mención que en Guatemala, se programaron ataques cibernéticos simulados, a portales de instituciones bancarias, distribuidoras de energía, ministerios, y todos los que manipulan información delicada fueron atacados por hackers éticos, diseñado por El Comité Interamericano Contra el Terrorismo (CICTE), adscrito a la Organización de Estados Americanos (OEA), efectuados en mayo de 2013, para activar sus sistemas de protocolo. El ejercicio que tuvo como objeto el impulsar en las instituciones, el fortalecimiento de esos protocolos adquiridos para mejorar la respuesta y el manejo de una crisis eventual, que al momento de un debilitamiento en su infraestructura a causa de delincuencia cibernética, tenga la certeza del resguardo de la información proporcionada por los usuarios.

Medios de ejecución

- Medios Tecnológicos
- Computadoras
- Celulares
- Drónes
- Tabletas, etcétera.

Sujetos:

- **Activo**: Cualquier persona física con conocimientos en Cibernética.
- **Pasivo:** Cualquier persona física o moral.

Objeto Materia: Es indistintamente, la cosa mueble o inmueble, incluso abarca derechos y demás cosas incorpóreas.

[59]Antonio José, Choclan Montalvo. *Infracciones patrimoniales en los procesos e transferencia de datos, en el cibercrimen. (*Granada, España: Dykinson, 1997.) 227.

Clasificación:

- Por la conducta**:** De acción u omisión.
- Por el número de actos**:** Unisubsecuentes – plurisubsecuentes.
- Por el daño: De resultado material o psicológico.
- Por su duración: Instantáneo o continuo.

Consumación del delito o fraude: Se presenta cuando el activo se hace de la cosa o alcanza el lucro indebido, es decir, aquel en el que se integra el resultado típico, antijurídico y culpable, al agotarse todos los elementos tipo.

En virtud de esas nuevas tendencias científicas y debido a que la informática tiende a evolucionar más rápido que la legislación, existen conductas criminales por vía informática, que no pueden considerarse como informáticos per se y, que deben por consiguiente ser objeto de regulación. Como se establece en la *Ley Colombiana* Decreto 1273 sobre ***"***La protección de la información y de los datos***"***, referente a la Interceptación de datos informáticos:

> "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses*".*[60]

[60]Congreso de la República colombiana. *Ley 1273 Colombiana*. Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemasinformáticos.http://www.mintic.gov.co/portal/604/articles3705_documento.pdf (Bogota,Colombia: 5 de enero de 2 009) Artículo 269 C.

3.2.1 Concepto

Fraude Cibernético: Es toda aquella conducta o acción, típica antijurídica y culpable en la que una persona accesa a información de propiedad informática, sin autorización del titular del derecho. Sean éstos archivos personales o corporativos, fotografías, videos o documentos en general contenidos ya sea en correos electrónicos o redes sociales, o sustraídas en perjuicio de la data o información de un tercero o sobre las que tenga interés directo o no, que estén incorporadas en un computador, teléfono, tableta, dispositivo o sistema operativo que utilice tecnología de información o programas específicos para descifrar códigos personales.

3.3 Competencia jurisdiccional para diligencias novedosas en Guatemala

La ausencia de mecanismos legales para la administración de la justicia, en los casos de violaciones a derechos fundamentales protegidos por el Estado, cometidos por medios tecnológicos como producto de la creación de nuevas formas de interacción en redes sociales, ha generado una serie de discusiones y propuestas al respecto. A través de estas redes sociales, se han generado formas de violación a derechos fundamentales de las personas, como lo son: daño físico, moral, psicológico y en algunos casos más graves, que ponen en peligro la integridad física de las personas. Éste uso indebido de las redes sociales, sirve de plataforma para la comisión de diferentes tipos delictivos que no se encuentran regulados, y por consiguiente no hay un órgano jurisdiccional competente especializado para sancionarlos.

Según la congresista Nineth Montenegro, de la bancada "*Encuentro por Guatemala,*" es necesaria la creación de una fiscalía de delitos cibernéticos a través de la propuesta de reformas al Decreto 1773, Código Penal, en materia de delitos electrónicos y cibernéticos, debido a "El uso de perfiles falsos con fines delictivos como promesa de un futuro trabajo y promesa de beneficios económicos o remuneraciones laborales para realizar actos con fines sexuales o eróticos deben ser penalizados"[61] En la iniciativa presentada por la bancada (EG) se estipula una sanción de hasta 5 años de privación de libertad para funcionarios que por medio de influencias se hagan de información que pueda ser revelada, cedida o transmitida para dañar a personas individuales o jurídicas.

La Convención de las Naciones Unidas contra la delincuencia organizada transnacional, suscrita por Guatemala con fecha 12 de diciembre de 2000 y aprobada mediante el Decreto Número 36-2003, tiene como propósito promover la cooperación para prevenir y combatir eficazmente la delincuencia organizada transnacional, comprometiéndose el Estado de Guatemala, a adoptar las medidas legislativas correspondientes a efecto de combatir y erradicar la delincuencia organizada, estableciéndose mecanismos especiales de investigación.

3.3.1 Diligencias novedosas

De la aplicación de la tecnología procedente de la evolución en la informática y la comunicación, surgen las Tecnologías de la

[61]Nineth, Montenegro.*https://www.elderechoinformático.com/index/php?option=com_content&view=article&id=1801:proponen-crear-fiscalia-de-delitosciberneticos-enguatemala&catid=130.elderechoinformatico-guatemala&Itemid=13*6. (22 de ma yo de 2 015).

Información y de la Comunicación, conocidas como normas (*TIC*), reconocidas a nivel internacional, también como una necesidad de regular respecto de la protección y autodeterminación de las empresas en beneficio de los derechos de contratación e información comercial, que en otras legislaciones es conocido como Hábeas Data Financiero**.**

Se evidencia la necesidad de implementar nuevas herramientas de investigación como, la cibernética forense, que a través de un órgano especializado, aplique nuevas diligencias valiéndose de tecnologías destinadas a preservar elementos de prueba, fundamentales y susceptibles de la información contenida en archivos personales, sean éstos de carácter individual, jurídico o bien de contenido comercial y, que pueden en el desarrollo de la investigación, proteger otros derechos, evitando el mal tratamiento de la prueba, durante el proceso de indagación de un hecho concreto.

Sin embargo, en nuestro país, respecto de la conservación del contenido de estos archivos en las diligencias novedosas, que deberán ser implementadas en su momento en una Ley especial y en materia procesal, se debe tomar en cuenta el perfil de los profesionales idóneos con especialización en una carrera judicial de cibernética forense. Para ello en nuestro país, es necesaria la creación de carreras judiciales en dicha materia.

En relación a la protección de la prueba informática, se observa dos aspectos: Por una parte, su característica especial "técnica de preservación de la prueba informática*",* como un

elemento clave que garantice el control sobre la información relacionada con las personas, sus documentos y archivos personales, en la cadena de custodia de la prueba tecnológica; los niveles de intromisión y exposición del contenido del tratamiento de los datos que de ellos consten en cualquier tipo de archivo y, que forme parte de la prueba, deben ser resguardada por personal con conocimiento técnico idóneo.

Según el tratadista ***Libardo Riascos[62],*** el proceso de tratamiento de la información o de los datos de carácter personal, conforma una serie de etapas, fases o ciclos informáticos, tales como: la recolección, almacenamiento, registro, circulación y transferencia de datos.

> "Las diferentes legislaciones del mundo han regulado este procedimiento informático desde el punto de vista del derecho administrativo y civil y para protegerlo como último ratio, en todo o en parte, se han añadido mecanismos jurídicos de tipo penal, para tutelar los derechos al acceso a la información, las facultades estructurales del hábeas data (conocimiento, actualización, rectificación y cancelación de datos); y por supuesto, los derechos y libertades fundamentales, tales como la intimidad".[63]

Por otra parte, su característica de protección del derecho constitucional y fundamental <*Derecho de Hábeas Data*>, que busca no sólo el reconocimiento de un derecho a la autodeterminación informativa, sino, al no condicionamiento de

---

[62] Libardo Orlando, Riásco Gómez. *Derecho constitucional*. (Lleida, España: Editorial jurídica, 1 999.) 3

[63] Ibíd.,

las opciones y elecciones al momento de ingresar datos personales a bases de datos públicos o privados, y al buen uso del tratamiento de éstos, durante el proceso de investigación de la prueba; a la necesidad de reconocer el derecho de protección de datos y autodeterminación empresarial, y en general actuar libremente dentro del tipo de proceso, sea éste privado o público, sin violar la norma que debe contenerse en una Ley especial como *Ley de Autodeterminación Informativa*.

A nivel internacional innumerables se busca restablecer el equilibrio, entre un desarrollo tecnológico que evoluciona y la privacidad, la que indudablemente se ve redefinida, con las aplicaciones de las nuevas tecnologías, redes sociales y nuevas formas de interacción social, que han cambiado de forma considerable la vida en sociedad, y comercialización, como lo son por ejemplo: las nuevas formas de contratación en línea, las diferentes formas de compras por internet, los intercambios de derechos por medio de acuerdos digitales, compromisos laborales adquiridos por medios cibernéticos, obligaciones pactadas en redes sociales y otros que aún no son regulados.

Se genera el interrogante de cuál debe ser la naturaleza de esta protección del Estado, ante éste constante evolucionar de la tecnología y a la forma en que debe ser concebido el derecho de privacidad y determinar, cuáles actos o hechos deben ser considerados como amenazas que deben ser investigadas de oficio, sancionables, penalizables o no.

El *Código Civil* guatemalteco, como procedimiento novedoso de investigación, incluye en el año 2008, el uso de métodos científicos, con el manejo de aparatos tecnológicos, en búsqueda

de la prueba de *ADN* para incluir o excluir a los denunciados dentro de procesos civiles, no obstante, aún se tienen ciertas limitaciones para el uso de éstos métodos en otro tipo de procesos. Esos peritajes forenses, coadyuvan en la persecución y búsqueda de prueba genética, no considerada como delitos, en especial lo referente a la paternidad y filiación; a pesar de lo expuesto, es fundamental ampliar sobre el uso de éstas técnicas de investigación en otro tipo de escenas delictivas.

Como prueba técnica forense principal el *ADN o DNA* en nuestro país es utilizado para esclarecer el parentesco, sin embargo, también en hechos delictivos, como por ejemplo, violaciones. Que en muchos casos no se utilizan como recursos que proporciona el Estado, por los elevados costos de la investigación en la persecución penal, en cada proceso y al cúmulo de procesos que pendientes. Otros métodos novedosos implementados por el Estado, para la búsqueda de preparación de la prueba, son los enunciados en el Decreto 16-2013:

> "En los casos para recibir declaraciones de niños, niñas y adolescente víctimas y /o testigos, la Constitución Política de la República y Tratados Internacionales en materia de Derechos Humanos, establecen que es obligación del Estado proteger de forma integral a la niñez y la adolescencia, se les debe garantizar un trato digno y acorde a su edad, particularmente en los procesos de persecución penal y protección integral; debiendo aplicarse las técnicas y procedimientos adecuados para la entrevista, declaraciones y pruebas anticipadas; con una atención especializada, observando el interés superior del niño, en forma libre, integra y

> espontánea, evitando de esta manera un mayor grado de victimización".[64]

Los peritajes forenses adecuados en materia de evidencia digital, han sido objeto de investigación y análisis, no obstante, en nuestro país deben ser materia de análisis y prioridad, ya que es pertinente evaluar tanto el personal técnico capaz e idóneo para realizar los peritajes cibernético-forenses, así como establecer los métodos específicos para determinados procesos de investigación, para la obtención de la prueba digital, no sólo para asegurar un adecuado tratamiento de los datos contenido en los archivos, sino también, para preservar la prueba digital sin alteraciones hasta que sea objeto de investigación e incorporada como prueba fidedigna al debido proceso.

3.3.2 Competencia jurisdiccional

Jurisdicción es la facultad que tiene el Estado para administrar justicia en un caso concreto por medio de sus órganos jurisdiccionales, sin embargo, aunque exista la violación de un derecho que se posee, por ser objeto de propiedad, al no existir una norma que regule y sancione determinado hecho punible, la violación simplemente queda impune. El problema que se presenta con los delitos de índole informática, es que en ocasiones, sus efectos nocivos tienden a ser no identificables a primera vista y sus efectos en otros casos son transnacionales. Ese elemento de transterritorialidad, es un elemento importante

[64] Corte Suprema de Justicia. *Acuerdo número 16-2 013*. *Instructivo para el uso y funcionamiento de la cámara Gesell, circuito cerrado y otras herramientas para recibir las declaraciones de niños, niñas y adolescentes víctimas y /o testigos*. (Guatemala: CSJ, 2 013).

en la determinación del órgano competente para la administración de la justicia, en virtud de la investigación que se produce por la comisión de un hecho delictivo denunciado por la parte afectada.

Competencia conforme a lo que establece la *Ley del Organismo Judicial*, “sólo podrán ejercer su potestad en los negocios y dentro de la materia y el territorio que se les hubiese asignado…”, siendo que los delitos cibernéticos no están tipificados en nuestro ordenamiento jurídico, no hay juzgados especializados en conocer lo referente a los delitos de carácter cibernético. Muchos de éstos delitos se caracterizan por cometerse por medios tecnológicos, que no necesariamente se cometen dentro del territorio afectado, según establece la Ley “… no impide que en los asuntos que conozcan puedan dictar providencias que hayan de llevarse a efecto en otro territ*orio*”.

En aquellos juzgados en los que se presenten denuncias de delitos de carácter cibernético, pueden resolver conforme a lo que la ley dispone para los asuntos que no tienen una regulación específica, sin embargo al no estar tipificados, en caso de haber un proceso, no hay equidad en la sanción impuesta.

En la Ley se establece que toda persona tiene libre acceso a los tribunales de justicia, para accionar ante los órganos jurisdiccionales sus pretensiones, en defensa de un derecho vulnerado conforme a la norma. No obstante, al no existir una norma específica que regule esa figura como punible, ese derecho es violentado. Es decir, al no existir una norma especial en materia de delitos informáticos que la tipifique como delito, no

puede haber persecución penal. Sin embargo, la *Ley del Organismo Judicia*l establece que:

> "Prevalece el bien social sobre los intereses particulares, los derechos de las personas protegidos por las constituciones como fundamentales, son inviolables, sean públicos o no".[65]

> En éste sentido el Decreto 17- 73, establece reformas al Código Penal, en el Artículo 4 sobre referente a la territorialidad de la *Ley Penal*, "Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción".[66]

El *Código de Derecho Internacional Privado*, Decreto Número 1575, en su libro tercero, instituye de los Artículos 296 al 313, lo relacionado a las *Leyes Penales,* que establecen las normas que rigen a todos los que residen en el territorio, sin más excepciones que las establecidas bajo el criterio de la territorialidad, sin embargo, algunos de los delitos tecnológicos tienen efectos transterritoriales.

Es importante entonces, conocer las modificaciones a las disposiciones penales que actualizan la aplicación de las leyes penales en cuanto a las sentencias extranjeras, en virtud de que en el Artículo 176 numerales 1 y 6 se establece que "…el imputado será juzgado según la Ley guatemalteca, aun cuando haya sido absuelto o condenado en el extranjero" en aquellos

[65] Congreso de la República de Guatemala. Ley del organismo judicial. (Decreto 2-89). (Guatemala: Librería jurídica, 1 992). Artículo 22.

[66]

presupuestos en los que estos delitos son cometidos en nuestro país y tiene efectos jurídicos fuera del territorio, deben aplicarse las leyes contenidas en los convenios, para la aplicación de las sanciones establecidas, que deben tener concordancia con otros cuerpos legales de carácter internacional.

3.4 Juzgados especializados

En Guatemala no existen juzgados especializados para conocer delitos de carácter cibernéticos. Pero existe el juzgado contra el femicidio, iniciativa que surge en 1993, en virtud de los niveles de violencia contra las mujeres. La iniciativa ingresó en el 2008 y fue aprobada por el Congreso en abril el mismo año, surge como primer juzgado especializado de *Femicidio y Otras Clases de Violencia Contra la Mujer*, en América Latina, creada para coadyuvar con los operadores de justicia, implementando para el buen desempeño de sus funcionarios su respectiva capacitación, en virtud de la importancia de esta institución legal. Así mismo, se implementaron tres fiscalías especiales,[67] una para delitos contra periodistas, delitos contra sindicalistas, delitos contra operadores de justicia y delitos contra activistas de derechos humanos.

Leonor Calderón, representante en Guatemala del *Fondeo de Población de las Naciones Unidas* (UNFPA) al referirse sobre el desempeño de los juzgados y Tribunales Especializados en delitos de femicidio y otras formas de violencia contra las Mujeres, expresa:

[67] *Reporte sobre el estado de los sistemas judiciales en las Américas*. *2 002-2 003*. https//www.oas.org/dsp/Observatorio/Tablas/Guatemala/sistema judicial-GT.pdf. (24 de junio de 2 015).

> "…Surge como estrategia para apoyar la iniciativa y ofrecer una colaboración tanto al Ministerio Público y el Organismo Judicial, la capacitación de los operadores de justicia de ambas instituciones y campaña de divulgación y difusión de esta nueva judicatura para fortalecer los niveles de confianza a las entidades del Estado".[68]

Con la existencia de los vacíos legales, en nuestro ordenamiento jurídico se observa una inestabilidad futura, respecto de los efectos derivador de la comisión de los delitos informáticos. Se hace una tarea difícil para el juzgador, al tener que adecuar el derecho violentado, al ejercicio judicial, sin una figura punible. Dentro de un ordenamiento jurídico que no prevé las herramientas jurídicas necesarias para evitar o contrarrestar la comisión de un hecho delictivo determinado y nuevo en su género, es una tarea titánica para el juzgador, el tener que aplicar una determinada sanción que sea congruente al derecho violentado; siendo que como en el caso de los delitos cometidos por medios tecnológicos, la norma vigente no se adecúa a las necesidades que se presentan en el ejercicio de la aplicación del derecho a casos concretos.

Es necesario que el Estado como garante, evalúe el impacto social que se ejerce por la falta de regulación de delitos relacionados con alta tecnología, y cómo lo ha resuelto el sistema judicial, para determinar si la falta de tipificación de estos delitos y la ausencia de cuerpos legales, obliga a los legisladores en la creación de la Ley específica contra delitos informáticos, procurando que las figuras que se tipifiquen tengan esa fuerza restrictiva suficiente, para generar confianza en la defensa de los derechos protegidos. Las propuestas e iniciativas legales, se generan de la insuficiencia de normas existentes, en la búsqueda de la prevalencia

[68]Leonor, Calderón. Thelma Esperanza, Aldana Hernández. *Centro de reportes de información de Guatemala*. https://www.youtu.be.// (Publicado el 26 de septiembre de 2 012). (24 de mayo de 2 015).

del resguardo de los derechos individuales, son una constante necesidad de introducir nuevas figuras en concordancia con la cooperación mutua entre naciones.

3.4.1 Cibernética forense

Es la ciencia que se encarga del estudio por medio de análisis de pruebas con la intervención de profesionales o peritos especialistas en informática, con pleno conocimiento de técnicas específicas para la recuperación de información que ha sido modificada o disfrazada. Ésta técnica se conoce como técnicas forenses de recuperación de datos. Esta inclusión de conocimientos para recabar datos ocultos conocida como cibernética forense, necesita la aplicación de técnicas científicas y analíticas que coadyuven en la determinación, identificación y preservación de datos, analizando y exhibiendo datos que sean pertinentes dentro de un colegiado proceso de investigación legal. Las indagaciones de cómputo forense, toman en cuenta códigos binarios en las nuevas escenas del cibercrimen.

Dichas técnicas incluyen reconstruir el bien informático, es decir en caso de siniestro o tentativa de destrucción del sistema operativo, utilizando métodos especiales para recuperar el contenido, examinando los datos residuales, autenticado datos y explicando las características técnicas del uso de la metodología, aplicando a los datos y bienes informáticos el tratamiento

adecuado. Según ***Andrés Velázquez***[69], como especialista e investigador del Crimen Digital forense, es importante tomar en cuenta:

- **Cómputo forense**:

También llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Un examinador forense digital, dentro del proceso del cómputo forense, puede llegar a recuperar información que haya sido borrada desde el sistema operativo, a través de las diferentes fases:

- **Identificación**

  Conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto al levantamiento del bien, búsquedas y las estrategias de investigación.

- **Preservación**

  Revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis.

- **Análisis**

  Aplican técnicas científicas y analíticas a los medios duplicados por medio del proceso forense, para poder encontrar pruebas de ciertas conductas.

- **Presentación**

[69] Velázquez, Andrés. *Crimen digital 2 010*. http://es.slideshare.net/lideresacadémicos/andres-velazquez-presentacion. (21 de mayo de 2 015)

> La información resultante del análisis quedará registrada en un dictamen técnico, que puede ser presentado internamente o en un procedimiento legal.

Pese a que, en nuestro ordenamiento jurídico estas conductas son consideradas como no admisibles, típicas, antijurídicas y culpables, como cualquier hecho delictivo, no constan en nuestro sistema legal. Es necesario entonces, ampliar la discusión en cuanto a los métodos de investigación y técnicas forenses a aplicar; así como, el estudio de los perfiles de idoneidad de los profesionales elegidos como peritos especializados en la persecución de los medios de prueba cibernética. Basados en la protección y preservación de datos de carácter patrimonial, así como el tratamiento de datos contenidos en archivos personales.

3.4.2 Importancia de la cooperación internacional contra la cibercriminalidad

Según Carlos Ochaita, los Convenios o Tratados se consideran en la actualidad como fuente de derecho, debido a que los Estados tienden a dejar todo por escrito en un afán de <*Codificar Lato Sensu*> la costumbre internacional. Se fundamenta en el principio básico de derecho civil *"Pacta Sunt Servanda",* es decir, lo pactado obliga. Locución latina que se refiere a que lo pactado en el contrato es Ley entre las partes y debe ser fielmente cumplida.

Nuestro ordenamiento jurídico establece lo referente a la exclusión por analogía, según lo preceptuado en el Artículo 7 del *Código Penal*, que por lo cual los jueces no pueden crear figuras

delictivas ni aplicar sanciones. Es por ello que, se hace necesario el implementar normativas especiales para la aplicación de las sanciones correspondientes. En algunos países a nivel mundial, se han tomado medidas precautorias contra la cibercriminalidad, en algunos países se prevé normas especiales, así como normas de derecho internacional privado y público, determinadas a evitar efectos negativos derivados de la violación de la privacidad de la data o información de carácter personal, que pueden ser utilizados para realizar actos delictivos denominados fraude cibernético o cibercrimen en un amplio sentido.

Es importante que el gobierno de Guatemala a través de sus legisladores y órganos especializados, faciliten la colaboración internacional en los casos en que se requiera la aplicación de la fuerza judicial en territorio extranjero, a través de la creación de herramientas jurídicas que favorezcan la aplicación del derecho, y ratifique su adhesión a los Convenios Internacionales, para combatir en forma conjunta, el crimen organizado; y asimismo, coadyuvar en la lucha contra los delitos cibernéticos a nivel internacional.

- **Convenios en materia procesal**

  La *Convención Interamericana Sobre Recepción de Pruebas en el Extranjero y su Protocolo Adicional, "*establecen el marco aplicable a los exhortos o cartas rogatorias que soliciten la obtención de pruebas o informes en el extranjero, tanto de índole civil o comercial, emitidos por la autoridad competente de uno de los Estados parte, a

> la autoridad competente de otro. Estos tratados constituyen instrumentos valiosos para la ubicación, detención, extradición, y enjuiciamiento de criminales en acciones penales y civiles simultáneas, así como para la ubicación y repatriación de fondos depositados en instituciones financieras en otros países".

3.5 Amplitud en la admisión de pruebas de cibernética forense

La amplitud en cuanto a la admisión de las pruebas obtenidas en cibernética forense, son de suma importancia en el resguardo de los derechos fundamentales, en éste sentido la *Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas* preceptúa que:

> "Las comunicaciones electrónicas serán admisibles como medios de prueba. No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el sólo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original".[70]

En el vocabulario jurídico dirigido por ***Capitant,*** en colaboración con la *Universidad Degli Studi del Sannio*, Italia, se define de forma muy general a la prueba como:

> 'Demostración de la existencia de un hecho material, o de un acto jurídico en las formas admitidas por la ley'; o bien el 'medio empleado con que se pretende mostrar y hacer patente la verdad o

[70]Congreso de la República de Guatemala. Ley para el reconocimiento de las comunicaciones y firmas electrónicas. (Decreto 47-2008). (Guatemala: Librería jurídica, 2 008). Artículo 11.

> falsedad de una cosa y más concretamente, justificación de la verdad de los hechos controvertidos en juicio, hecha por los medios que autoriza y reconoce como eficaces la Ley'.[71]
>
> "Acreditación de la certeza de un hecho. Así también establece que la prueba puede concebirse desde ángulos diversos. Puede considerarse como una actividad lógica y material orientada en el mismo sentido de la realidad que se trata de averiguar, eso es, como operación y esfuerzo amparados en la verdad: **es la prueba fin**. Pero también puede valorarse como el conjunto particular de recursos que pueden utilizarse para obtener aquella demostración: **es la prueba medio**. Aquí interesa la prueba como medio". [72]

Es obligación del Estado el ajustarse a las nuevas tendencias de investigación tecnológica, para coadyuvar en la prevención del delito y la protección de la prueba cibernética; con la implementación de diligencias novedosas de búsqueda de evidencias y la ejecución de técnicas, sistemas de alta tecnología, creación de banco electrónico de datos de huellas digitales, protocolo de seguridad de las pruebas cibernéticas, almacenamiento y herramientas jurídicas de aplicación transnacional. El Estado debe actualizarse para prevenir el delito cibernético en general, de lo contrario, se destruye el espíritu de la creación de la prueba cibernética, la cadena de custodia de material digital y los métodos conceptualizados que debe poner en práctica el poder judicial.

Conforme los establecido para las técnicas y herramientas de informática forense, según *Oscar Amaya*, "el Buró Federal de Investigación (*Federal Bureau Investigation*), conocido por sus siglas en inglés o FBI, y otras agencias a nivel internacional, dedican esfuerzos al combate de delitos informáticos, procedimientos científicos que persiguen la búsqueda de la verdad y el cumplimiento de la Ley, como institución

[71]Diccionario jurídico Omeba. *La prueba.* http://www.fiuxy.net/ebooks-gratis/762570-enciclopedia-juridica-omeba-completa.html (19 de junio de 2 015).

[72] Diccionario jurídico Espasa. *Prueba*. (Madrid: Calpe, 1 999.) 825.

especializada en investigación y utilización de herramientas tecnológicas en laboratorios especializados desde 1984, ha desarrollado programas especiales para examinar evidencia computacional", conceptualiza la informática (o computación) forense como:

"Como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional".[73]

"*High-tech crime is one of the most important priorities of the Department of Justice*" (Los crímenes de alta tecnología son la prioridad más importante en el departamento de justicia) Lo que claramente evidencia el impacto internacional de los delitos de carácter cibernético, pese a ser delitos de características no violentas, pueden llegar a causar daños económicos, psicológicos y comerciales que pueden llegar a ser irreversibles.

Gerberth Adín, Ramírez R,[74] identifica los objetos de la información forense con el fin de perseguir y procesar judicialmente a los criminales; investigando la creación y aplicación de políticas para prevenir posibles ataques cibernéticos y en caso de existir antecedentes, evitar casos similares; asimismo, el compensar daños causados por los criminales o intrusos. Aunque la ciencia de cibernética forense es relativamente nueva, se han logrado avances en cuanto a técnicas de investigación que benefician en el desarrollo de investigación de la prueba digital, tanto en delitos comunes, como en fraudes individuales, financieros, narcotráfico, terrorismo, tráfico de personas, etcétera.

[73] Oscar, Haver Amaya; Ricardo, León Coatura; Beatríz, Acosta. Informática forense. @uniandes.edu.co (20 de junio de 2 015) 2

[74] Ibíd.,

***Ureta Arreaga*,** en su tesis doctoral, al referirse sobre la investigación tecnológica y los retos a superar en la administración de justicia ante los delitos informáticos, expresa que en la república de EL Ecuador en cuanto a los elementos de prueba dentro de un proceso:

> "son de vital importancia, ya que mediante su investigación se llega a determinar la confirmación o desvirtuación de lo que corresponde a la verdad. Es trascendental, tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, ante un hecho de delito informático" *(SIC).*[75]

> Para ***Jeimy J. Cano M***.,[76] "la evidencia digital refiere que es la prima para los investigadores, donde la tecnología informática es parte fundamental del proceso. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es dubitable, es alterable y modificable, es eliminable".

Según el autor, estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Además, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado a: su debido registro, admisibilidad, valor probatorio, preservación, transformación y recuperación.

---

[75] Laura Alexandra, Ureta Arreaga. Retos a superar en la administración de justicia ante los delitos informáticos en El Ecuador. Guayaquil, Ecuador: 2 009) 9

[76] Ibíd.,

3.5.1 Alcance normativo

Guatemala cuenta con el primer juzgado especializado en delitos contra el femicidio, tres fiscalías especiales: para delitos contra periodistas, sindicalistas y operadores de justicia y una última para delitos contra activistas de derechos humanos, sin embargo, es necesario crear nuevos juzgados especializados sobre delitos informáticos, que en virtud del impacto social que pre suponen puedan llegar a colapsar el sistema de justicia, como delitos especiales, los delitos de carácter informático o cibernéticos necesitan de una regulación especial, en Guatemala y en Latinoamérica se ha advertido la necesidad de crear normas de carácter coercitivo para contra restar los efectos negativos del crimen organizado y garantizar el derecho de propiedad cibernética o informática.

CAPÍTULO 4
ANÁLISIS DE LA PROPUESTA DE LA LEY 4055 CONTRA EL FRAUDE CIBERNÉTICO EN GUATEMALA

4.1 Análisis de iniciativa

Guatemala, ha sido catalogada como país en vías de desarrollo económico, cultural, político, comercial, social y tecnológico. Con diversidad pluricultural y con la creciente necesidad de implementar los nuevos avances tecnológicos en beneficio del actuar cotidiano de sus ciudadanos, profesionales y sistema judicial en general; y con esa proyección de los efectos jurídicos, resultado del uso de esa nueva tecnología, en virtud de las emergentes formas de contratación, y la constante evolución de los sistemas cibernéticos y las diferentes aplicaciones que en la sociedad encuentran sus usos, necesariamente se generan repercusiones en el derecho ciudadano y por consiguiente, en el ejercicio de administración de justicia se generan retos al no encontrarse figuras delictivas que encuadren en delitos tradicionales con el derecho vigente, lo que genera inestabilidad en la administración de justicia.

En virtud de las denuncias a violaciones de derechos fundamentales, que constan en la Procuraduría General de la Nación, que pese a no estar incluidos en una normativa, son derechos considerados inherentes a la persona humana, y que muchas veces trascienden sus efectos fuera

del territorio, se catalogan como delitos de efectos transnacionales. Entonces, es necesario regular el derecho de protección de la información de datos personales, así como la protección de los datos contenidos en archivos de las personas jurídicas y la implementación de Leyes Especiales de Tecnología de la Información y Comunicaciones (TIC).

El proyecto de "*Ley* de *Delitos Informáticos"*, Dictamen Número 17-2009, Iniciativa Número 4055, consta de cinco títulos, sus respectivos capítulos y 54 Artículos, la Ley que persigue el fraude cibernético fue presentada con fecha 15 de mayo de 2009 y se conoció el 18 de agosto de 2009, ante el *Honorable Pleno del Congreso de la República*, en su tercer considerando establece que:

Con dicha iniciativa, se pretende contribuir en la creación de herramientas jurídicas en beneficio social, creando fuentes de investigación y uso de medios tecnológicos como nuevos métodos de información, exploración y asistencia en la cooperación internacional, basada conforme a lo establecido en el segundo considerando de la *Constitución Política de la República de Guatemala*, y lo contenido en la *Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas,* Decreto Número 47-2008 del Congreso. La iniciativa adquiere relevancia social, en cuanto a la protección a los ciberderechos inherentes a la condición humana, derechos que aún sin estar tipificados en nuestra legislación, deben ser protegidos por el Estado.

No obstante, carece de fuerza coercitiva y de una real visión de protección a los delitos que se observan en el uso de los diferentes medios tecnológicos.

El objeto o espíritu de la Ley, según su Artículo 1, se orienta a la preservación de la integridad y disponibilidad de la información contenida en sistemas que utilizan tecnologías de la información y sus componentes definiéndola como una protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información, congruente con lo previstos por la Ley. La iniciativa, consta de V títulos distribuidos de la siguiente forma: “Título I. Disposiciones Generales y Conceptuales; Título II. De Los Delitos; Título III. Organismos Competentes y Reglas de Derecho Procesal; Título IV. Cooperación Internacional y Asistencia Jurídica Mutua; Título V. Disposiciones Finales”.

El objetivo general, se fundamenta en los principios Constitucionales, principalmente determina los efectos negativos de la falta de regulación legal de nuevos derechos fundamentales. Lo que para el Estado se convierte en una obligación, para el ciudadano se convierte en un derecho. Como ejemplo de delitos informáticos, no incluidos se puede citar: la tentativa de tráfico infantil a través de redes sociales, y que no está regulado en nuestro ordenamiento jurídico; la prevención de los delitos del crimen organizado relacionados con la informática y el secuestro de infantes es una de las prioridades que el Estado debe garantizar como obligado de ejercer esa protección.

Los bienes jurídicos protegidos, incluidos en la iniciativa son:

- Integridad y disponibilidad de la información contenida en sistemas que utilizan tecnologías de la información y sus componentes;
- La información o los datos que se almacenan o transmiten a través de éstos;
- Transacciones;

- Acuerdos Comerciales o de cualquier índole que se llevan a cabo por su medio; y
- Confidencialidad de éstos.

Mismos que son insuficientes en Guatemala para ofrecer una seguridad jurídica a la población, en especial a los delitos cibernéticos más comunes en redes sociales, por ejemplo: amenazar, coaccionar, intimidar, acosar, engañar, difamar e interceptar patrimonio informático por medios tecnológicos, entre muchos otros, que son medio para cometer otro tipo de delitos tradicionales como: el secuestro o el asesinato por encargo. Según establece el *Congreso de Colombia*, en la Ley 1273 de 2009, en las adiciones a su *Código Penal* se crearon nuevos bienes jurídicos tutelados denominados “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Es fundamental el incorporar en Guatemala a estos bienes jurídicos tutelados, otros como lo son el derecho de autodeterminación o derecho de hábeas data, acoso e intimidación, entre muchos otros, para garantizar la protección del patrimonio informático. Asimismo, es necesario el analizar lo concerniente al derecho contractual informático e incorporarlo al derecho positivo como hábeas data financiero, en virtud de la importancia de la inclusión de dicha temática en la protección y tratamiento de la autodeterminación de datos contenidos en archivos de información comercial.

En esencia, trata los delitos contra la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información; el segundo

capítulo enuncia lo referente a los delitos contra la persona; y el capítulo tercero lo relativo a los delitos contra la nación y actos de terrorismo.

Sin embargo, faltan muchas figuras delictivas que son determinantes para ofrecer una verdadera seguridad jurídica. El proyecto de Ley del Perú, Número 2520-2012, Oficio Número 103-2013 "*Ley de Represión de la Cibercriminalidad*", en el apartado respecto a la incorporación o modificación de delitos en rubros sistemáticos preexistentes del Código Penal Peruano detalla, el delito de fraude informático y lo tipifica como el apoderamiento ilícito del patrimonio ajeno a través de la manipulación de datos o sistemas informáticos, en concordancia con el convenio de Budapest y que comprende a diversas formas de apoderamiento ilegítimo de bienes ajenos a través del uso de TIC. La guía para los países en desarrollo, de la Unión Interamericana de Telecomunicaciones, preceptúa que:

> "El uso del internet y las TIC ha permitido desarrollar un conjunto de aplicaciones informáticas para el desarrollo del cibergobierno, el cibercomercio, la cibereducación, la cibersalud y el ciberentorno, entre otros, lo cual ha permitido mejorar la calidad de los servicios brindados a la sociedad y, en especial, ha facilitado la integración progresiva de poblaciones en zonas remotas, lo cual es un factor importante de inclusión social".[77]

El Artículo 12 de la Declaración Universal de los Derechos Humanos se regula que "nadie será objeto de la injerencia arbitraria en su vida privada, su familia, su domicilio o en su correspondencia, ni de ataque a

[77]Guía para los países en desarrollo de la unión interamericana de telecomunicaciones. *Ciberdelito*. (Ginebra, Suiza: 2 009) 10.

su honra o a su reputación.” Así mismo, lo relativo a que “Toda persona tiene derecho a la protección de la Ley contra injerencias o ataques*”.*[78]

Al no existir una Ley que regule figuras delictivas propias del fraude cibernético, se genera un ambiente de impunidad, que favorece la violación de derechos básicos de privacidad de las personas, propiedad cibernética y el derecho a la vida, entre muchos otros, al ser sujetos susceptibles de delitos tradicionales como por ejemplo: el secuestro, al ser interceptados en redes sociales, por proporcionar su ubicación. Al no estar tipificados, se favorece una plataforma para la comisión de delitos no tradicionales y crimen organizado que quedan impunes, sin una norma coercitiva que especifique y determine una sanción.

Los delitos contenidos en la iniciativa de Ley, incluyen violaciones contra: la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información; acceso ilícito, daño informático, reproducción de dispositivos de acceso, dispositivos fraudulentos, espionaje informático, violación a la disponibilidad, fraude cibernético, Interceptación ilícita, falsificación informática. (*Agravantes generales*) en las acciones delictivas descritas en los Artículos 5 al 13, 16, 17, 18, 19 y 20. Respecto a los delitos contra la persona, incluye: delitos de pornografía infantil, control de acceso a pornografía infantil, difusión y alteración de imágenes personales**.** En cuanto a los delitos contra la nación y actos de terrorismo, integra además, el uso de identidad ajena.

No obstante, y derivado del análisis del contenido del proyecto de Ley y sus considerandos, es pertinente especificar en cuanto a la necesidad

[78]Carlos, Larios Ochaita. *Derecho internacional público*. Universidad de San Carlos de Guatemala. (Guatemala: F&G Editores, 2 001) 36.

de incluir otras figuras delictivas que han sido tomadas en cuenta por otros cuerpos legales de derecho comparado, como: la Ley 1273 de la *República de Colombia*, Ley No. 53-07 de la *República Dominicana*, Proyecto de Ley 2520- 2012 de la *República del Perú*, Ley 7425 de la *República de Costa Rica*, y demás figuras contenidas en organismos internacionales, que son necesarias incluir en virtud de cometerse a través de un ordenador utilizando en algunos casos las redes sociales, sistemas operativos, programas maliciosos o plataformas virtuales en general, tales como:

- Abuso de autoridad o cargo, abuso de mecanismos y dispositivos informáticos, acceso ilícito para servicios a terceros, acoso informático, adquisición y posesión de pornografía infantil, atentados a la integridad de los sistemas informáticos privados, atentados a la integridad del sistema bancario, autodeterminación informativa, bullying, chantaje, clonación de dispositivos de acceso, comercio ilícito de bienes y servicios, daño o alteración de datos personales, delitos relacionados a la propiedad intelectual y afines, desvío de tráfico, difamación, discriminación, divulgación de códigos de acceso, eliminación de códigos de acceso, estafa, falsedad de documentos y firma electrónica, falsificación de datos probatorios, fraude de proveedores de servicios de información en línea.

- Hurto por medios informáticos, Injuria pública, Interceptaciones de cuentas de usuarios en banca virtual o redes bancarias, Interferencias telefónicas no autorizadas, Intervención de Centrales privadas, Intimidación, Manipulación ilícita de equipos de telecomunicaciones, Obtención ilícita de fondos, Proposiciones a niños con fines sexuales por medios tecnológicos, Publicidad engañosa, Robo de identidad,

Robo de línea, Robo mediante la utilización de alta tecnología, Sabotaje, Suplantación de sitios web para capturar datos personales, Transferencia electrónica de fondos, Transferencia no consentida de activos, Uso de equipos para invasión de privacidad, Uso de software malicioso, Violación al Hábeas Data (*Como delito anticonstitucional, en ley especial*), Violación al Hábeas Data Financiero.

- Y otros contenidos en convenios o en cuerpos legales de derecho internacional. En cuanto a temas de derecho comparado, es importante puntualizar en la necesidad de confrontar normas jurídicas en relación a las legislaciones que hayan regulado respecto a los delitos de carácter informático, La Asamblea Legislativa de la *República de Costa Rica,* según expediente 17.613, modificó la sección VIII, del Código Penal. *Denominada Delitos Informáticos y Conexos*, al Título VII, Artículo 1, se reforma: (167) Corrupción, (196) Violación de Correspondencia o Comunicaciones, (196 bis) Violación de Datos Personales, (209) Hurto Agravado, (216 bis) Estafa Informática, (229 bis) Daño Informático, (288) Espionaje.

Por consiguiente, pese a la presentación del contenido del proyecto de ley, sus fundamentos constitucionales y la aplicación de normas de derecho internacional, se considera que la iniciativa de ley 4055 *Ley de Delitos Informáticos*, favorece principalmente al sector comercial, dejando un vacío legal y vulnerabilidad de los derechos fundamentales no contenidos en dicha Ley.

En cuanto a los organismos competentes y reglas de derecho procesal, es importante señalar la necesidad de crear una

reestructuración de las Leyes actuales que se encuentran en desuso, de las que no tienen una verdadera fuerza coercitiva o de las que están desactualizadas, y sobre todo anticipar la creación de Leyes futuras, necesarias para evitar conflictos de interpretación, debido al impacto internacional que presuponen los delitos de carácter informático, y que por su naturaleza de origen, surten efectos en el extranjero o viceversa; de igual forma, prever que tengan una efectiva persecución penal, anticipando respecto a la jurisdicción y competencia.

Ampliar la visión jurídica sobre las reformas procesales y actualizar la legislación nacional general en concordancia con normas de aplicación internacional en materia penal, es obligación del Estado, en virtud de la evolución constante de la tecnología, y en especial, al fraude cibernético.

En cuanto a los organismos competentes se refiere, se plantea la creación del Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala, como ente adscrito al Ministerio de la Defensa Nacional "**CSIRT**", (Comité de Respuesta a Incidentes de Seguridad Informática); sin embargo, se debe considerar que un ente capacitado sin vínculos militares, como la **Comisión Internacional Contra la Impunidad en Guatemala**, se adscriba al referido ministerio, para garantizar una ejecución imparcial del tratamiento de datos que en determinados casos puedan ser fácilmente manipulados por el mismo Estado.

En el Artículo 22, se establece que dicho comité estaría integrado por:

a) Un **comité director**, integrado por cada una de las instituciones siguientes:

1. Ministerio de Defensa;
2. Ministerio de Relaciones Exteriores;

3. Ministerio Público;
4. Ministerio de Gobernación;
5. Superintendencia de Bancos;
6. Superintendencia de Telecomunicaciones; y
7. Secretaría Técnica del Consejo Nacional de Seguridad.

b) Un **comité operativo**, integrado por dos o más delegados de las instituciones siguientes:

1. Ministerio de Defensa;
2. Ministerio Público; y
3. Ministerio de Gobernación.

c) Y por todas aquellas personas **jurídicas públicas o privadas**. Aquellas que deseen adherirse al "**CSIRT-gt**", de conformidad con las normas que se establezcan en el reglamento respectivo. Es importante hacer notar que según se establece en las tendencias de seguridad cibernética en América Latina y El Caribe, el equipo de respuesta a incidentes de seguridad cibernética de Guatemala, CSIRT-gt, sirve como el principal punto de contacto y organismo de coordinación nacional para asuntos relacionados con seguridad cibernética, Sin embargo, en ningún Artículo de la iniciativa se especifica sobre las calidades o requisitos para ser parte integrante de dichos comités, aunque conste en sus reglamentos, debe especificarse en la norma, para no generar conflictos de interpretación y desestabilidad jurídica.

La imparcialidad o la seguridad en el resguardo de los mismos. Se establecen funciones específicas para cada comité, sin embargo, debe redefinirse y ampliar el campo de las actuaciones para las organizaciones no gubernamentales y organizaciones civiles, que se adhieran a dichos comités. En dicha iniciativa se propone la creación de una Fiscalía

Especial del Ministerio Público, en la investigación y persecución de los delitos contenidos en la ley, el inconveniente es que deja un vacío legal, al no incluir los delitos no tipificados, lo que no beneficia realmente a la población en general, sino en especial al sector empresarial.

Es necesario además crear un departamento técnico forense, para el resguardo de la información digital, con profesionales calificados y una constante actualización de conocimientos sobre informática de dicho personal. Garantizar la custodia y resguardo del contenido de los archivos durante el tratamiento de datos, evitando violar derechos de terceros durante el proceso de investigación, evitando la fuga de información durante el tratamiento de datos, delimitando responsabilidades en tales casos, en virtud de lo delicado del contenido y el tratamiento de la información. Según las consideraciones con relación a la regulación de los delitos informáticos de los países latinoamericanos.

Las sanciones que se proponen en el proyecto de *Ley de Delitos Informáticos* carecen de fuerza coercitiva, y deben ser equivalentes al daño causado. Debido a que no existe en nuestro ordenamiento jurídico un ente colegiado especializado en delitos cibernéticos, y a la necesidad de realizar una efectiva capacitación en cuanto a temas novedosos, es obligación del Estado el proporcionar los medios científicos, humanos y técnicos necesarios para que la fiscalía especial que se cree sea efectiva, con profesionales capacitados en carrera judicial que formen parte del Ministerio Público, encargados de la investigación de los delitos de carácter informático, que cuenten con las herramientas técnico-científicas necesarias para realizar sus investigaciones.

Asimismo, analizar normas internacionales con experiencia sobre temas del cibercrimen, metodologías en cuanto a la detección previa a cometerse el hecho delictivo, para anticipar medidas de seguridad, y fortalecer el sistema judicial desde su creación, en la implementación de carreras judiciales.

En cuanto a las Medidas Cautelares y Procesales, que son necesarias en la aplicación de la norma, no obstante lo preceptuado en la iniciativa, en este sentido aunque se delimitan las responsabilidades de los proveedores de los servicios de internet, se debe detallar los límites de esos derechos y sancionar con fuerza coercitiva, cuando se cometan delitos por incumplimiento, de igual forma, especificar los derechos y obligaciones de los usuarios. El Artículo 26 establece al respecto que para garantizar ese funcionamiento conforme establece la persecución penal, las dependencias centralizadas, descentralizadas, autónomas y semiautónomas, que hasta la entrada en vigencia de la ley realicen actividades concernientes a la investigación de delitos informáticos.

Respecto a la cooperación internacional y asistencia jurídica mutua, en la iniciativa de Ley, en los Artículos del 44 al 50, entre las disposiciones concernientes a la capacitación, las reuniones interinstitucionales, convenios, asistencia jurídica mutua, la doble incriminación, la inmovilización de activos, convenios ratificados por Guatemala para coadyuvar en la persecución de los delitos de carácter cibernético, son de suma importancia para generar estabilidad y seguridad jurídica, tanto en el ámbito de las relaciones internacionales en pro de la cooperación de las naciones contra los delitos informáticos o cibernéticos, como también, a las relaciones interpersonales nacidas de la utilización de redes sociales o cibernéticas, y las nacidas en las relaciones comerciales electrónicas, que cada vez son más comunes.

Según su Artículo 44, es obligación del Estado el propiciar esa cooperación internacional a través de sus órganos competentes, con el fin de fortalecer los programas de prevención, investigación y represión en especial la persecución del delito y la preservación y custodia de la prueba cibernética.

En los Considerandos 2 y 3 de la *Ley Contra la Delincuencia Organizada,* Decreto Número 21-2006, se establece que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, fue suscrita por Guatemala con fecha 12 de diciembre de 2000 y aprobada mediante el Decreto Número 36-2003, cuyo propósito es promover la cooperación para prevenir y combatirla delincuencia organizada transnacional. Comprometiéndose el Estado a adoptar las medidas legislativas correspondientes para establecer mecanismos especiales de investigación, sin embargo, no se han aprobado Leyes especiales al respecto. Actualmente el Estado de Guatemala se encuentra atravesando una serie de problemas graves de corrupción a nivel institucional.

Por lo anterior, se ha generado colapso en el sistema judicial y un ambiente de inestabilidad laboral, educacional, económica, sistema de salud, y en una constante tensión social con repercusión a diferentes representantes del Estado y un masivo repudio general al régimen político. En espera de la resolución a la petición social de reformas legales, y en especial, para que de urgencia nacional se apruebe la iniciativa. Luego de los ataques dirigidos a los medios de comunicación, se solicitó al Ministerio de Gobernación un informe acerca de la utilización de tecnología y de las videocámaras instaladas en las manifestaciones pacíficas. La cooperación internacional siempre ha

generado estabilidad en las naciones que se adhieren a las normativas internacionales, con el objeto de coadyuvar en el desarrollo económico, social, cultural y en especial en temas de seguridad para cada nación.

En cuanto a la interpretación de la norma extranjera y la resolución de conflictos que se susciten, la forma de analizar lo contenido en convenios, acuerdos, tratados o pactos cuando son ratificados por varios países, es autenticándolo en diferentes idiomas. Los principios básicos convencionales de interpretación se fundamentan: en el sentido normal de los términos, en contexto, el objeto y fin del tratado y la buena fe. Doctrinariamente se sigue el siguiente orden: primero se debe atender al sentido literal y expreso, como se establece en nuestra *Ley del Organismo Judicial:*

En el Artículo 10 establece que en caso de ambigüedad u oscuridad, se usa cualquiera de los métodos siguientes:

a. **Interpretación auténtica**: Los mismos Estados contratantes se ponen de acuerdo sobre el significado de los términos o conceptos.

b. **Interpretación judicial**: Un tribunal interpreta el tratado, aplicando las normas de interpretación universalmente aceptadas; para que sea obligatoria debe preceder la manifestación expresa de acatar el fallo; e

c. **Interpretación Unilateral**: Es hecha por un órgano de uno de los Estados; es conflictiva la mayor parte de las veces.

El Centro de Estudios de Justicia de las Américas (CEJA), es una entidad intergubernamental con autonomía técnica y operativa creada en 1999 por la OEA, con sede en Santiago de Chile. Sus actividades se desarrollan de acuerdo a mandatos de las Reunión de los Ministros de

Justicia de las Américas (REMJA) y de las Cumbres de las Américas y Asambleas Generales de la OEA, con la misión de contribuir a la modernización de los sistemas de justicia en la región a través de la cooperación. El CEJA mantiene un Centro de Información sobre el funcionamiento del Sector Justicia en la región; realiza un seguimiento de los procesos de reforma de la justicia y desarrolla actividades de capacitación y asistencia técnica para los países miembros de la OEA.

> "Más de 80% de esos actos tienen su origen en alguna forma de actividad organizada, con mercados negros cibernéticos establecidos en un círculo de creación de programas informáticos maliciosos, infección informática, gestión de redes zombie o "Bonet", recolección de datos personales y financieros, venta de datos y obtención de dinero a cambio de información financiera".(SIC)[79]

Conforme informe proporcionado por la *Oficina de Naciones Unidas Contra la Droga y el Delito*, en la "*II Convención de La Conectividad Mundial y el Delito Cibernético*" efectuada en Viena del 23 al 28 de febrero de 2013. (@UNODC). Se ha determinado que las plataformas tecnológicas como redes sociales o páginas web, son medios en los que usuarios son víctima de delincuencia organizada, que utilizan la comercialización de productos que en ocasiones, son negocios ilícitos con apariencia legal.

Es tarea del Estado, el proporcionar medios efectivos para la persecución, investigación y sanción de delitos considerados de alta

[79] Organización de naciones unidas. La conectividad mundial y el delito cibernético.https://www.undoc.org/documents/organizedcrime/UNDOC_CCPCJ_EG.4_2013/2_S.pdf. (25 de mayo de 2 015).

tecnología, que vulneren derechos personales, públicos, privados, semi privados o comerciales, utilizando herramientas y medios efectivos con fuerza coercitiva, para garantizar el resguardo de los derechos fundamentales de los ciudadanos, usuarios del servicio informático. Aunque la implementación de la *Ley de Delitos Informáticos,* es en éste sentido de urgencia nacional, debe ser plenamente analizada e incluir las figuras delictivas adecuadas a nuestra realidad nacional y que se encuentran contenidas en otros cuerpos legales internacionales, para que la Ley que se apruebe, sea congruente con éstas. En especial se debe tomar en cuenta lo establecido al respecto en el Artículo 25 del Código de Budapest.

Respecto a las disposiciones finales, se plantea lo relativo a la responsabilidad civil y penal de las personas jurídicas, acciones administrativas, pago de indemnizaciones, tribunal competente, derogatorias, resoluciones electrónicas, reglamentos y la entrada en vigencia, estableciendo como tribunales competentes, los judiciales correspondientes a los delitos que se cometan haciendo uso de sistemas que utilicen tecnologías de la información, serán conocidos por los tribunales ordinarios correspondientes o por lo Juzgados de la Niñez y la Adolescencia, dependiendo del caso, pese a que en el Artículo 25 de la iniciativa 4055, se propone la creación de una fiscalía especial.

Cabe destacar que con la promulgación de la *Ley de Delitos Informáticos*, se deroga el contenido del Artículo 274 incisos A, B, C, D Y F del Código Penal. Debiéndose modificar y reevaluar lo relativo a la pena en los delitos informáticos, evitando interpretaciones ambiguas.

En el Artículo 51, se establece que las personas jurídicas son responsables civilmente de las infracciones cometidas por sus órganos, representantes, empleados o cualquier persona que preste sus servicios para dicha entidad; no obstante, a que en el segundo párrafo se establece lo relativo a la responsabilidad de las personas físicas, autor o cómplice de los hechos; las sanciones propuestas para las personas denominadas físicas no son congruentes,(literal a) pues se contemplan con una multa igual o hasta el doble de la observada para el hecho ilícito en dicha norma para las personas jurídicas, cuando son utilizadas como medios para la comisión de un hecho punible, lo que es inconstitucional, al no haber igualdad en cuanto a las sanciones propuestas.

Al no contemplar actos ilícitos cibernéticos, en determinados casos puede llegar a emitirse una resolución absolutoria, lo que daña no sólo los derechos fundamentales, sino afecta directamente el factor seguridad física y económica. En cuanto al pago de indemnizaciones, en el Artículo 53 se preceptúa que las personas físicas o jurídicas podrán ser condenadas al pago de indemnizaciones civiles a favor del sujeto pasivo; sin embargo, no establece el procedimiento a seguir o la forma en que deban indemnizarse los daños cibernéticos, aunque esto es relativo, pues el daño informático no tiene dimensión cuantificable en un plazo fijo, pues resulta difícil determinar daños cibernéticos, sin un procedimiento adecuado y específico. Así mismo, no se estable el plazo en que deberá hacerse efectivo dicho procedimiento.

En relación a las resoluciones electrónicas, en el Artículo 56 que, establece que derivado de la importancia de las comunicaciones electrónicas y su constante evolución, es necesario que la *Corte Suprema de Justicia* y *el Ministerio Público* generen sus respectivas firmas

electrónicas, para jueces y fiscales competentes, se deduce que de esta forma puedan ejercer sus funciones sin ser víctimas de actos ilícitos en el desarrollo de sus actuaciones y para garantizar la celeridad del proceso; no obstante, y debido a lo delicado de la importancia del tratamiento de datos electrónicos, es necesaria la intervención de la Comisión Internacional contra la Impunidad en Guatemala o CICIG, en cada caso, para garantizar y evitar actos de corrupción.

Según datos referidos por las "*Tendencias de Seguridad Cibernética en América Latina y el Caribe",* de una población de 15, 440.000, la cobertura de internet es de un 16 % de los suscriptores de banda ancha. Las entidades del sector privado no están obligadas por legislación a brindar información sobre incidentes específicos a las autoridades nacionales, y actualmente no hay acuerdos formales entre ambas partes respecto a dicha cooperación.

Para establecer un vínculo directo entre la realidad nacional y la protección de los derechos fundamentales, que se pretende implementar con la entrada en vigencia del proyecto de Ley 4055 y el ofrecido por las leyes vigentes, en los casos de violaciones contra derechos fundamentales, relacionados directa o indirectamente con la tecnología, se realizó el presente trabajo de investigación, incluyendo el previo análisis de las fortalezas y debilidades del proyecto, así como la visión que se plantea con la entrada en vigencia de la *Ley de Delitos Informáticos*.

4.2 Presentación, análisis y discusión de resultados

En Guatemala no se cuenta con una herramienta jurídica especializada en delitos cibernéticos, tampoco consta un registro de denuncias efectuadas por los ciudadanos, como sucede en varios países que incluso cuentan con una policía especial, registro nacional o regional de delitos relacionados con alta tecnología, un número específico para reportar o denunciar ser víctima de éste tipo de delitos o una fiscalía especial para conocer los delitos relacionados con la informática; para citar algunos ejemplos del bloque europeo, cabe destacar:

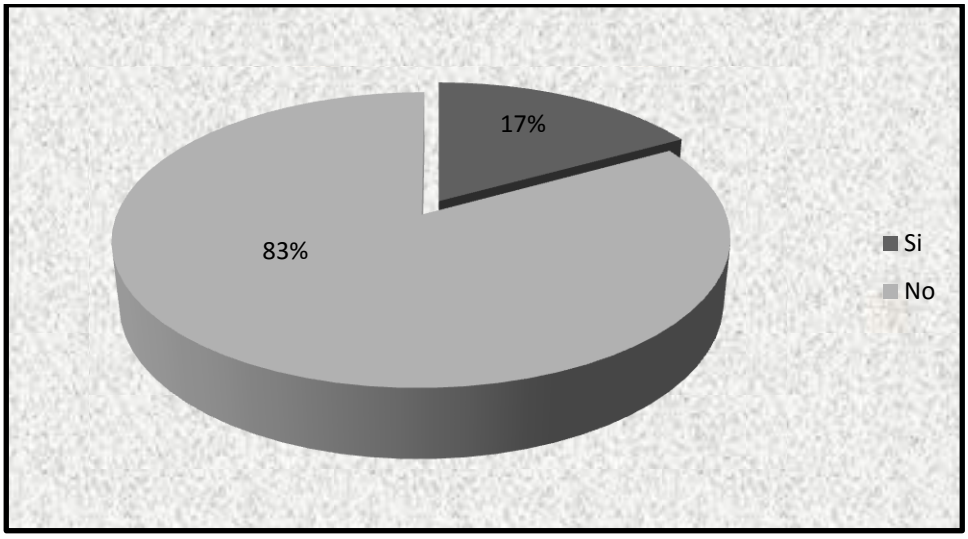
Bélgica, España y Suiza, que cuentan con efectivos métodos para denunciar, perseguir y sancionar el crimen cibernético.

Asimismo, en algunos países latinoamericanos se cuentan con herramientas eficaces para combatir éste flagelo, como por ejemplo: Colombia, República Dominicana y Costa Rica. En el uso del derecho al acceso de la información, se consultó los registros de Memorias Del Estado*,* de los períodos comprendidos entre el 2010 al 2013, para investigar el índice de cibercriminalidad reportada en el país; sin embargo, no consta ningún registro específico en los archivos respecto a los delitos cibernéticos. El ciudadano tiene el derecho de solicitar de las autoridades, información contenida en los registros de carácter público, en especial lo referente a éste tipo de delitos, pues sí han sido denunciados, como consta en los reportes dados a conocer por la Procuraduría General de la Nación en 2012, que incluyó un total de 259 denuncias relacionadas con delitos de carácter cibernético.

Conforme a los objetivos planteados en el presente trabajo de investigación, a través de los resultados obtenidos se logra determinar que es necesario realizar reformas legales en diferentes cuerpos legales, incluyendo nuestra carta magna, así también en materia penal y en específico, se recomienda el analizar la creación de una herramienta jurídica que concuerde con las disposiciones normativas contenidas tanto en la *Constitución Política de Guatemala*, como en disposiciones vertidas en el Convenio de Budapest, para poder utilizarla como herramienta de asistencia mutua entre naciones, con la suficiente fuerza coercitiva, para persuadir al delincuente.

Es importante hacer del conocimiento el lector, que se efectuó investigación de campo, utilizando la encuesta como medio para la obtención de datos, realizada por medio de la página social de Facebook, como medio tecnológico de interacción y comunicación social, efectuada del 21 de junio al 21 de julio de 2015. No obstante, debido a la falta de interés en los usuarios, en cuanto a contestar encuestas, durante tres meses no se obtuvieron datos, entonces, se procedió a motivar a los encuestados por medio de información previa, a través de videos educativos respecto del tema, el cuarto mes se obtuvo respuesta, la cual proporcionó los siguientes datos porcentuales:

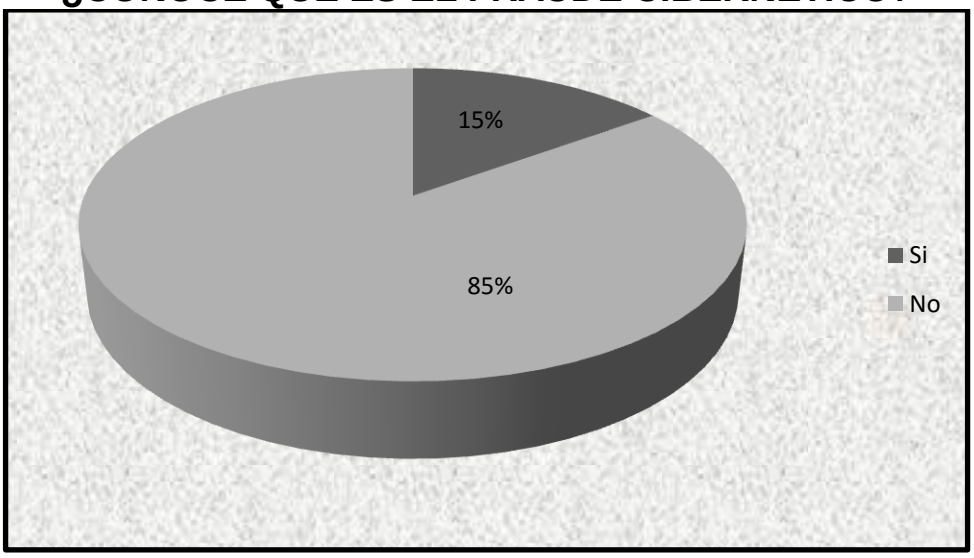
GRÁFICA 5
¿HA ESCUCHADO EN MEDIOS DE COMUNICACIÓN SOBRE LOS PELIGROS DEL USO INDEBIDO DEL INTERNET?



Fuente: Investigación de campo, 2015.

En cuanto a la pregunta expuesta el 17% admitió haber escuchado al respecto, mientras que, el 83% de los encuestados expresaron no haber escuchado en medios de comunicación, sobre los peligros del uso indebido del internet. Es evidente la importancia que representan los medios de comunicación, en cuanto a hacer del conocimiento de la población, sobre información que coadyuve a la prevención de éste u otro tipo de delitos, y colaborar así en la educación y protección de los ciudadanos, como herramienta tecnológica masiva de difusión, en beneficio de la población. No obstante, es obligación del Estado informar a la población sobre asuntos de interés nacional, ofreciendo una cobertura y seguimiento de las noticias de interés social, sobre todo lo referente a los contenidos de los usos indebidos del internet, para evitar que la población vulnerable, es decir, jóvenes y niños usuarios consuetudinarios de las redes sociales, y páginas de descarga de programas operativos, se vea afectada.

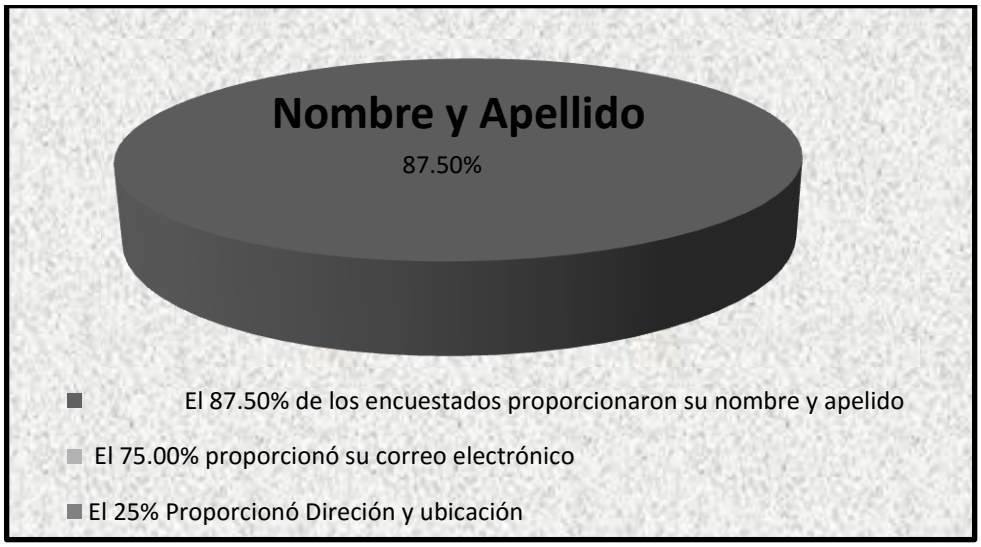
GRÁFICA 6
¿CONOCE QUÉ ES EL FRAUDE CIBERNÉTICO?



Fuente: Investigación de campo, 2015.

Respecto a la pregunta efectuada, el 85% de los consultados, refirió desconocer qué es el fraude cibernético; en contraste un 15% de la población encuestada, admitió conocer qué es el fraude cibernético. De acuerdo a los resultados de la investigación, se deduce que existe una confusión en la población, en cuanto a lo que se considera un delito cibernético o no. Suele confundirse el fraude tradicional, con el fraude cometido por medios tecnológicos, y es que, por el uso de medios tecnológicos, es un delito que puede ser continuado o no, identificable o no, pero sobre todo, con características de efectos transnacionales, de transgresión a derechos fundamentales. Es por ello, que aunque consta como delito en el proyecto de Ley 4055, debe contener una sanción equiparable al daño causado al usuario, sea éste natural o jurídico.

GRÁFICA 7
SEÑALE CUÁL DE LOS SIGUIENTES DATOS PERSONALES HA PROPORCIONADO POR INTERNET, TELÉFONOS CELULARES, CORREO ELECTRÓNICO U OTRO MEDIO TECNOLÓGICO:



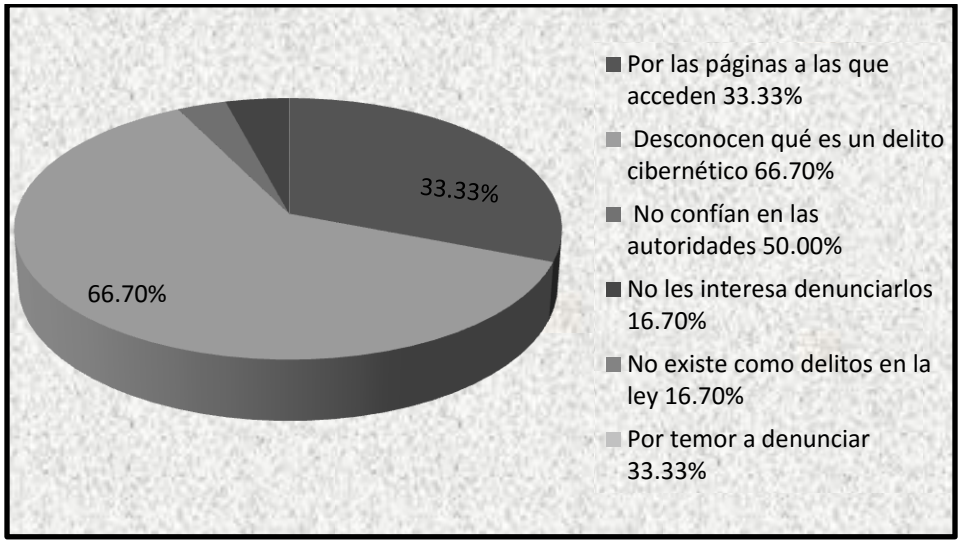
Fuente: Investigación de campo, 2015.

Es preocupante que el 87.50% de los encuestados admitieron que proporcionaron su nombre y apellido por el denominado ciber espacio, red o internet, a través de medios tecnológicos como: teléfonos inteligentes, computadoras, tabletas, iPod, GPS, para accesar a distintos servicios que solicitaban como requisito el correo electrónico u otros datos personales. Cabe destacar, que los usuarios ingresan a sitios web o espacios virtuales, sin ningún tipo de precaución, lo que favorece al crimen organizado, que por medio de interfaces aparentemente legales e inofensivas, infectan los equipos de cómputo con programas maliciosos afectando el sistema operativo de los ciberciudadanos, por lo que pueden llegar a ser víctima de otro tipo de delitos vinculados al crimen organizado.

Un 75% proporcionó su correo electrónico, lo que es de uso general, sin embargo, esta acción puede generar inconvenientes en cuanto al contenido de la información que ingresa al correo electrónico, pues es plataforma para los denominados spam o correo no deseado, que puede contener malwares o virus, que afecten no sólo el sistema operativo, sino que pone en peligro el contenido que se conserva en el equipo de cómputo ya sea personal o colectivo, pudiendo ser víctimas de los conocidos como troyanos, spoofing, keloggers o phishing que capturan información que además de ser privada, puede ser delicada, como por ejemplo: fotografías, documentos, estados de cuenta, etcétera.

Mientras que el 25% proporcionó dirección y ubicación en diferentes medios tecnológicos, lo que puede ser utilizado por el crimen organizado para la comisión de otro tipo de delitos, como: trata de blancas, tráfico de órganos, secuestro y asesinatos por encargo, entre muchos otros. Cabe destacar que, aunque fue un grupo reducido, el 12.50% proporcionó lugar y hora de reunión en redes sociales. El proporcionar datos personales por medios tecnológicos, hace de los usuarios que accesan a páginas sociales o sitios web, ser víctimas constantes de éste tipo de delitos, pues al desconocer sobre los peligros del internet en forma constante son violentados en sus ciber-derechos.

GRÁFICA 8
¿POR QUÉ CONSIDERA QUE LAS PERSONAS NO DENUNCIAN SER VÍCTIMAS DE DELITOS CIBERNÉTICOS?



Fuente: Investigación de campo, 2015.

En cuanto a la pregunta efectuada, el 66.70 % de los encuestados, refirió desconocer qué es un delito cibernético, y es que, pese a que algunos usuarios los han denunciado, han sido clasificados como delitos tradicionales es decir: como hurto, siendo patrimonio informatico, amenazas por medio de redes sociales y clonación de tarjetas de crédito, para citar algunos y todos relacionados con la tecnología. En especial los diferentes tipos de delitos que se han dado a conocer a nivel internacional, como lo son: la estafa a la salud, al ofrecer productos y servicios en donde se solicita número de tarjeta de crédito y datos personales, que pueden hacerse desde cualquier país, sin ser detectado.

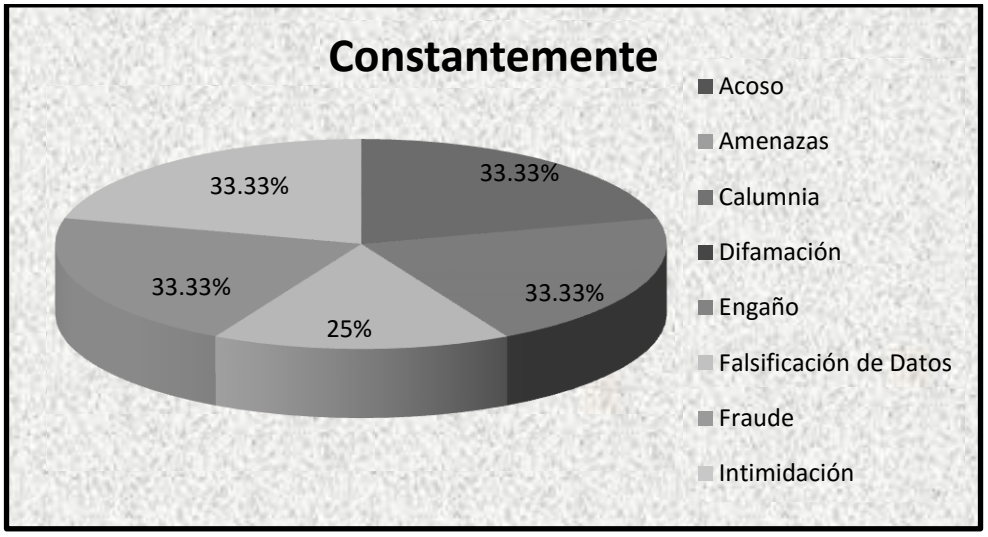
La importancia de la denuncia de éste tipo de delitos, radica en la incidencia de la comisión del delito y la necesidad de ser regulado, no obstante, en Guatemala no se observa una cultura de denuncia, en especial por la creciente desconfianza que se percibe de la población,

hacia el sistema de justicia. Cabe destacar que, por el tipo de pregunta de opción múltiple, el 50% de los encuestados refirió no confiar en las autoridades, debido a que se han visto envueltos en un complicado sistema de corrupción institucional.

El 33.33 % refirió no efectuar las denuncias por temor, debido a que la institución del sistema policial, se ha visto empañada no sólo por actos de corrupción, sino también, porque un alto índice de delincuencia organizada, es integrada por los miembros de la policía nacional civil, lo que desvirtúa la existencia del resguardo por parte del Estado, y genera un ambiente de inseguridad e inestabilidad social, haciendo que la violencia invada gran parte del territorio, sin una protección efectiva.

De acuerdo a la presente investigación se logra determinar que el 16.70 % de los encuestados, al expresar que no existen como delito, evidencian no sólo la desinformación, sino que también, una falsa seguridad en cuanto a los peligros relacionados a las redes sociales y páginas web, que sirven de plataforma para la comisión delitos de alta tecnología; de igual forma, al poco interés en temas relacionados con la prevención de delitos cibernéticos en redes sociales, y los usos de aparatos tecnológicos en general. Es necesario puntualizar en que, el desconocimiento de los encuestados en cuanto a qué delitos son considerados cibernéticos, es evidente y preocupante. Es obligación del Estado el hacer pública la información a los ciudadanos para prevenirlo y sancionarlo, así como, el crear normas especiales que las regulen.

GRÁFICA 9
¿CONSIDERA QUE HA SIDO VÍCTIMA DE LOS SIGUIENTES DELITOS INFORMÁTICOS?



Fuente: Investigación de campo, 2015.

La característica principal de los delitos cibernéticos, es precisamente que tienen apariencia de delitos no violentos, por tal razón los ciberciudadanos no advierten los peligros que éstos medios tecnológicos presuponen y navegan por sitios web, sin saber cómo identificar si están en peligro inminente. El Estado de Guatemala, está obligado a ejercer esa protección a los nuevos bienes jurídicos o derechos fundamentales, nacidos por los uso de las relaciones informáticas, por ejemplo: la clonación de las tarjetas de crédito es un delito que se reporta y que tampoco está regulado en una Ley especial, y no consta como bien jurídico tutelado en la iniciativa de Ley 4055;

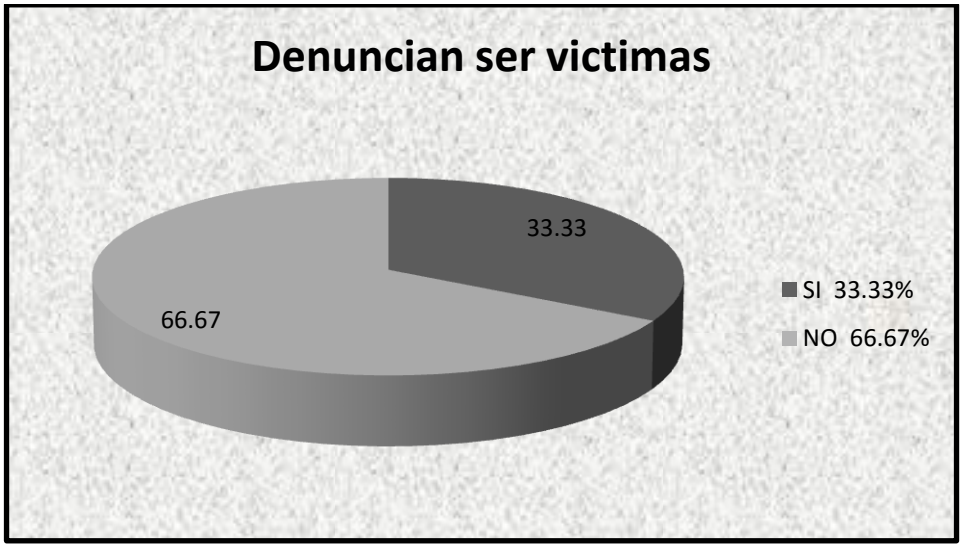
Sin embargo, en las *Memorias de Labores del Gobierno*, en los períodos que comprenden del 2010 al 2013, se evidencia la falta de interés en las autoridades, por observar y clasificar los delitos de carácter cibernético como una prioridad, al no incluirlos dentro de las

denuncias efectuadas específicamente como delitos informáticos, pese a las denuncias efectuadas por la Procuraduría General de la Nación.

Independientemente de ser clasificados en datos estadísticos como delitos o no, se hace necesario integrar los datos contenidos en archivos de la Procuraduría General de la Nación, respecto a la población afectada por el cibercrimen y hacerlos públicos, en beneficio de los usuarios. De los delitos más frecuentes en redes sociales la encuesta proporcionó los siguientes datos porcentuales, el 91.66% de los usuarios refirió haber sido víctima constante de: falsificación de datos 25%, fraude 33.33% e intimidación 33.33%; así mismo, los encuestados refirieron ser víctima de engaño y calumnia en un 33.33% respectivamente. Debido a la vulnerabilidad observada de la población encuestada, se logra determinar la necesidad de instruir a la población sobre éste tipo de delitos.

En la propuesta de Ley 4055, se prevé: acceso ilícito, daño informático, reproducción de dispositivos de acceso, dispositivos fraudulentos, espionaje informático, violación a la disponibilidad, fraude cibernético, interceptación ilícita, falsificación informática, delitos de pornografía infantil, control de acceso a pornografía infantil, difusión y alteración de imágenes personales, uso de identidad ajena, delitos contra la nación y actos de terrorismo informático; No obstante, son insuficientes para ejercer una verdadera protección por parte del Estado, pues existe una diversidad de hechos delictivos que no encuadran en esas figuras punibles, como por ejemplo: la intimidación, acoso, ofrecimientos obscenos, entre muchos otros.

GRÁFICA 10
¿ALGUNA VEZ HA DENUNCIADO SER VÍCTIMA DE DELITOS COMETIDOS POR INTERNET?



Fuente: Investigación de campo, 2015.

De los encuestados, el 66.67 % afirmó no haber denunciado ser víctima de delitos cibernéticos, mientras que un 33.33% refirió haber denunciado ser víctima de delitos relacionados con la tecnología. No obstante, al no estar regulados como delitos los cometidos con medios tecnológicos, el juzgador se ve en la necesidad de adecuarlos a delitos tradicionales, por lo que las sanciones no son equivalentes al daño causado, lo que hace que la pena no ejerza una fuerza coercitiva efectiva, para prevenir la comisión de éste tipo de delitos, ni es persuasivo como para evitar que se multipliquen los efectos negativos de la no regulación.

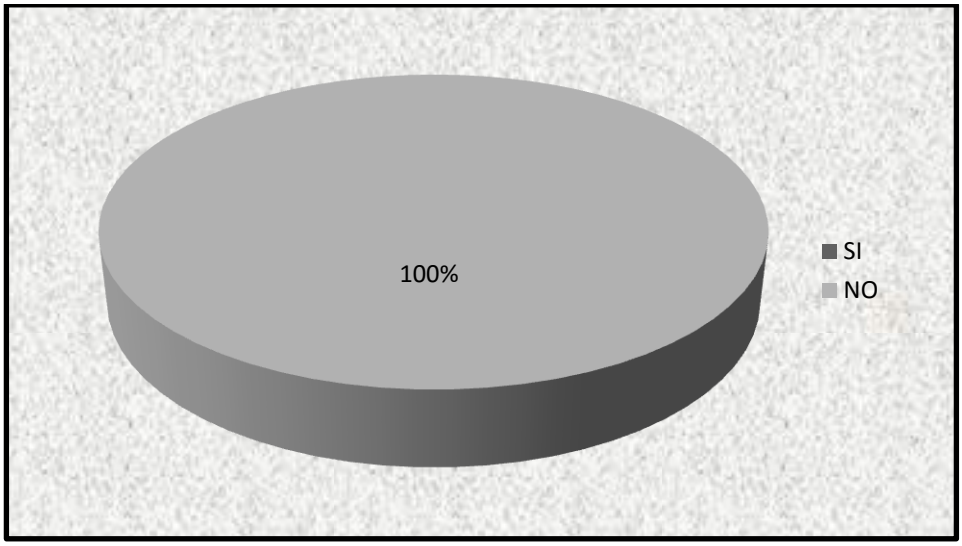
Derivado de la investigación de campo, se deduce que en Guatemala, no se cuenta con una cultura de denuncia ante los diferentes tipos de delitos, y en especial los delitos carácter cibernético, que al no estar regulados en nuestra legislación, son difíciles de encuadrar en una figura legal, por lo que al acudir a un órgano jurisdiccional, no coinciden

las sanciones con el daño causado, debido a que son encuadrados con los delitos tipificados en forma tradicional, por lo que los usuarios prefieren no denunciarlos. Las sanciones no equivalen al daño causado, como consta en el expediente **1356-2006**.

Por lo que la iniciativa 4055, debe integrar los bienes jurídicos no tradicionales que se protegen en los delitos informáticos, adecuándolos a nuestra realidad nacional, es decir, se debe realizar un estudio específico de los delitos más frecuentes en nuestro entorno, para ofrecer una protección jurídica eficaz.

El temor en la población ante la participación de los mismos agentes del orden en hechos delictivos, que se van haciendo cada vez más comunes, hace que las denuncias no se efectúen, debido a que los agentes del orden lideran bandas delincuenciales y en algunas ocasiones favorecen al crimen organizado. Además de ejercer un ambiente de impunidad en los juzgados, al no ejercer las funciones judiciales apegadas a la norma, y en general, al colapso del sistema de justicia que afecta la convivencia social, al favorecer un sistema de anarquía, según los índices de violencia actual. Al no contener los suficientes bienes jurídicos, conforme nuestra realidad nacional, no proporciona esa seguridad jurídica de defensa y resguardo de los derechos fundamentales, ante delitos informáticos.

GRÁFICA 11
¿SABE SI LOS DELITOS INFORMÁTICOS ESTÁN REGULADOS EN LEYES ACTUALES?

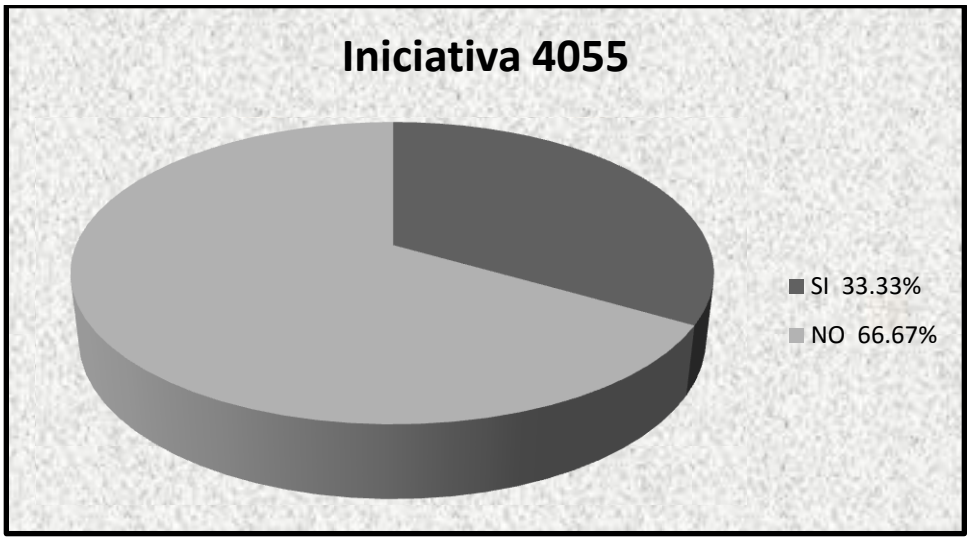


Fuente: Investigación de campo, 2015.

A la pregunta efectuada, los encuestados respondieron en un 100%, no saber si los delitos informáticos están regulados en leyes actuales, algunos factores que influyen en los resultados de la encuesta son:

1. La falta de interés por parte de los ciudadanos en cuanto a conocer de las normativas o proyectos pendientes de aprobar y del desconocimiento de la ley en general;
2. La falta de publicidad por parte de entidades del gobierno, en cuanto a las leyes que están pendientes de aprobar, para que la población se exprese al ser afectados en sus derechos; y
3. A que en los programas implementados por el Ministerio de Educación, no se analizan estrategias para instruir y prevenir a la población juvenil, sobre el uso inadecuado de la tecnología e introducir una cultura de ciudadanía, es decir, interés por conocer las normas que regulan la convivencia social, y conocimiento de las leyes en general.

GRÁFICA 12
¿SABE QUE ACTUALMENTE SE ENCUENTRA PENDIENTE DE APROBACIÓN LA PROPUESTA DE INICIATIVA DE LEY 4055 SOBRE DELITOS INFORMÁTICOS?



Fuente: Investigación de campo, 2015.

De la opinión de la población encuestada en cuanto a la pregunta expuesta, se determinó que en un 66.67% las personas desconocen que se encuentra pendiente de aprobación la iniciativa de proyecto de Ley 4055, pues no ha recibido la publicidad necesaria para que la población se interese en conocer acerca de la temática; mientras que el 33.33% argumentó que si la conocen. No obstante, es necesario hacer del conocimiento de las personas todos aquellos proyectos de ley que se pretendan aprobar, para ser analizadas y evitar que solo algunos sectores sean favorecidos con la entrada en vigencia de dichas leyes.

GRÁFICA 13
¿TIENE INTERÉS EN CONOCER EL CONTENIDO DE LA INICIATIVA DE LEY 4055, SOBRE DELITOS INFORMÁTICOS?

Fuente: Investigación de campo, 2015.

Al ser consultados los encuestados, en cuanto a la opinión a la pregunta expuesta con anterioridad el 100% de los que integran el estadístico, expresó interés en conocer sobre la iniciativa de Ley 4055. Debido a que los encuestados tienen interés en conocer el contenido de la iniciativa de Ley, se deduce que están conscientes que sólo a través de la creación de normas, las personas pueden acudir a los órganos jurisdiccionales para ejercer sus derechos ciudadanos de protección, ante este tipo de delitos cometidos a través de medios tecnológicos, que aún no se encuentran regulados.

El Estado debe analizar la inclusión de bienes jurídicos no tradicionales que deben ser tutelados, y que son vulnerados en nuestra realidad nacional, asimismo, se debe proteger tanto la vulnerabilidad de las personas individuales-naturales, como las jurídicas-colectivas, para fortalecer el sistema de justicia en cuanto a los delitos de carácter

tecnológico. Es indispensable hacer un estudio estadístico a nivel nacional en cuanto a la transgresión de éste tipo de delitos.

4.3 Desarrollo de la investigación

Conforme a los resultados proporcionados por la encuesta realizada en la presente investigación, se logra determinar que los índices de cibercriminalidad en la red social indagada, en relación a los delitos estudiados, son preocupantes debido a que muchos usuarios desconocen cuáles son considerados delitos cibernéticos, no obstante, el número de la población encuestada fue representada de la siguiente manera:

1. La población a la que se expuso la encuesta en la página social de Facebook, fue de 382 personas.

2. De la población total, 30 respondieron a la encuesta, lo que representa un 7.9 % del total a investigar.

3. De los delitos cibernéticos que se incluyen en la iniciativa de Ley 4055*, sólo dos forman parte de la encuesta efectuada, por ser delitos más comunes reportados según estudios realizados por organismos internacionales. De acuerdo a los datos obtenidos, fraude cibernético 33.33%, y falsificación informática 25 % son de mayor incidencia y en forma constante son víctima de delitos informáticos los usuarios, en sitios web y páginas sociales.

4. De las 30 personas que consintieron contestar la encuesta efectuada, el 33.33% refirió haber sido víctima de: Acoso, amenaza, calumnia, engaño, fraude, interceptación ilícita e intimidación. Es decir, de 30 encuestados, 10 refieren ser víctima de delitos relacionados con la tecnología.

5. Es evidente la necesidad que surge en nuestro ordenamiento jurídico, de incluir delitos informáticos contenidos en herramientas legales de derecho comparado y en especial, las contenidas dentro de los estudios actualizados, realizados tanto por los contenidos en el Convenio de Budapest, como de los estudios realizados para minimizar la incidencia de ciberdelincuencia para América Latina y del Caribe, en especial de los estudios necesarios a realizar en Guatemala a nivel nacional, para ofrecer una mayor protección, que sea acorde a nuestra realidad nacional, en la defensa de los derechos fundamentales de los ciberciudadanos.

6. Entre los tipos penales de mayor incidencia en redes sociales, se logra determinar por medio de los datos obtenidos en la encuesta efectuada, que los usuarios reportan haber sido víctima de algún delito cibernético en redes sociales, delitos que no se encuentran regulados en leyes vigentes, ni están contenidos en el proyecto de Ley 4055, (excepto los delitos de fraude e interceptación ilícita). Para determinar cuántos usuarios son afectados y qué tipos de delitos son los más frecuentes, es necesario realizar un estudio a nivel nacional.

CUADRO 2
TIPOS PENALES DE MAYOR INCIDENCIA IDENTIFICADOS EN LA RED SOCIAL

Delito Cibernético	Encuesta 2015
Intimidación/Contra el honor	33.33 %
Fraude*	33.33 %
Falsificación de datos	25%
Interceptación ilícita*	33.33%
Engaño	33.33%
Difamación/Contra el honor	33.33%
Calumnia/ Contra el honor	33.33%
Amenazas/Coacciones	33.33%
Acoso/Delitos sexuales	33.33%

Fuente: Investigación de campo, 2015.

CONCLUSIONES

1. Los principales derechos constitucionales que se vulneran al cometer fraude cibernético en Guatemala, según los resultados de la investigación son: Autodeterminación informativa, propiedad informática, reserva, seguridad, intimidad y confidencialidad de los datos, la información, entre muchos otros, pues por la magnitud del daño cibernético y las modalidades para cometer los distintos delitos de carácter tecnológico, es necesario realizar un estudio exhaustivo a nivel nacional, para determinar, no sólo la incidencia delictiva, sino también, los delitos cibernéticos más frecuentes para analizar la inclusión de nuevos bienes jurídicos a tutelar por el Estado en una Ley especial.

2. Existe escasa regulación en cuanto a delitos de alta tecnología, y es no positiva, por tener muy poca aplicación. Los bienes jurídicos que se contempla y tutelan deben evolucionar, por lo que las disposiciones legales actuales son insuficientes para ofrecer una protección a los derechos fundamentales, en cuanto a los delitos de carácter informático. Los bienes jurídicos a tutelar por la propuesta de Ley 4055 sobre Delitos Informáticos, en el marco de la prevención del fraude cibernético, no son congruentes con la protección que debe garantizar el Estado, pues son insuficientes para proteger a la población contra los delitos informáticos, debido a que las disposiciones vertidas, son más bien de defensa al sector comercial.

3. Los delitos no tipificados en la propuesta de Ley 4055 sobre Delitos Informáticos, y que son vulnerables en cuanto al tratamiento de datos de carácter personal que han sido plenamente estudiados por otras legislaciones y, que tienen mayor concordancia con las disposiciones contenidas en el Convenio de Budapest, y más frecuentes en Guatemala son: acceso ilícito, acoso, amenazas, chantaje, coacción, difamación, engaño, estafa, falsificación de datos, fraude, hurto, injuria, intimidación, publicidad engañosa, robo de códigos de acceso, uso de equipos para invasión de privacidad (*drone*), entre muchos otros que deben ser identificados, para ofrecer una mejor protección al ciberciudadano.

4. El derecho de *Hábeas Data*, es un derecho constitucional e inherente a la persona humana y plenamente reconocido a nivel internacional. En consecuencia de lo anterior, al avance tecnológico y a la intervención del crimen organizado en las tecnologías de la comunicación, la violación al derecho de habeas data o autodeterminación informativa, es un delito que puede y debe ser penalizado por el Estado. Así también, es un derecho que es plenamente protegido por el Estado de Guatemala, según lo establecido en los Artículos 31 y 44 de nuestra Carta Magna, como un derecho civil, desde el momento en que se vierte el contenido de datos personales en archivos y registros Estatales.

5. Nuestro ordenamiento jurídico, cuenta con la *Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008*, que contiene normativas específicas para garantizar el comercio electrónico, sin embargo, contiene vacíos legales que no pueden ser subsanados a través de ésta u otras Leyes existentes. Al no existir figuras o elementos punibles, se favorece a la comisión de hechos delictivos de carácter tecnológico como una plataforma para la comisión de actos ilícitos que no

se encuentran tipificados, lo que hace casi imposible al juzgador el poder encuadrar un delito común, a otro que utiliza como medio para la comisión del hecho un aparato tecnológico. En consecuencia, las disposiciones legales actuales no ejercen fuerza coercitiva, ni garantizan la seguridad de la información contenidos en archivos de datos personales.

RECOMENDACIONES

1. Es necesario integrar a las Leyes actuales, bienes jurídicos adecuados a nuestra realidad nacional, teniendo en cuenta que las normativas contenidas en la iniciativa de Ley 4055 sobre Delitos Informáticos, deben ser congruentes con las herramientas jurídicas internacionales, se recomienda evaluar el contenido y ampliar las figuras propuestas, en virtud de una futura asistencia mutua lo que debe favorecer en beneficio de los ciudadanos y la seguridad jurídica, en el combate al crimen organizado.

2. El Ministerio Público debe crear la Fiscalía Especial Contra Delitos Informáticos e incluir a los profesionales idóneos especializados en temas informáticos; para favorecer la investigación es necesario incluir en la metodología, nuevas técnicas para la obtención de la prueba, medios tecnológicos para preparar, preservar, custodiar y tratar datos contenidos en dispositivos tecnológicos, que puedan fundamentar la prueba de acuerdo a lo dispuesto por la cibernética forense y que sean acorde a la evolución tecnológica del momento, para brindar así la estabilidad jurídica necesaria en respuesta al fenómeno del crimen organizado, incluyendo medios de indagación especializada y novedosa conforme evoluciona.

3. Se debe garantizar la persecución penal de los delitos cometidos contra el patrimonio cibernético, sean éstos de personas individuales o jurídicas, y aplicar sanciones equivalentes al daño causado, para sancionar la tutelaridad de los nuevos bienes jurídicos, que sean vulnerados derivados

de la comisión de los delitos tecnológicos. Asimismo, es necesario fortalecer nuestro sistema judicial y jurídico legislativo, y analizar las normas que se encuentran en desuso, las que no tienen aplicación en las normas de cooperación mutua internacional, y en especial crear carreras judiciales especializadas en delitos cibernéticos. Además, por la importancia que suponen las transgresiones a los bienes jurídicos tutelados, violentados por los delitos cibernéticos, se debe crear una oficina especial, para que personas puedan realizar sus denuncias, pues no existe un registro estadístico nacional en cuanto a éste tipo de delitos, y las penas a imponer deben tener un efecto social regenerador.

4. Al instituir los comités sugeridos en el Artículo 22 de la iniciativa de Ley 4055 sobre Delitos Informáticos, se debe gestionar un proceso claro de elección de los miembros de la institución e incluir personal profesional, idóneo y capacitado; también, se debe garantizar la no politización de las comisiones con intervención de la Comisión Internacional Contra la Impunidad en Guatemala. De igual forma, es pertinente evaluar el gasto de inversión estatal en la persecución del delito cibernético, y comparar con legislaciones que hayan obtenido beneficios específicos en el resguardo y custodia de los datos contenidos en archivos electrónicos; tanto para proteger el derecho individual como el colectivo, y así garantizar el adecuado tratamiento de los datos informáticos, y proteger los nuevos bienes jurídicos a tutelar por el Estado, en base a un presupuesto que debe ser previamente analizado conforme a nuestra realidad nacional.

5. Es importante incluir los nuevos bienes jurídicos tutelados, nacidos del uso de las nuevas tecnologías, como lo son: el derecho a la autodeterminación informativa o habeas data, así como otros que en virtud de las características de los delitos cibernéticos se deben crear y proteger como derechos fundamentales, en una ley especializada para prevenir los delitos de alta tecnología. Según el Artículo 17 de nuestra Carta Magna, “no hay

delito sin Ley anterior", es decir, que según consta en la norma y en la *Convención Americana de Derechos Humanos*, "nadie puede ser condenado por acciones u omisiones que no estén tipificadas como delitos". En consecuencia, es necesario regular e integrar a la norma figuras punibles, para el resguardo de los derechos, y en especial, los derechos del ciberciudadano.

BIBLIOGRAFÍA

Acurio del Pino, Santiago. *Delitos informáticos generalidades.* Quito, Ecuador: Editorial CEP, 2 009.

Aguilar Guerra, Vladimir Osman. *Derechos fundamentales*. Guatemala: Serviprensa, 2 005.

Asamblea Nacional Constituyente*. Constitución Política de la República de Guatemala*, Guatemala: Serviprensa, 1 985.

--------. *Ley* de *emisión del pensamiento*. (Decreto 9) Guatemala: Librería jurídica, 1 966.

--------. *Ley del orden público*. (Decreto 7). Guatemala: Librería jurídica, 1 966.

--------*. Ley de amparo, exhibición personal y de constitucionalidad*. (Decreto 1-86). Guatemala: Liberia jurídica, 1 986.

Bequai, August. *The white-collar crime*, Massachusetts, USA: Lexington Books, 1 978.

Bermejo García, Miguel Alexander. *Tipificación del delito informático de robo de identidad.* Tesis, licenciatura, facultad de ciencias jurídicas y sociales. Universidad de San Carlos de Guatemala. Guatemala: USAC, 2 011.

Buonanno R, Luis. *Delitos bancarios computarizados*. Caracas, Venezuela: Ediciones y distribuciones Mangón, 1 997.

Caballenas de Torres, Guillermo. *Definiciones*. Buenos Aires, Argentina: Editorial Heliaste, 1 976.

Calderón, Leonor. Centro de reportes informáticos sobre Guatemala. CERIGUA: https://www.youtube.com/watch?v=9HZIg8KOAm0.(24 de mayo de 2 015).

Camacho, Losa. *El delito informático*, Madrid, España: Gráficas Cóndor, 1 987.

Cámara Internacional de Comercio. *Principios sobre la personalidad informática*.https://www.Velascocalle.co (24 de mayo de 2 015).

Carrasco, Andrino. M.M. *El acceso ilícito a un sistema informático*. https://www.Pc bjuridico.com/docs/libros/la-adecuaion.pdf. (21 de mayo de 2 015).

Choclan Montalvo, José Antonio. *Infracciones patrimoniales en los procesos de transferencia de datos, en el cibercrimen*: nuevos retos jurídico-pénales, nuevas respuestas político-criminales. Granada, España: Dykinson, 1 997.

Cibercriminalidad ministerio del interior. http://www.proyectoamparo.net/files /Ciberdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf./y/htt p://www.crimecommission.gov.au/publications/crime. (22 de julio 2 015).

*Ciberdelito en América latina y El Caribe.*http://www.proyectoamparo.net/files/Cib erdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf./y/http://ww w.crimecommission.gov.au/publications/crime. (22 julio de 2 015).

Congreso de la República de Colombia. *Ley de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos* (Decreto 1273) http://www.mintic.gov.co/ portal/ 604/articles-3705_documento.pdf. (25 de mayo de 2 015).

--------. *Ley sobre seguridad de la información y habeas data*. (Decreto 1777). http://www.mintic.gov.co/portal/604/articles-3564_documento.pdf (22 de mayo 2 015).

--------. *Delitos informáticos y entorno jurídico en Colombia.* (ISSN 0123-1472) Bogotá, Colombia: Editorial jurídica, 2 010.

Congreso de la República de Guatemala. *Código penal guatemalteco*. (Decreto 17-73) Guatemala: Librería Jurídica, 1 973.

--------. *Ley del organismo judicial*. (Decreto 2-89) Guatemala: Librería Jurídica, 1 989.

--------*. Código procesal penal guatemalteco*. (Decreto 51-92) Guatemala: Librería Jurídica, 1 992.

--------. *Ley de derechos de autor y derechos conexos*. (Decreto 33-98) Guatemala: Librería Jurídica, 1 998.

--------. *Ley de acceso a la información pública*. (Decreto 57-2008) Guatemala: Librería Jurídica, 2 008.

--------. *Ley para el reconocimiento de las comunicaciones y firmas electrónicas*. (Decreto 47-2008) Guatemala: Librería Jurídica, 2 008.

Congreso de la República del Perú. *Ley de delitos informáticos.* (Decreto 27309) http://www.oas.org/juridico/spanish/cyb_per_ley_27309.pdf (21 de mayo de 2 015).

--------. *Ley de represión de la cibercriminalidad*. (2520) Lima, Perú: Impresiones jurídicas, 2 013.

Congreso de la República Dominicana. *Ley sobre crímenes y delitos de alta tecnología.* (Decreto 53-07). http://www.oas.org/juridico/PDFs/repdom _ley5307. (22 de mayo de 2 015).

Corte Suprema de Justicia. *Acuerdo número 16-2 013*. *Instructivo para el uso y funcionamiento de la cámara gesell, circuito cerrado y otras herramientas para recibir las declaraciones de niños, niñas y adolescentes víctimas y /o testigos*. Guatemala: CSJ, 2 013.

De La Mata Barranco, Norberto Javier. *Los delitos vinculados a las tecnologías de la información y la comunicación en el código penal*. *Panorámica general, en el delito e informática*. Bilbao, España: Tirant Lo Blanch, 2 007.

Delito cibernético. http://www.prensalibre.com/internacional/Crece-delito-ciber netico-OEA_0_913108723.html. (25 de mayo de 2 015).

Delitos de cuello blanco. https///abogados.lawinfo.com/recursos/ley-criminal /crimen-de-cuello-blanco/delitos-de cuello-blanco.html. (15 de mayo de 2 015).

Diccionario Jurídico Espasa. *Derecho natural, prueba.* Madrid, España: Calpe, 1 999.

Flor, Roberto. *Permanenza non autorizzata in un sistema informatico o telema tico, violazione del segreto d'uffi cio e concorso nel reato da parte dell'extraneus*, en *cassazione penale*, Italia: Giapetto editore, 2 009.

Fraude cibernético. http://www.elsiglo21.com/index.php/tecnologia/53486-alertan-usuarios-gmail-y-netflix-por-nuevo-fraude-cibernetico. (25 de mayo de 2 015).

Hernández Díaz, Leyre. *El delito informático*. (Vol. I n°23 10/11/2 001); 230. San Sebastián, Gobierno Vasco, España: Eguzkilore, 2 009.

Larios Ochaita, Carlos. *Derecho internacional público*. Universidad de San Carlos de Guatemala. Guatemala: F&G Editores, 2 001.

M. Di Giorgi, Rosa María Ragona. *L'informatica giuridica en l'informatica del diritto. Milano, Italia:* Edito da Giuffrè, *2 004.*

Morán, Hugo. *Proyecto de ley de delitos informáticos*. (Decreto 4055) Guatemala: Editorial jurídica, 2 010.

Organismo Judicial*. Sentencias*. informática@cc.gob.gt / gacetas@cc.gob.gt. (22 julio de 2 015).

Organización de Estados Americanos. *Reporte de delitos informáticos*. (OC-13 /93, serie A, No. 13) Washington, USA: OEA., 1 993.

--------. *Ciberdelincuencia*. (OC-1/82 Serie A n° 1, párr. 25) Organización de Estados Americanos: OEA, 1 982.

--------. *Delitos cibernéticos*. (OC-15/97 serie A, No. 15) Washington, USA: OEA, 1 997.

Organización de Naciones Unidas. *Acuerdos de paz*, Guatemala: ONU., 1 996.

--------. *Convenio de Berna*, Berna, Suiza: ONU, 1 979.

--------. *Convención de Palermo*. *Contra la delincuencia organizada transnacional*. Palermo, Italia: ONU, 2 000.

--------. *Convenio sobre cibercrimen*. Concejo europeo. Viena, Budapest: ONU, 2 001.

--------. *Seguridad informática*. Nueva york, USA: ONU., 2 002.

--------. Convenio de Budapest. *Tratado internacional, sobre la ciberdelincuencia*. http://www.interior.gob.es/prensa/noticias//asset_publisher/GHU8Ap6ztgsg/content/id/2037736. (21 de julio de 2 015).

--------. *120º Sobre prevención del delito y justicia penal*. Washington, USA: ONU, 2 010.

--------. *Panorama del derecho informático en américa latina y el caribe*. Santiago, Chile: CEPAL, 2 010.

--------*. Manual para la prevención y control de delitos informáticos*. Washington, USA: ONU, 2 012.

--------. *La conectividad mundial y el delito cibernético*. https://www.unodc.org /documents/organized-crime/UNODC_CCPCJ_EG.4_2013/2_S.pdf. (25 de mayo de 2 015).

Ossorio, Manuel. *Diccionario de ciencias jurídicas, políticas y sociales*. Buenos Aires, Argentina: Editorial Heliaste, 2 014.

Pajuelo Bertrán, Carlos Alberto. *Ensayo crítico de la gestión dogmática del bien jurídico tutelado en los delitos informáticos en el Perú.* Lima, Perú: Sunat, 2 012.

Peña. Carlos A. *Derecho y las tecnologías de la información*. Informática jurídica y derecho informático*.* Buenos Aires, Argentina: C&T, 2 010.

Peñaranda Quintero, Héctor Ramón. *Iuscibernética. Interrelación entre el derecho y la informática*. https//www.monografías.com. (14 de mayo de 2 015).

Real Academia Española. RAE. *Fraude, informática jurídica*. Madrid, España: Espasa, 2 014.

Reporte sobre el estado de los sistemas judiciales en las américas. (2 002-2 003). https//www.oas.org/dsp/Observatorio/Tablas/Guatemala/sistema judicial-GT.pdf. Pág. 7. (24 de junio de 2 015).

Revisión de proyecto de ley estatutaria.http://Oiprodat.com/jurisdicción-relacionada/jurisdicción-sudamericana/jurisdicción-Colombia. (2 de junio de 2 015).

Riasco Gómez, Libardo Orlando. *Derecho constitucional*. España: Editorial jurídica, 1 999.

Romeo Casanoba, Carlos María. *Poder informático y seguridad jurídica*. Madrid, España: International, 1 988.

Sánchez Azofeifa, Ever. *Desarrollo de la prueba en delitos informáticos y uso de documentos electrónicos*. https//www.poderjudicialmichoacan.gob.mx/. (22 de mayo de 2 015).

Sarzana, Carlos. *Definición de delito informático*. https://www.angelfire.com /la/legislador/defin.htlm. (22 de mayo de 2 015).

Seguridad personal contra delitos cibernéticos. https//revista.unam.mx/vol.5/ num8/art52/sep_art52.pdf. (14 de mayo de 2 015).

Suñé Llinas, Emilio. *Informática jurídica y derecho informático. El observatorio iberoamericano de protección de datos*. Distrito Federal, México: Editorial Porrúa, 2 006.

Téllez Valdés, Julio. *Definiciones de delito informático*. https://www.angelfire. com/a/legislador/defin.htlm. (21 de mayo de 2 015).

Vásquez, Perrota. *Crímenes y delitos de computadora y alta tecnología en la República Dominicana*. República Dominicana: Ediciones Jurídicas, 2 013.

Velázquez, Andrés. *Crimen digital 2 010*. http://es.slideshare.net/lideresacadémicos/andres-velazquez-presentacion. (21 de mayo de 2 015).

V. ° B. °:

Margarita Pérez Cruz
Bibliotecaria General
CUNOR

ANEXOS

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
CENTRO UNIVERSITARIO DEL NORTE

ENCUESTA
SOBRE EL FRAUDE CIBERNÉTICO

Principio del formulario Preguntas obligatorias fueron contestadas (en su totalidad).

1. ¿Conoce sobre los riesgos que existen en internet?

- sí
- no

2. ¿Conoce qué es el Fraude Cibernético? *

- sí
- no

3. ¿Ha escuchado en medios de comunicación sobre los peligros del uso indebido del internet?

- sí
- no

4. ¿Ha contestado por medios tecnológicos (computadora, teléfono móvil, Tablet, etc.) encuestas con preguntas dudosas o de datos personales?

- sí
- no

5. ¿Ha contestado encuestas que no comprende?

- sí
- no

6. ¿Sabías que, las páginas que visitas por internet se re-direccionan a tu correo electrónico?

- ○ No me interesa
- ○ No lo sabía
- ○ No es cierto
- ○ Lo sé

7. Señale cuál de los siguientes datos personales ha proporcionado por internet, teléfonos celulares, correo electrónico u otro medio tecnológico: *

- ☐ Nombre y Apellido
- ☐ Dirección
- ☐ Número de tarjeta de crédito
- ☐ correo electrónico
- ☐ ubicación
- ☐ lugar y hora de reunión en redes sociales

8. ¿Con qué frecuencia utiliza los siguientes elementos?

Utilice los campos necesarios

	Computadora	Correo Electrónico	Teléfono móvil	Tablet	Páginas web	Redes Sociales
Lunes	☐	☐	☐	☐	☐	☐
martes	☐	☐	☐	☐	☐	☐
miércoles	☐	☐	☐	☐	☐	☐
jueves	☐	☐	☐	☐	☐	☐
viernes	☐	☐	☐	☐	☐	☐
sábado	☐	☐	☐	☐	☐	☐
domingo	☐	☐	☐	☐	☐	☐

9. ¿En qué nivel considera que los sitios que frecuenta son seguros?

0 % a 100 % [ ]

10. ¿Alguna vez escuchó sobre los virus informáticos?

- sí
- no

11. ¿Actualiza el antivirus en su computador?

- a diario
- cada semana
- cada mes
- cada año
- nunca

12. ¿Cuál de las siguientes páginas considera segura?

- hhtp:/
- https:/
- https://
- hhtps://
- Ninguna de las anteriores

13. ¿Sabe si los delitos cibernéticos están regulados en las leyes actuales?

- sí
- no

14. Considera que ha sido víctima de alguno de los siguientes delitos cibernéticos:

Utilice los campos necesarios y agregue el valor que considere que corresponde en orden de importancia, en el cuadro celeste

	CONSTANTEMENTE	RARA VEZ	NO ME HE DADO CUENTA	ALGUNAS VECES	NO ME INTERESA	NUNCA	--	-	+	++
ACOSO										
AMENAZAS										
CALUMNIA										
DIFAMACIÓN										
ENGAÑO										

FALSIFICACIÓN DE DATOS	○	○	○	○	○	○	○	○	○	○
FRAUDE	○	○	○	○	○	○	○	○	○	○
INTIMIDACIÓN	○	○	○	○	○	○	○	○	○	○

15. ¿Por qué considera que las personas no denuncian ser víctima de delitos cibernéticos?

- ☐ Por las páginas a las que acceden
- ☐ Porque desconocen qué es un delito cibernético
- ☐ Porque no confían en las autoridades
- ☐ Porque no les interesa denunciarlos
- ☐ Porque no existen como delitos en la Ley
- ☐ Por temor a denunciar
- ☐ _____

16. ¿Alguna vez ha denunciado ser víctima de delitos cometidos por internet?

- ○ si
- ○ no

17. ¿Sabe que actualmente se encuentra pendiente de aprobación la propuesta de iniciativa de Ley 4055 sobre DELITOS INFORMÁTICOS?

- ○ sí
- ○ no

18. ¿Tiene interés en conocer el contenido de la iniciativa de Ley 4055, sobre delitos informáticos?

- ○ sí
- ○ no

No. 086-2016

CUNOR | CENTRO UNIVERSITARIO DEL NORTE
Universidad de San Carlos de Guatemala

El director del Centro Universitario del Norte de la Universidad de San Carlos de Guatemala, luego de conocer los dictámenes de la Comisión de Trabajos de Graduación de la carrera de:

LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, ABOGADO Y NOTARIO

Al trabajo titulado:

TESIS
ANÁLISIS JURÍDICO DEL FRAUDE CIBERNÉTICO EN GUATEMALA

Presentado por el (la) estudiante:

ROSA IVONNE ESCOBEDO SOMOSA

Autoriza el

IMPRIMASE

Cobán Alta Verapaz 16 de Mayo de 2016.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA CENTRO UNIVERSITARIO DEL NORTE -COBAN, A. V.- DIRECCION

Lic. Erwin Gonzalo Eskenasy Morales
DIRECTOR