

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

**LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO
IMPACTO SOCIAL EN GUATEMALA**

JOSÉ DANIEL RUIZ ALQUIJAY

GUATEMALA, NOVIEMBRE 2012

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

**LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO
IMPACTO SOCIAL EN GUATEMALA**

TESIS

Presentada a la Honorable Junta Directiva
de la
Facultad de Ciencias Jurídicas y Sociales
de la
Universidad de San Carlos de Guatemala
Por

JOSÉ DANIEL RUIZ ALQUIJAY

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, noviembre 2012

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

DECANO: Lic. Avidán Ortiz Orellana
VOCAL II: Lic. Mario Ismael Aguilar Elizardi
VOCAL III: Lic. Luis Fernando López Díaz
VOCAL IV: Br. Modesto José Eduardo Salazar Dieguez
VOCAL V: Br. Pablo José Calderón Gálvez
SECRETARIA: Licda. Rosario Gil Pérez

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lic. César Augusto Conde Rada
Vocal: Licda. María del Carmen Mancilla Girón
Secretaria: Licda. Rosa Amelia Cajas Hernández

Segunda Fase:

Presidente: Lic. Homero Nelson López Pérez
Vocal: Lic. Ronald David Ortiz Orantes
Secretario: Lic. Marco tulio Pacheco Galicia

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



Lic. Luis Alfonso Campos Ramírez
Abogado y Notario

11 avenida 2-06, Residenciales Valle de la Mariposa
municipio de Amatitlán, departamento de Guatemala
Teléfono 41425630

03 AGO. 2012

Guatemala 03 de agosto de 2012

Doctor Bonerge Amilear Mejía Orellana
Jefe de la Unidad Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales de la
Universidad de San Carlos de Guatemala
Presente:

Señor Jefe:

Atentamente me dirijo a usted con el objeto de rendir dictamen favorable en mi calidad e Asesor de Tesis, del trabajo presentado por José Daniel Ruiz Alquijay, para su graduación profesional en nuestra facultad, intitulado "LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO IMPACTO SOCIAL EN GUATEMALA", para el efecto, me permito informar lo siguiente:

A) Contenido científico y técnico de la tesis: considero que el tema investigado por el bachiller José Daniel Ruiz Alquijay, es de suma importancia respecto a su contenido científico y técnico, ya que el mismo se enfoca desde la perspectiva doctrinaria y exegética de los textos legales con el análisis jurídico desde el enfoque del Derecho Procesal Penal.

B) Metodología y técnicas de investigación utilizadas: la estructura formal de la tesis, fue realizada en una secuencia ideal para un buen entendimiento de la misma, así como la utilización de la metodología concerniente al método jurídico e inductivo. En lo que concierne a las técnicas de investigación documentales, comprobándose con ello que se hizo uso de la recolección bibliográfica actualizada.

C) Redacción: la redacción utilizada reúne las condiciones exigidas en cuanto a claridad y precisión, de tal forma que sea comprensible al lector y a las personas que se interesen sobre la utilización de la informática forense dentro del Derecho Procesal Penal guatemalteco.

D) Contribución científica: el aporte científico que el tema investigado por el sustentante, indica la importancia de la aplicación que se le ha dado informática forense en el procesal penal guatemalteco, para así poder resolver casos de alto impacto y de esa forma proveer una mayor seguridad jurídica al momento dictar una sentencia, poniendo de manifiesto la utilidad de esta herramienta importante contra la impunidad.

Lic. Luis Alfonso Campos Ramírez
ABOGADO Y NOTARIO

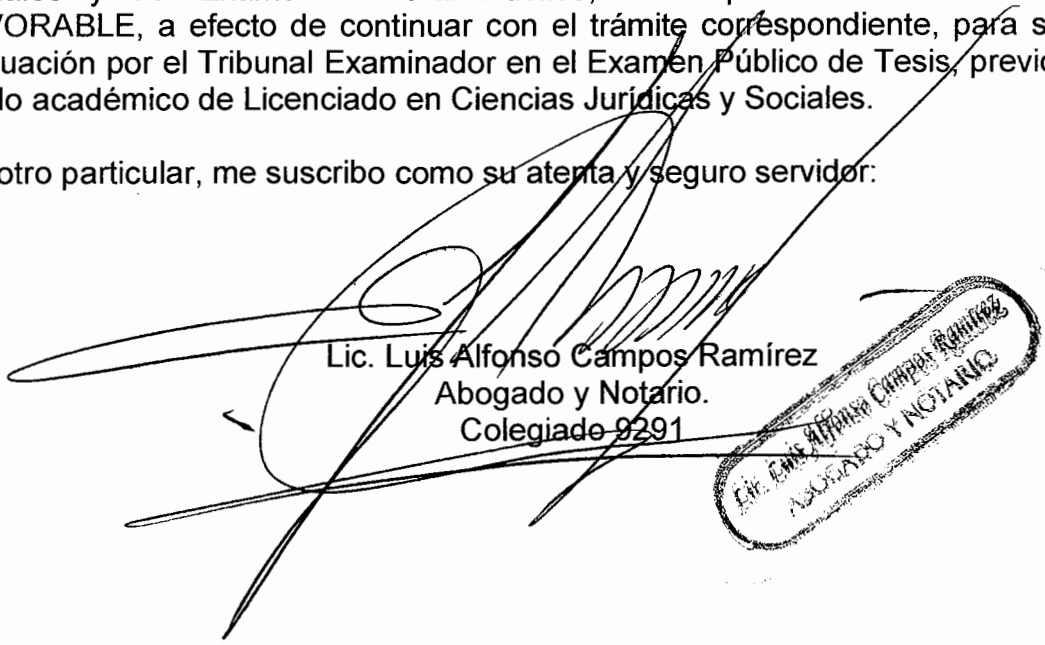


E) Conclusiones y recomendaciones: las conclusiones y recomendaciones son acertadas y oportunas, reflejan el conocimiento del tema investigado, denotando además, la existencia de variadas conducta que obligan a la autoridades, a mantener actualizados a todas las personas que actúan dentro de la administración de justicia, tanto del Organismo Judicial, como del Ministerio Público, Defensa Pública Penal, y Policía Nacional Civil, entre otras, así como realizar una campaña de información para la población acerca de las conductas delictivas que han surgido.

F) Bibliografía utilizada: cabe destacar que la bibliografía utilizada es reciente, acorde y exacta para cada uno de los temas desarrollados en la investigación realizada.

En definitiva, el contenido del trabajo de tesis, se ajusta a los requerimientos científicos que se deben cumplir de conformidad con los requisitos exigidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciaturas en Ciencias Jurídicas y Sociales y del Examen General Público, razón por la cual emito DICTAMEN FAVORABLE, a efecto de continuar con el trámite correspondiente, para su posterior evaluación por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Sin otro particular, me suscribo como su atenta y seguro servidor:



Lic. Luis Alfonso Campos Ramírez
Abogado y Notario.
Colegiado 9291





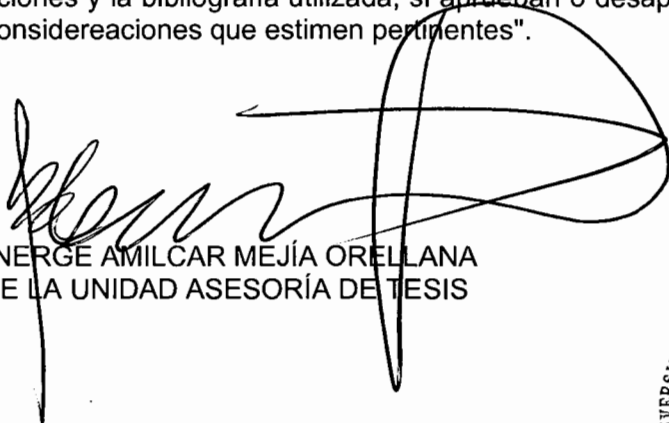
FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, Guatemala

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.
Guatemala, 05 de septiembre de 2012.

Atentamente, pase a el LICENCIADO EDGAR ANIBAL ARTEAGA LOPEZ, para que proceda a revisar el trabajo de tesis de el estudiante JOSE DANIEL RUIZ ALQUIJAY, intitulado: "LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO IMPACTO SOCIAL EN GUATEMALA".

Me permito hacer de su conocimiento que está facultado para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título del trabajo de tesis. En el dictamen correspondiente deberá cumplir con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual establece: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".



DR. BONERGE AMILCAR MEJÍA ORELLANA
JEFE DE LA UNIDAD ASESORÍA DE TESIS

cc.Unidad de Tesis
BAMO/sllh.

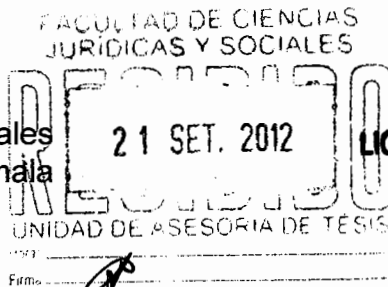


Lic. Edgar Anibal Arteaga Lopez.
3ª calle "C" 10-57, zona 6 de Villa Nueva,
departamento de Guatemala. Tel. 66320782

Guatemala, 19 de septiembre de 2012.



Doctor:
Bonerge Amilcar Mejía Orellana
Jefe de la Unidad Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Presente.



LIC. EDGAR ANIBAL ARTEAGA LÓPEZ
ABOGADO Y NOTARIO

Respetable Doctor:

De conformidad con el nombramiento emitido el cinco de septiembre del año en curso, en el cual se me faculta para realizar las modificaciones de forma y de fondo en el trabajo de investigación como Revisor de Tesis del Bachiller José Daniel Ruiz Alquijay, me dirijo a Usted haciendo referencia a la misma con el objeto de informar mi labor y oportunamente emitir dictamen correspondiente, en relación a los extremos indicados en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, se establece siguiente:

I) El trabajo de tesis se denominó originalmente "LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO IMPACTO SOCIAL EN GUATEMALA".

II) Al realizar la revisión sugerí correcciones que en su momento consideré necesarias para mejorar la comprensión del tema desarrollado, las cuales en su momento se corrigieron, constando la presente tesis en cinco capítulos realizados en un orden lógico y siendo un tema de carácter penal y jurídicamente importante, siendo un aporte invaluable.

III) En relación a los extremos indicados en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público se establece lo siguiente: a) Contenido científico y técnico de la tesis: El sustentante abarca tópicos de importancia en materia penal enfocado desde un punto de vista jurídico-penal, por ser un tema importante que se enfoca a la realidad de nuestro país en cuanto al uso forense de los medios de informática para la resolución de aquellos casos que son catalogados como de alto impacto. b) La metodología y técnicas de la investigación: Para el efecto se tiene como base el método analítico, para comprender los elementos o componentes característicos de la importancia que tiene la informática forense, par la resolución de los casos que se califican como de alto impacto y su incidencia en el sector justicia en materia penal; y por último las técnicas investigativas, siendo la bibliográfica y documental para recopilar y seleccionar adecuadamente el material de estudio, ya que a través de las cuales se estudió el tema investigado y culminó con la comprobación de la hipótesis planteada estableciendo los objetivos generales y específicos con el objeto de establecer doctrinaria y jurídicamente las repercusiones legales en su utilización para la solución de los casos de índole penal de alto impacto en Guatemala; c) La redacción: la estructura formal de la tesis está

Lic. Edgar Anibal Arteaga Lopez.
3ª calle "C" 10-57, zona 6 de Villa Nueva,
departamento de Guatemala. Tel. 66320782



compuesta de cinco capítulos se realizó en una secuencia ideal empezando con temas que llevan al lector poco a poco al desarrollo del tema central para el buen entendimiento del mismo que ha cumplido con todos los procedimientos del método científico; d) Conclusiones y recomendaciones: Las mismas obedecen a una realidad jurídico penal. Conclusión importante a la cual arribó el sustentante es la importante necesidad de regular la conducta delictiva que se comete dentro de la informática y la importante necesidad de utilizar las técnicas informático-forenses para la resolución de los casos que de allí se deriven. Además, se comprobó que la bibliografía fuera correcta, así como que los métodos y técnicas se aplicaran adecuadamente, en virtud que con ellos, se obtuvo la información necesaria y objetiva para la elaboración, redacción y presentación final del presente trabajo.

IV) En conclusión y atendiendo a lo indicado en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, informo a usted, que APRUEBO, ampliamente la investigación realizada, por lo que con respecto al trabajo realizado por el sustentante, Bachiller José Daniel Ruiz Alquijay, emito DICTAMEN FAVORABLE, ya que considero el tema constituye un importante aporte.

Sin otro particular, me suscribo de usted, con muestras de mi consideración y estima.


LIC. EDGAR ANIBAL ARTEAGA LÓPEZ
ABOGADO Y NOTARIO
Lic. Edgar Anibal Arteaga López
Abogado y Notario - Col. 5791



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES
Ciudad Universitaria, zona 12
GUATEMALA, C.A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 29 de octubre de 2012.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JOSÉ DANIEL RUIZ ALQUIJAY, titulado LA UTILIZACIÓN DE LA INFORMÁTICA FORENSE EN LOS CASOS DE ALTO IMPACTO SOCIAL EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

BAMO/iyf.

Lic. Avidán Ortiz Orellana
DECANO



Rosario





DEDICATORIA

- A Dios:** Por haberme dado la vida e iluminado mi camino en todo momento.
- A la Virgen María:** Por su ejemplo y amor maternal.
- A mis Padres:** José Arcadio Ruiz Arreaga y Adela Alquijay Argueta, gracias por su amor, ayuda, sabiduría y comprensión.
- A mi esposa:** Cynthia Betzaida Tobar Yanes, por su amor y comprensión constante.
- A mi hermano:** Francisco Javier Ruiz Alquijay por su ayuda incondicional, cariño y por que cada día me enseña nuevas facetas de lo que significa tener una familia.
- En especial a:** María Yanes, por su cariño y apoyo incondicional.
- A mis amigos:** Mary, Isabel, Astrid, Silvia, Robin, Gerson, Ragde, Ursy, Ribel, Karen, Ricardo, Mardo, Melvin y a las familias Gómez Quiroa, Hidalgo Calderón y Quixtan Sum, con aprecio y cariño.
- A la Universidad de San Carlos de Guatemala y a la Facultad de ciencias Jurídicas y Sociales:** Por haberme enseñado más que derecho, una filosofía para la vida.



ÍNDICE

	Pág.
Introducción	i

CAPÍTULO I

1. Derecho, informática y derecho penal	1
1.1. La informática y el derecho	1
1.2. El derecho como una ciencia	3
1.3. La época del ciber-jurista y los ciber-tribunales	6
1.4. Derecho informático	8
1.5. Derecho penal	11
1.6. El derecho penal y la complementación del derecho informático	12
1.7. El derecho informático y su relación con otras ciencias	14

CAPÍTULO II

2. Crimen informático y derecho penal	27
2.1. Generalidades de los delitos vinculados a la informática	27
2.2. El delito informático	28
2.3. La teoría del bien jurídico	30
2.4. Crimen informático, criminalidad informática o delitos informáticos	32
2.5. Bienes jurídicos penales en el delito informático	33
2.6. Problemas de interpretación en la delincuencia informática	38
2.7. Efectos procesales del tema	41

CAPÍTULO III

3. El derecho penal informático	45
3.1. Noción e ilustración del derecho penal informático	45
3.2. La elación entre el derecho penal y la informática	46
3.3. Acciones ilegales suscitadas con el uso de la informática	49



Pág.

3.4. Las innovadoras tecnologías de la informática.....	50
---------------------------------------------------------	----

CAPÍTULO IV

4. La informática forense.....	53
4.1. Noción y definición.....	54
4.2. La evidencia digital.....	57
4.3. Protocolo de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.....	58
4.4. La cadena de custodia de las evidencias digitales.....	60
4.5. Análisis de los medios informáticos.....	61
4.6. Reconocimiento de la evidencia digital.....	61
4.7. La validación y confiabilidad de las herramientas forenses en la informática.....	61

CAPÍTULO V

5. El manejo de la informática en el esclarecimiento de los casos de alto impacto en el ordenamiento jurídico penal guatemalteco.....	65
5.1. Generalidades del fenómeno estudiado.....	66
5.2. Las tecnologías de la información y el proceso penal.....	68
5.3. Las tecnologías de la información y la investigación criminal.....	71
5.4. La administración de justicia y los retos del Estado ante la guerra frente a la Criminalidad.....	72
5.5. El derecho a la autodeterminación informativa.....	75
5.6. Funcionalización del derecho penal en el estado de derecho.....	80
5.7. Procesos penales en boga en Guatemala donde se utilizó la informática.....	83
CONCLUSIONES	97
RECOMENDACIONES	99
BIBLIOGRAFÍA	101



INTRODUCCIÓN

Las nuevas tecnologías de la información generan transformaciones en la sociedad. Es indudable que sus adelantos fraguan una nueva época en la historia de la humanidad. La informática y las telecomunicaciones indistintamente facilitan el desarrollo de internet, elemento revelador de las nombradas nuevas tecnologías de la información. La informática entendida, permite almacenar y alternar grandes cantidades de información, mientras las telecomunicaciones enlazan a personas situadas en lugares alejados entre sí, con sorprendente facilidad en breve tiempo.

La constante ola de criminalidad y organización criminal en Guatemala, el aprovechamiento de las fallas humanas al utilizar procedimientos tecnológicos para concertar los delitos, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con la manera de identificar a los responsables de tales ilícitos y resolver los casos en concreto, utilizando como medio la informática forense en el derecho procesal penal. A pesar del escenario anterior, la informática forense ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales.

Con esta investigación se persiguen varios objetivos, como lo son: determinar la complementación entre la informática forense, el derecho penal y el derecho procesal penal para el esclarecimiento de los casos de alto impacto en el ordenamiento jurídico penal guatemalteco y fomentar en el medio, el empleo de la tecnología con responsabilidad, ya que el usuario debe tener presente que este beneficio tecnológico de comunicación rápido y económico tiene que usarse con responsabilidad, sobre todo en la administración de la información.

Además, la hipótesis formulada oportunamente, fue comprobada, al apreciar la necesidad de incorporar la informática forense en el proceso penal guatemalteco, para coadyuvar al esclarecimiento de la verdad histórica de los hechos punibles que se juzgan, sobre todo, en lo referente a casos de alto impacto.



En este estudio, se tomó en cuenta el método dialéctico, en virtud que éste se apoya, tanto en el método inductivo como en el deductivo, lo cual permitió partir de proposiciones particulares para alcanzar proposiciones generales y viceversa. Además, dicho recurso metodológico hace uso del método de análisis, de los elementos que se investigan o examinan, para posteriormente sintetizar y obtener un nuevo punto de vista.

Esta tesis está integrada en cinco capítulos, los cuales se detallan a continuación: En el primero, se aborda el tema de derecho informático y derecho penal; el segundo, trata el crimen informático y derecho penal; el tercero, se relaciona con el derecho penal informático; el cuarto, capítulo contiene el tema de la informática forense y; en el quinto, se aborda el manejo de la informática en el esclarecimiento de los casos de alto impacto en el ordenamiento jurídico penal guatemalteco.

Al concluir este estudio se puede decir que la informática forense hace, entonces, su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiera aportar en un proceso de alto impacto social en Guatemala.



CAPÍTULO I

1. Derecho, informática y derecho penal

Entre el Derecho y la **informática** se podrían apreciar dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la informática jurídica. Pero al considerar a la informática como objeto del derecho, se hace alusión al derecho de la informática o simplemente derecho informático.

1.1. La informática y el derecho

El derecho, implica una serie de normas obligatorias, se puede sancionar a aquellas personas que no cumplan esas normas. El derecho no puede tener normas que regulen todo a priori, entonces se recurre a la moral o a la ética para rellenar esas lagunas. Puede decirse que una de las formas en que se relaciona el derecho con la informática, se debe a la protección de la intimidad. Existen varias soluciones para la protección de la intimidad. Deontológica: consiste en la elaboración de códigos o principios de comportamiento ético en materia de informática; se creyó que la única manera de controlar el uso indebido de la informática era la elaboración de códigos deontológicos. Esta solución deontológica no es suficiente. Jurídica: Consiste en encauzar a través del derecho los problemas que plantea la informática. Hay que tener en cuenta que la solución jurídica se ramifica en dos términos:

- a. Informática jurídica: supone la utilización de la informática por los juristas.



b. Derecho informático: conjunto de principios y reglas que contemplan las actividades llevadas a cabo por sistemas informáticos. El espacio jurídico del derecho informático es muy amplio.

La relación entre derecho e informática tiene dos líneas de investigación: los aspectos normativos del uso de la informática, desarrollados bajo el derecho de la informática, y la aplicación de la informática en el tratamiento de la información jurídica, conocida como informática jurídica. Al respecto, se señala que el punto de partida deriva de la constatación de un fenómeno: El razonamiento jurídico, el cual no constituye una operación aislada, sino que se integra dentro de un proceso compuesto de varias etapas.

Sin profundizar en el estudio de la lógica del raciocinio jurídico, se ha señalado que el origen de la informática jurídica, parte de un sistema lógico-interpretativo del mismo, ya que al respecto se ha determinado que la lógica del derecho es el estudio sistemático de la estructura de las normas, los conceptos, y los razonamientos jurídicos, esto es porque aluden siempre al orden del ser, y aseveran que a tal o cual objeto conviene o no, tal o cual determinación.

El discurso jurídico está basado en un sistema normativo, que parte de proposiciones lógicas en cuanto al ser y al deber ser, y de la combinación en una cierta estructura surge el ordenamiento jurídico, que constituye el objeto mismo de la ciencia del derecho.

Por tanto, se puede decir que el desarrollo de la informática jurídica parte del establecimiento de un sistema cuyos elementos están íntimamente ligados con el fin de crear, a su vez, otros sistemas organizativos y estructurales de la información jurídica.

De esto debe partir precisamente la informática jurídica. Sin embargo, es necesario determinar que la misma analiza, reestructura, amplía y formaliza términos cibeméticos-informáticos al propio derecho. Entiéndase la cibemética e informática como el estudio interdisciplinario de la estructura de los sistemas reguladores de la información. Es decir, la informática jurídica en el desarrollo de la humanidad, ha venido creando nuevas teorías, nuevas doctrinas, nuevos conceptos jurídicos fundamentales los cuales hoy en día, norman nuevas conductas de las personas.

1.2. El derecho como una ciencia

Importantes e influyentes corrientes como la de Luis Recaséns Siches en el panorama del pensamiento jurídico del siglo XX sostienen que el derecho es, en lo fundamental, un conjunto de normas y principios generales. De ello se sigue que la ciencia es un conocimiento sistemático del aspecto normativo del derecho. Esta parte del trabajo quiere ofrecer una visión diferente, proponiendo que el saber propiamente jurídico ni es general ni tiene por principal objeto lo normativo. Es conocimiento jurídico por excelencia aquel que informa la decisión de una contienda específica entre partes. Que tal sea el sentido primario de nuestra scientia, saber de lo justo en una causa particular, tiene consecuencia porque lo más importante que hacemos en ejercicio del hermoso arte del derecho es con miras a la decisión de un conflicto actual o potencial.



Que el derecho sea esencialmente el conjunto de normas y principios generales que regulan coercitivamente el comportamiento de los seres humanos que vivimos en sociedad, es algo que de tan repetido llega a parecer evidente, no necesitado de mayor explicación. El fenómeno más propio de lo jurídico, se dice y reitera, encuentra su foco en la ley, paradigma de la regla general de conducta, por lo cual los saberes jurídicos son conocimientos organizados referidos fundamentalmente a normas generales y a los principios que de esas normas se deducen.

Revisando los textos que más influencia han tenido en la formación jurídica en el mundo durante el siglo veinte, no es otra la visión que se obtendrá.

“El derecho es el conjunto de reglas a cuya observancia el hombre puede y debe ser obligado por la fuerza.”¹

“A su vez, se vale habitualmente de la voz “derecho” en el sentido de regla o ley y describe el ordenamiento jurídico como un conjunto de normas.”²

Culminando con la tradición intelectual mencionada, se señala que:

“Derecho objetivo es el conjunto de normas que, en una sociedad organizada y autónoma, disciplinan, generalmente bajo amenaza de sanción, el comportamiento de los miembros de

¹ Claro Solar, Luis. **Explicaciones de derecho civil chileno y comparado**. Santiago: Editorial Jurídica de Chile, 1978. Pág. 4.

² Pescio, V. **Manual de derecho civil**. Tomo I. Santiago: Editorial Jurídica de Chile, 1978. Pág. 25.

ella en las relaciones que entablan entre sí para satisfacer sus necesidades materiales y espirituales y lograr el bien común.”³

“El pensamiento jurídico nacional en la materia no se aparta en esto de tendencias que predominan en diversas tradiciones jurídicas. La tradición continental, centrada en la obra de Hans Kelsen, y la tradición del derecho común cuyos mejores expositores han sido Austin y H. L. A. Hart, comparten en lo sustancial la idea de que el derecho es principalmente un asunto de normas. La norma fundamental hipotética propuesta por Kelsen y la regla de reconocimiento de Hart son, pese a múltiples diferencias entre ellas, ilustraciones de la preeminencia que lo normativo tiene en sus respectivos sistemas de explicación del derecho.”⁴

Vodanovic, resumiendo muchos decenios de docencia jurídica nacional, expone que: “La Ciencia del Derecho se ocupa del origen y evolución de los principios teóricos y normas de orden jurídico, sea en un país determinado o en el mundo en general: compara las instituciones jurídicas de diversos países y las agrupa en sistemas, atendiendo a sus caracteres fundamentales comunes; también analiza las diferencias legislativas en el tiempo; de acuerdo con las necesidades sociales, prevé los cambios de los ordenamientos jurídicos y se adelanta a proponer las soluciones y, en fin, concibe diversos métodos de interpretación del derecho.”⁵

³ Vodanovic, Antonio. **Tratado de derecho civil: parte preliminar y general**. Tomo I. Santiago: Editorial Jurídica de Chile, 1998. Pág. 15.

⁴ Streeter Prieto, Jorge. **Ensayo la ciencia del derecho**. Universidad de Santiago de Chile, Chile, 2002. Pág. 286.

⁵ Vodanovic, Antonio. **Ob. Cit.** Pág. 15.

Un autor extranjero de similar opinión señala que: “Se denomina ciencia jurídica a aquella disciplina que trata de conocer el derecho desde el punto de vista normativo, es decir, tiene como objeto la descripción del aspecto normativo del derecho o, mejor, el derecho visto como conjunto de normas.”⁶

Si se concibe el derecho como un conjunto de normas generales y principios, y si se cree también que la ciencia no es de lo singular, sino de lo general, pareciera que lo que han tratado de hacer juristas de los siglos XIX y XX es, hasta donde lo permite la naturaleza especial de lo que aceptan como res iuridica, construir una disciplina al estilo de la geometría, como la jurisprudencia de conceptos, o al modo de la física, como la jurisprudencia de intereses, entendidos éstos casi como fuerzas de acción y reacción.

Teniendo un objeto como son las reglas generales, la demanda de verdad que hace toda ciencia estaría satisfecha por la coherencia de las proposiciones que se mientan sobre las normas, construidas en un sistema u ordenamiento jurídico.

1.3. La época del ciber-jurista y los ciber-tribunales

Davara Rodríguez destaca en su manual de derecho informático: “En el mundo jurídico, con la utilización de los modernos medios técnicos, el derecho adquirirá precisión y claridad, tanto en su comprensión como en su aplicación, y las nuevas tecnologías asociadas al ordenador cambiarán los métodos y estructuras de pensamiento del jurista.”⁷

⁶ A., Calsamiglia. **Ciencia Jurídica. El derecho y la justicia.** Madrid: Editorial Trotta, 1996. Pág. 17.

⁷ Davara, Rodríguez, Miguel Ángel. **Manual de derecho informático.** Pamplona: Aranzadi. 1997. Pág. 22.



Sigue diciendo Davara Rodríguez:

“Por ello debemos adaptarnos a estos nuevos métodos, de forma que retomemos los antiguos problemas bajo una óptica diferente y adecuemos nuestra actividad jurídica al desarrollo tecnológico.” (Davara, 1997: 22).

La sociedad camina en nuestros días hacia la época plena del “ciberjurista”. Cada vez crece la conciencia de que el proceso abierto con el avance de las nuevas tecnologías de comunicación es irreversible. Van en aumento los bufetes jurídicos que proporcionan sus servicios a través de internet: Asesoría y práctica jurídica interactiva a través de la red.

La información es calificada como un auténtico poder de las sociedades avanzadas. Ya tenía su importancia en la antigüedad, pero con el desarrollo de la telemática su valor ha crecido de forma tal que se dirige a un futuro prometedor para todos.

El comercio, por ejemplo, ha sido pionero en innovaciones jurídicas introducidas en el pasado por medio de la costumbre. Actualmente está en pleno desarrollo el e-commerce.

A propósito de Guatemala, Miguel Ángel Rodríguez, afirmó durante un seminario de la Cámara de Comercio e Industria Guatemalteco Mexicana, en el año 2,002, “que la falta de confianza de los comerciantes guatemaltecos en las transacciones por Internet, ha hecho que nuestro país se beneficie poco de las ventajas que ofrece la Web.”⁸

⁸ Barrera López, Horacio Mauricio. **Derecho informático en la curricula universitaria**. Universidad de San Carlos de Guatemala. Guatemala. 2003. Pág. 36.

Dijo este técnico que “aún hay empresarios en Guatemala que se resisten a utilizar la Web, principalmente por temor a la posibilidad de que los números de las tarjetas de crédito sean interceptados y utilizados por hackers o piratas interactivos. Añadió que todos estos temores desaparecerán en la medida en que el público conozca que existe un amplio mecanismo jurídico que lo defiende.”⁹

Inicialmente las transacciones económicas se venían realizando a través de los medios electrónicos, sin más soporte legal que el pacto entre las partes. Sin embargo, la contratación electrónica poco a poco se viene abriendo paso y crece en forma espectacular. Una vez más los hechos caminan delante del derecho, entendiendo éste como derecho positivo. Muchas veces sucede que cuando tratamos de adecuar estos nuevos hechos a las figuras jurídicas existentes, se encuentran con dificultades. Las viejas instituciones jurídicas que a través de los siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo respecto a estas nuevas tecnologías, en cierto modo protestan y las admiten con reservas. Así ocurre cuando se trata de adaptar el concepto de firma, tal como antiguamente se concebía al nuevo campo de las transferencias electrónicas.

1.4. Derecho informático

Se puede definir el derecho informático, derecho de internet o informática Jurídica como: “El conjunto de doctrinas, principios y normas jurídicas que estudian las

⁹ Loc. Cit.



modernas tecnologías de la información, los derechos y obligaciones que nacen de la utilización de la computadora, el internet y el ciberespacio, en busca de la protección de sus usuarios en particular y de la humanidad en general.”¹⁰

El registro de marcas y patentes es una de las actividades de los abogados especializados en Derecho Mercantil que más auge ha cobrado en los últimos años en los países desarrollados. La Organización Mundial de la Propiedad Intelectual (OMPI), que administra los tratados mundiales sobre marcas, busca imponer un tratado de marca global a los países del mundo, especialmente en Latinoamérica. Un sistema global de representación de marcas, junto con un sistema de seguimiento y administración de marcas, que permita que los gobiernos de cada país no pierdan su recaudación por estos trámites y que los bufetes de marcas de cada uno de los países no pierdan el trabajo profesional.

El hecho de utilizar Internet nos habla de la urgencia de que sean abordados estos temas en nuestra escuela de derecho, con total profundidad, por medio de una asignatura específica, dispuesta dentro de la modernización del plan de estudios de todas la Universidades del país.

La Informática no es ajena al Derecho, aunque en algunas ocasiones parezca estarlo o quererlo y, por ello, en las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las modernas tecnologías de información y las comunicaciones, surgen los problemas de cómo resolver determinados conflictos nacidos de esa relación.

¹⁰ *Ibíd.* Pág. 38.

Así, por ejemplo con la necesidad de una relación jurídica de los derechos y obligaciones consecuentes de la creación, distribución, explotación y/o utilización del hardware y software, con su protección de los derechos de propiedad intelectual.

Conviene que exista una regulación sobre:

- a. "Las responsabilidades, derechos y obligaciones, derivados de la transferencia electrónica de fondos monetarios o de datos, incluso entre diversos países con diferentes regulaciones jurídicas, y las responsabilidades consecuentes de operaciones en cadena, por medio de redes de comunicaciones pertenecientes a distintos territorios y bajo dispares ordenamientos jurídicos.
- b. La validez probatoria de los documentos generados por medios informáticos, o que se encuentran en soportes susceptibles de tratamiento informático.
- c. El llamado delito informático, al hacer referencia al delito cometido por, o sobre, medios informáticos.
- d. Los derechos de los compradores, y usuarios en general, ante la posición dominante de algunas multinacionales de la Informática.
- e. La vigencia de las leyes de defensa de la competencia frente a los grandes productores y distribuidores de Informática.
- f. La protección jurídica del software, considerado hoy en día como un bien inmaterial, que necesita para su elaboración una gran carga de creatividad intelectual, contra la llamada piratería del software.

- g. El desarrollo de las telecomunicaciones, a partir de un mercado como el actual, monopolista y oportunista, negocio que necesita la normativa adecuada.
- h. En el marco jurídico del internet, internacional y nacionalmente se registran los nombres de dominio, o sea la asignación de direcciones numéricas a los usuarios de la internet, específicamente quienes tienen una presencia permanente, como la página web.”¹¹

1.5. Derecho penal

El derecho penal es el conjunto de normas jurídicas que regulan la potestad punitiva del Estado, asociando a hechos, estrictamente determinados por la ley, como presupuesto, una **pena**, medida de seguridad o corrección como consecuencia, con el objetivo de asegurar los valores elementales sobre los cuales descansa la convivencia humana pacífica.

Cuando se habla de **derecho** penal se utiliza el término con diferentes significados, de acuerdo a lo que se desee hacer referencia; de tal modo, se puede mencionar una clasificación preliminar tal como: derecho penal sustantivo, y por otro lado, el derecho penal adjetivo o **procesal penal**.

El primero de ellos está constituido por lo que generalmente conocemos como **Código Penal** o **leyes** penales de fondo, que son las **normas** promulgadas por el Estado,

¹¹ **Ibíd.** Pág. 39

estableciendo los **delitos** y las penas, mientras que el **derecho procesal penal** es el conjunto de **normas** destinadas a establecer el modo de aplicación de aquellas.

El derecho penal no se reduce sólo al listado de las conductas consideradas **delitos** y la **pena** que a cada uno corresponde, sino que –fundamentalmente– su misión es proteger a la **sociedad**. Esto se logra a través de medidas que por un lado llevan a la separación del **delincuente** peligroso por el tiempo necesario, a la par que se reincorpora al medio social a aquellos que no lo son mediante el tratamiento adecuado en cada caso para lograr esta finalidad.

La fuente del derecho es aquello de donde el mismo emana, de dónde y cómo se produce la norma jurídica. Entonces, la única fuente del derecho penal en los sistemas en los que impera el principio de legalidad es la **Ley**, de la cual emana el poder para la construcción de las demás normas y su respectiva aplicación, por lo tanto, sólo ésta puede ser la creadora y fuente directa del derecho penal.

1.6. El derecho penal y la complementación del derecho informático

La rápida evolución de la informática ha dado lugar al apareamiento de delitos nuevos, muchos de ellos pertenecientes al campo penal.

“Se considera que un delito informático es cualquier comportamiento ilegal en el que está involucrada una computadora. También se habla de actitudes ilícitas en que se tiene a la computadora como instrumento, como los casos del uso indebido del



software, la apropiación indebida de datos, o la interferencia en sistemas de datos ajenos.”¹²

Generalmente, los supuestos “delincuentes informáticos” pueden encontrarse entre algunos operadores, programadores, analistas de sistemas, analistas de comunicaciones, supervisores, ingenieros en sistemas o funcionarios superiores. Víctimas de la delincuencia informática, según numerosos casos reportados por la prensa internacional, pueden ser empresas e instituciones, tales como bancos, compañías financieras, aseguradoras, universidades y entes estatales.

Diariamente el delito informático provoca grandes pérdidas económicas por robo de identidad, falsificación de cheques y tarjetas de crédito, variación de los activos y pasivos en las contabilidades, modificación, copiado y robo de información, uso no autorizado de programas de cómputo, alteración en el funcionamiento de los sistemas, acceso a áreas informatizadas en forma no autorizada e intervención en líneas de comunicación de datos o teleproceso.

En Guatemala el Código Penal (Decreto 17-73)⁴⁵, regula el Delito Informático en el título VI, CAPÍTULO VII: “De los delitos contra el Derecho de Autor, la Propiedad Industrial y Delitos Informáticos”, artículos 274 “A” al 274 “G”, contenidos en el Decreto 33-96 del Congreso de la República.

¹² Loc. Cit.

1.7. El derecho informático y su relación con otras ciencias

a. Con el derecho constitucional

“El Derecho Informático está relacionado con el Derecho Constitucional, pues debe dar atención prioritaria a la protección de los datos personales, de los derechos individuales, entre ellos el derecho a la intimidad. La privacidad de la libertad informática es concebida por algunos autores como: “el derecho de autotutela de la propia identidad informática”. En cuanto a la protección de los datos personales, hay que tomar en cuenta que existen recopilaciones en numerosos archivos con información como: fecha y lugar de nacimiento, domicilio, estado civil, raza, religión, inclinaciones políticas, ingresos monetarios, cuentas bancarias, historia clínica, los cuales son recopilados por diferentes entes, como los registros civiles, médicos, académicos, culturales, políticos, administrativos, fiscales, bancarios, laborales y otros, los cuales actualmente pueden estar a disposición de un interesado, para diferentes fines, en forma instantánea.”¹³

El derecho informático protege a las personas de que la información contenida en las bases de datos pueda ser empleada con fines publicitarios, comerciales, fiscales o policíacos, actividades que pueden alterar los derechos fundamentales de la sociedad, al margen de la Ley.

¹³ *Ibíd.* Pág. 41.



Todos los seres humanos tienen derecho a mantener su intimidad y la información que sobre ellos esté registrada en archivos escolares, universitarios, profesionales, médicos, políticos, financieros o religiosos.

Con la informática ha surgido la necesidad de proteger la vida privada de las personas, para evitar que la computadora se convierta en un instrumento para la comisión de actos ilícitos.

La protección de los datos personales y el derecho a la privacidad están amparados por figuras jurídicas como los derechos humanos, los derechos personales, los derechos patrimoniales, las libertades públicas y privadas, el derecho de la privacidad, el derecho a la intimidad y al honor de las personas, las garantías individuales y sociales.

En algunos países no existe una legislación adecuada para la protección de los datos personales, por lo que son necesarias leyes que tiendan a proteger la información de las personas, la libertad de gozar de dicha información y de regular el abuso que pueda ocurrir, menoscabando los intereses de las personas. Hay que recordar que en Guatemala es pública la información contenida en los registros: civil, mercantil, industrial, fiscal, de la propiedad, judicial, municipal, policiaco, etc.

b. Con el Derecho Administrativo

La administración jurídica del Estado se ha visto favorecida en numerosos países con el surgimiento de la Informática. Los profesionales encargados de realizar las

funciones administrativas, particularmente los abogados y notarios, cada vez hacen más uso de modernos equipos de computación.

Gracias a la Informática, el gobierno del Estado, ejercido por medio de los organismos Ejecutivo, Legislativo y Judicial, lleva a cabo con mayor rapidez sus funciones administrativas esenciales, definidas por los autores clásicos como: planificación, organización, dirección, coordinación y control.

El tratadista Jorge Mario Castillo González, en su obra *Derecho Administrativo*: “Destaca que esta ciencia jurídica vela por el bienestar, la felicidad y la vida de todos los seres humanos, y que tales propósitos se cumplen en el momento que persigue el buen funcionamiento de los mecanismos administrativos que rodean y que apoyan a los habitantes del país. Añade que en la sociedad moderna, la calidad de la administración, en cuanto ésta afecta vidas humanas, constituye la principal preocupación del Derecho Administrativo.”¹⁴

La rápida comunicación que permite la red de internet, por ejemplo, favorece la administración estatal que controla la producción, comercialización, calidad y precios de los productos, el financiamiento y los créditos para vivienda, la administración que vela por la propia institucionalidad, la salud popular, el control de los precios de las medicinas y el buen funcionamiento de los hospitales, etc.

¹⁴ Castillo González, Jorge Mario. *Derecho administrativo guatemalteco*. Guatemala. Editorial Impresiones Gráficas. 2005. Pág. 20.



c. Con el derecho procesal

En algunos países desarrollados existe ya la informatización del proceso jurídico, tanto en lo que se refiere a las soluciones de trámite, como a las que el juez elabora, tomando en cuenta modelos pre-formateados.

La Informática permite, de modo automático y con ayuda de un banco de datos, la realización de demandas pre-formateadas, la contestación, la realización de actos y documentos y el seguimiento de procesos.

En la fase probatoria, mediante la Informática existe la posibilidad de simular situaciones, se pueden verificar datos de identificación personal, compilar, organizar información durante el curso del proceso y efectuar comparaciones.

La prueba documental comprende todos los objetos materiales existentes, entre los que se encuentran los documentos electrónicos. El documento electrónico es uno de los mejores instrumentos de la Informática, pues constituye una prueba de carácter documental. También se considera documento electrónico aquel que ha sido creado en una computadora, grabado en un soporte informático, producido y reproducido. La falta de firma de los documentos informáticos no los inhibe como material probatorio.

Los medios de prueba informáticos consisten en: discos, cintas o cualquier clase de archivos magnéticos o de uso computacional, y en la reproducción por cualquier medio.

d. Con el derecho del trabajo

Especial atención merece la repercusión que ha tenido la Informática en el campo laboral, pues, por ejemplo, la utilización de la computadora redujo considerablemente el número del personal en muchas empresas.

El Derecho Laboral también debe ocuparse de la actividad informática en lo que se refiere a las jornadas de trabajo para quienes hacen uso de las computadoras, así como los períodos de vacaciones y días de descanso. Asimismo, debe regular los salarios y los riesgos que presenta este tipo de trabajo.

La Informática también está creando un nuevo orden laboral que rebasa nuestro tradicional Código de Trabajo. Plantea una organización descentralizada de las labores de cara al mejor aprovechamiento de los recursos.

Estamos ante la creación de un nuevo mercado de trabajo, totalmente diferente de la mentalidad que prevaleció durante siglos. Está adquiriendo gran fuerza el autoempleo o la generación de sus propios recursos o formas de trabajo por el propio individuo, algo a lo que la mayor parte de la sociedad no estaba acostumbrada.

A la utilización de los medios tecnológicos en la actividad laboral se le llama teletrabajo; o sea que un empleado puede cumplir con sus labores desde un lugar lejano o diferente de la empresa que lo ha contratado, por medio de la utilización de la computadora.



Con este sistema de trabajo el empleador no requiere la presencia física de sus colaboradores en sus oficinas.

Según los tratadistas del Derecho Informático, como el experto español Miguel Ángel Davara Rodríguez, la clásica oficina ya solamente necesita de una computadora, y una conexión telefónica o de internet, aunque ya hay sistemas de computadoras inalámbricas. Lo mismo puede instalarse en la habitación de un hotel que en la sala de espera de un aeropuerto o en el jardín de una residencia, con lo que se dispone de una mayor movilidad y versatilidad.

Es lo que se llama una oficina virtual; aunque no se trata de una oficina virtual sino de una oficina real o un nuevo concepto de oficina.

El teletrabajo surge de la necesidad de ahorro de costos y de tiempo, evitando también los múltiples viajes y reuniones, sustituyéndolos por las tele reuniones mediante videoconferencia y procesamiento de imagen e información.

El nuevo sistema también trae señalados inconvenientes. Se crea un lógico temor a una nueva explotación del trabajador, del tele trabajador, al crearse mayores inconvenientes para la defensa de sus derechos adquiridos a lo largo de los años. La utilización parcial de actividades a distancia plantea varios problemas de cara a una nueva explotación del mundo del trabajo. Se estima que los sindicatos perderán parte importante de su fuerza, siendo otro grupo social que se verá obligado a tomar medidas de organización distintas y una también distinta política de protección del mundo del trabajo.



e. Con el derecho civil

Es evidente la relación que existe entre el Derecho Informático y el Derecho Civil, como puede comprobarse con la responsabilidad civil informática que se deriva del incumplimiento en los contratos informáticos, la protección de los datos personales o de los programas de computación.

En el Código Civil encontramos la protección a la intimidad, con disposiciones que buscan reparar el daño material o moral causado a una persona física o jurídica por incumplimiento o infracción de las obligaciones contractuales o legales.

La responsabilidad informática no se funda únicamente en el campo contractual sobre el incumplimiento del contrato, pues se refiere también a la garantía de responsabilidad por defectos o deterioros de la computadora, la funcionalidad de los programas o el uso ilícito de los elementos informáticos.

Es fundamental el tema de la responsabilidad civil en la informática, especialmente en lo que se refiere a la contratación electrónica. También se considera el fraude, que se produce al no cumplir lo establecido en el contrato o cuando se trata de algún problema derivado de las características del software o del hardware.

También existe la responsabilidad por informes emitidos por un banco de datos que, por ejemplo, proporcione información errónea sobre legislación vigente, que dé motivo a obtener una decisión judicial que cause perjuicio a una persona o institución. Mención

especial merece la protección jurídica de los programas de computación, conocidos como software. Se protegen patentes, diseños, modelos, marcas, Derechos de Autor, secreto industrial y profesional. También se contempla la protección del Derecho de Autor, que es la potestad exclusiva que posee el creador de una obra literaria, científica o artística de usarla, autorizar su uso y disponer de ella o transmitirla por fallecimiento, ya que el Derecho de Autor caduca 50 años después del deceso de éste.

f. Con el derecho mercantil

El vertiginoso avance tecnológico del mundo de la Informática está llevando a la humanidad a un comercio nacional e internacional cada vez más ilimitado. Las redes de comunicación son cada vez más accesibles, más orientadas al servicio y con un costo menor. La explosión informativa está multiplicando las actividades comerciales. Ha crecido el intercambio de datos, sin necesidad de papeleo, con una dinámica mayor y reducción de tiempo.

En el nuevo sistema universal de la información se abren nuevos mercados o se modifican los existentes. Aparece la contratación electrónica, la transferencia de fondos y la utilización de los modernos medios de pago por internet, con el uso a distancia de las tarjetas de crédito, todo lo cual viene siendo estudiado por grupos especializados de la Organización de Naciones Unidas y la Comisión de las Comunidades Europeas, en Luxemburgo.



Relevancia especial debemos dar a la contratación informática. El doctor Miguel Ángel Davara Rodríguez, especialista en el tema, nos habla en su Manual de Derecho Informático sobre qué: "Entendemos por contratación informática aquella cuyo objeto sea un bien o un servicio informático, o ambos, o que una de las prestaciones de las partes tenga por objeto un bien o servicio informático."¹⁵

Los comerciantes están multiplicando sus posibilidades de intercambio de productos por medio del nuevo sistema de comunicaciones. Las operaciones financieras, por medio del correo electrónico están reemplazando a los medios tradicionales de comunicación. Como hemos dicho, muchas son las formas con las que empresas y particulares se benefician de la nueva sociedad de la información; entre ellas:

- la contratación electrónica y
- la transferencia electrónica de fondos.

Según los especialistas, los negocios de hoy dependen cada vez más de los sistemas informáticos, por los que se han hecho particularmente vulnerables, en último término, por la falta de seguridad jurídica en la contratación electrónica.

El término comercio electrónico era sinónimo de compra electrónica. Actualmente abarca los negocios realizados por internet y las tecnologías de la World Wide Web, WWW.

¹⁵ Davara, Rodríguez, Miguel Ángel. **Ob. Cit.** Pág. 35.



g. Con el derecho notarial

La Informática ha venido a revolucionar el desarrollo del derecho notarial y del derecho registral. El tratadista Luis Carral y De Teresa, en su obra Derecho Notarial y Derecho Registral destaca que la institución del notariado tiene una tradición secular dentro de la evolución del derecho hispánico, que se inició con el primer instrumento conocido cuando Argilo vendió unas tierras a Ernulfo en el año de 869, y que ya para el siglo XIV permitió que los notarios adquirieran conciencia corporativa en los estatutos de la Cofradía de San Luis y los sujetó, desde 1341, a sufrir un examen de capacidad, como lo expone la Real Cédula de Pedro IV de Aragón.

La función notarial fue activa para legitimar determinados actos y procedimientos de la conquista y la colonización de los países europeos, como España, Inglaterra, Holanda, Portugal, en el nuevo mundo.

Tal como lo señala el profesor guatemalteco Nery Roberto Muñoz en su Introducción al Estudio del Derecho Notarial, el notariado no se ha quedado al margen de los beneficios de la Informática, cuyos aparatos electrónicos están procesando información y reproduciendo con mayor rapidez los instrumentos públicos.

Muñoz destaca que miles de notarios del sistema latino se han beneficiado con la Informática. Refiere que Italia tiene un centro de informática jurídica con más de



550 terminales conectadas al Centro Electrónico de Documentación de la Corte Suprema de Casación de Roma, y recuerda que en Bruselas, Bélgica, existe el Centro Nacional de Informática, patrocinado por abogados, notarios y otros profesionales. Centros similares operan en Alemania, Austria y España.

Se añade que en el sector público de Guatemala el mejor esfuerzo corresponde al Organismo Judicial, que ha puesto en funcionamiento el Centro Nacional de Información Jurídica CENALEX, que funciona en el edificio de la Corte Suprema de Justicia. Tal centro se ha dedicado a efectuar una recopilación legislativa jurisprudencial y doctrinaria, totalmente actualizada, confiable y de inmediata consulta, además de una sistematización administrativa de la Corte Suprema de Justicia y la Sistematización Judicial de los Tribunales. Por otra parte, el

Organismo Judicial creó el Registro Central de Control de Detenidos (RECEDE), en el cual, a toda hora y hasta por teléfono se puede averiguar en pocos minutos si una persona se encuentra en cualquiera de los centros de detención del país.

Se atribuye al conocido notario Fernando José Quezada Toruño el siguiente razonamiento: "Cuando se habla de computación suele ser común oír términos con los cuales los notarios no estamos del todo familiarizados. Así, por ejemplo, escuchamos hablar de cibernética, memorias, menús, discos, impresoras, pantallas, terminales, microordenadores, procesadores de palabras, Informática, etc., para no citar sino algunos de los conceptos relacionados con la materia que han sido definidos en el idioma español, puesto que debemos reconocer que la



mayor parte de la terminología de ese campo proviene de otros idiomas, principalmente del inglés, y que tales términos han tenido que ser incorporados al lenguaje coloquial, y hasta en el escrito, de quienes se dedican al cultivo de las ciencias tecnológicas.”¹⁶

¹⁶ Quezada Toruño, Fernando José. **La informática jurídica y el notariado en guatemala.** Boletín No. 8 del Instituto Guatemalteco de Derecho Notarial. Guatemala. 2004. Pág. 10.



CAPÍTULO II

2. Crimen informático y derecho penal

Aparte de algunos de los casos ya citados, que podrían ser constitutivos de delito en varias jurisdicciones, quizás los ejemplos más significativos del llamado “Cibercrimen” son la difusión de pornografía infantil y los ataques a sistemas conectados a la Red (inutilización temporal de webs muy conocidas). Pero no deben olvidarse casos de difusión de virus informáticos (que se apoderan de las direcciones de correo almacenadas por el usuario infectado para mandar a nuevas víctimas potenciales “inofensivos” mensajes que al abrirse provocan el desastre) o el acceso no autorizado a ordenadores de terceros, sea para apoderarse de informaciones confidenciales, sea para destruir los sistemas ajenos o sea, simplemente, para probar la fiabilidad de las medidas de seguridad echando una “miradita”.

2.1. Generalidades de los delitos vinculados a la informática

La delincuencia informática se encuadra dentro de lo que se conoce como “Derecho informático”. Éste es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad, incluyendo como objeto de estudio: 1º el régimen jurídico del software; 2º el derecho de las redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho de la privacidad; 7º los delitos informáticos; y 8º otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos.



En lugar de crear una nueva rama del Derecho dedicada exclusivamente al estudio de estos aspectos, podría haberse abordado la regulación o estudio de cuanto concierne al ámbito de digitalización del mundo empresarial, administrativo e incluso personal desde un análisis por cada una de las ramas del ordenamiento jurídico ya existentes, en las que habría que encajar estas nuevas realidades en función del aspecto concreto a analizar. Así, de los contratos electrónicos se ocuparía el Derecho civil o mercantil, de las conductas ilícitas vinculadas a las nuevas tecnologías el Derecho administrativo o penal, etc.

Sin embargo, la complejidad de las relaciones informáticas, el crecimiento desmesurado de las mismas o el hecho de que en el estudio de estas nuevas relaciones se transite de una rama del ordenamiento jurídico a la otra constantemente (administrativa, civil, laboral o penal) ha favorecido que por motivos pragmáticos desde algunos sectores se haya reclamado la consideración de una nueva rama del ordenamiento jurídico que regularía las relaciones, cualesquiera, vinculadas con la informática que tendría como característica, precisamente, el hecho de que en la disciplina confluyan normas administrativas, civiles, laborales, penales, etc.

2.2. El delito informático

La nueva era de la informática o ciber sociedad, al igual que ha ocurrido con otras ciencias o disciplinas, ha dado lugar a delitos.



El doctor en Derecho Miguel Ángel Davara Rodríguez, director del Instituto de Informática Jurídica de la Universidad Pontificia Comillas de Madrid, señala: “Que en la ciber sociedad también se producen violaciones a la Ley.”¹⁷

Un serio problema ocurre cuando tales delitos no están previstos por la ley, en algunos países, debido a que, bien sabido es, no existe delito si no hay una ley que lo contemple (Nullun crimen, nulla poena, sine lege).

Se le da el nombre de delito informático a: un acto que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático o telemático, o vulnerando los derechos del titular de un elemento informático.

En muchos países no existe el delito informático en la legislación, ni se admite que exista como tal, por lo que habría que hacer uso de la interpretación analógica, como única forma para encuadrar los hechos ilícitos que no se encuentren tipificados en la legislación penal, por ejemplo. La analogía logra resolver las lagunas que existen en el Derecho, aunque algunos juristas destacan que este procedimiento atenta contra el principio de legalidad. Nos referimos a la comisión de un delito por medios informáticos, ya que otros ilícitos en este campo sí están contemplados dentro del Derecho Penal.

Es necesario que las distintas legislaciones de los países tipifiquen delitos para el ámbito informático. Por ejemplo, el Departamento de Justicia de los Estados Unidos

¹⁷ Davara Rodríguez, Miguel Ángel. Ob. Cit. Pág. 107.



define que Delito Informático así: Es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática sea esencial para su comisión.

Los delitos son cometidos en este campo por hackers, crackers y phreakers, piratas que actúan contra o mediante el sistema.

En Guatemala, por ejemplo, la piratería de programas software para computadora causó pérdidas por 198 millones de quetzales durante el año 2006, según informó la organización Business Software Alliance (BSA). Los programas más copiados fueron Windows y Office de Microsoft.

En seis mil setecientas empresas guatemaltecas, el 81 por ciento utiliza software ilegal, según BSA.

2.3. La teoría del bien jurídico

La teoría del bien jurídico se origina, como es conocido, con la obra de Birnbaum en las primeras décadas del siglo XIX. El origen del bien jurídico esta por tanto, en la pretensión de elaborar un concepto de delito previo al que forme el legislador, que condicione sus decisiones, pretensión característica de una concepción liberal del **Estado**, que concibe este como un instrumento que el **individuo** crea para preservar los "bienes" que la colectividad en su conjunto crea de suma conveniencia proteger.

En otras palabras el bien jurídico es la elevación a la categoría de "bien tutelado o protegido por el derecho", mediante una sanción para cualquier **conducta** que lesione o amenace con lesionar este bien protegido, de esta reflexión se puede deducir que el bien jurídico, obtiene este **carácter** con la vigencia de una norma que lo contenga en su ámbito de protección, más si esta norma no existiera o caducara, este no deja de existir pero si de tener el carácter de "jurídico".

Esta característica proteccionista que brinda la normatividad para con los bienes jurídicos, se hace notar con mayor incidencia en el **derecho penal**, ya que es en esta rama del derecho en la que la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico, por ejemplo el "delito de **homicidio**", busca sancionar actos contra la vida de la **persona**, el "delito de injuria", busca sancionar los actos que lesionen el honor de la misma.

Es importante tener en cuenta que la protección del bien jurídico, si bien se puede observar con mayor **fuerza** en el derecho penal, lo cierto es que esta protección va de parte de todo el ordenamiento legal, ya que sería totalmente contradictorio que mientras la norma penal sancione el homicidio, una norma civil o de cualquier otra índole, lo permitan o consientan.

En cuanto al origen natural del bien jurídico, un sector de la doctrina entre ellos el maestro Bustos, sostiene que este nace desde las entrañas del mismo **contrato social**, como un derecho a ser respetado y como un deber de

respetarlo, y como contraparte apareció el delito como lesión a este derecho pre-existente.

En la actualidad la conceptualización del bien jurídico, no ha variado en su aspecto sustancial de valoración de bien a una categoría superior, la de bien tutelado por la ley, en cuanto a ciertos criterios, como el origen, o como el área del derecho que deba contenerlos.

2.4. Crimen informático, criminalidad informática o delitos informáticos

En las primeras definiciones de “delito informático” que se han ido aportado por la doctrina no ha resultado fácil concretar un único concepto de delito informático; por ello, en la actualidad niega un sector de la doctrina la existencia de este concepto y, con ello, de esta tipología delictiva, prefiriendo utilizar para abarcar todo este conjunto de comportamientos que tienen que ver con la informática, de uno u otro modo, expresiones como “delincuencia informática”, “criminalidad informática” o, simplemente, en plural, “delitos informáticos”.

Con argumentos similares a los aportados a principios de los noventa por varios autores, son ya ahora muchos los autores que se decantan por expresiones que eludan el término “delito”, por la problemática antes apuntada en relación con las limitaciones que la utilización de un término que hace referencia a una realidad jurídica positiva conlleva: si sólo es delito lo que la ley penal establece como tal y en ella no existe referencia alguna al delito informático, no podría afirmarse,



cuando menos en el ordenamiento español, como en otros muchos, que exista tal delito.

Por ello la doctrina quizás hoy mayoritaria prefiere acudir a aquellas expresiones de “delincuencia informática” o “criminalidad informática” para incluir en ellas todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva.

Algunos autores añadirán la exigencia de que además las conductas incluíbles en tales expresiones reúnan los requisitos que delimitan el concepto de delito. Y otros, incluso, aun aceptando la heterogeneidad de estas conductas, dejan fuera del grupo aquéllas en las que los sistemas informáticos, o la información en ellos contenida, es el objeto sobre el que recae la conducta delictiva.

2.5. Bienes jurídicos penales en el delito informático

A pesar de las discrepancias doctrinales ya comentadas en torno a la existencia o no de un concepto de “delito informático”, cada vez son más las voces doctrinales que en el ámbito de la delincuencia informática sostienen la necesidad de creación de una nueva categoría jurídico penal que abarque las conductas vinculadas con el hecho informático, entendiendo que no estamos sólo —o no en absoluto— ante la lesión de bienes jurídicos tradicionales, sino ante la lesión de un nuevo interés que merece ser objeto de atención también por el derecho penal.

Esta idea, extendida cada vez más entre los nuevos autores no conlleva, sin embargo, una unidad de criterio a la hora de entender cómo debe explicarse este interés y cómo debe definirse el bien jurídico penal a que pretende hacerse referencia.

Las distintas posturas al respecto, no siempre tan divergentes, son básicamente las siguientes.

a. La Seguridad Informática

La primera de las interpretaciones hace hincapié en la seguridad informática como bien jurídico colectivo a tutelar, objeto de ataque con las conductas vinculadas a la cuestión informática. Se trata de un bien, se dirá, cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual puestos en peligro con tales conductas atentatorias contra la seguridad de las redes y sistemas informáticos, pero no siempre efectivamente dañados. La extensión en el uso de redes y sistemas informáticos se dirá en otros términos, imprescindibles hoy para el desarrollo económico y social, para el correcto funcionamiento del ámbito tanto público como privado, hace que la protección de su seguridad sirva como medio para proteger otros bienes de carácter individual (patrimonio, intimidad, libertad sexual, honor, etc.) e, incluso, otros bienes de carácter supra individual (orden público, paz pública, seguridad del Estado).

Pero es esta expansión y dependencia social de las Tecnologías de la Información y Comunicación –TICs- 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, se señala, no sólo se daña un bien jurídico individual, sino que se generan riesgos para toda la comunidad de usuarios.

Se trata, por tanto, de un bien jurídico de naturaleza colectiva, indisponible, como tal, por el individuo concreto, que no encuentra suficiente protección mediante la salvaguarda en exclusiva de bienes jurídicos de naturaleza individual, pues muchas veces, al margen de otras consideraciones, no existirá la voluntad lesiva de dañarlos de manera efectiva, lo que no impide que pueda entenderse idóneo un adelantamiento de las barreras de protección a la de meras situaciones de peligro para lo cual esta perspectiva puede ser eficaz.

b. Integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos

En un sentido bastante similar, otros autores hablan de la necesidad de proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos contenidos en ellos. Se toma en consideración la informatización de todos los datos, tanto pública como privada, y la necesidad de poder confiar en su autenticidad y en su disponibilidad plena como garantía para un desarrollo económico y social acorde a los tiempos actuales. Esto es lo que garantizaría la tutela de la incolumidad de los datos, de su libre disposición y de su mantenimiento en los términos en que los ha configurado su titular, bien jurídico también de carácter supraindividual que adelanta la intervención penal en cuanto al mismo

tiempo es instrumental respecto de otros bienes jurídicos que pueden verse dañados o en peligro con el menoscabo de la accesibilidad, integridad o confidencialidad de determinados datos.

c. Intimidad informática

La consideración del bien jurídico intimidad informática –habeas data o autodeterminación informática– se ha contemplado de un modo especial en la doctrina italiana –téngase en cuenta que en este ordenamiento se contempla el delito de acceso abusivo a un sistema informático, sin ulterior lesividad, ya desde el año 1993–, que entiende que lo que ha de protegerse frente a esta clase de conductas vinculado al hecho informático es, principalmente, el bien jurídico individual “intimidad e inviolabilidad informáticas”, como una nueva vertiente, si se quiere, de lo que es el domicilio físico de cada persona.

Ello sin perjuicio de que además se reconozca que la protección haya de ir encaminada a garantizar, también, la seguridad y la integridad de los sistemas informáticos, es decir, la seguridad informática.

La intimidad informática –por algunos denominada libertad informática– se plantea como bien jurídico autónomo y diferenciado, de naturaleza estrictamente informática, merecedor y necesitado de protección penal específica. Su contenido central vendría dado por el derecho del individuo a decidir qué información personal se puede difundir sobre él y su familia y cuál pueda ser el destino de esta difusión.



Pero, en realidad, estamos ante un derecho complementario del que tradicionalmente trata de garantizar la tutela de la intimidad en su sentido más amplio, simplemente vinculado al desarrollo concreto de la informática.

En todo caso, y esto es lo importante frente a otro tipo de posturas, no se trata sólo de reconocer el derecho de excluir a los demás de un determinado ámbito que el titular considera reservado y que ha de protegerse frente a intromisiones indeseadas, sino de un poder positivo de control sobre la información personal que los demás pueden tener de cada uno y sobre el uso que puedan hacer de la misma. Por eso se entiende necesario este nuevo concepto, entendiendo que lo que pretende abarcar no está suficientemente garantizado ni por los tradicionales medios de tutela de la propiedad o la posesión de las cosas materiales, ni por la protección prestada al secreto, a la intimidad personal y domiciliaria o a otro tipo de bienes inmateriales.

d. Otras propuestas

En un sentido parecido se apunta como nuevo bien jurídico de carácter supraindividual característico de los delitos informáticos la confianza en el funcionamiento de los sistemas informatizados. Como ya se ha mencionado en relación a las propuestas que aluden a la idea de la seguridad informática, los delitos vinculados con la informática no sólo dañan en su comisión bienes jurídicos individuales y concretos; su comisión también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de

transmisión de datos. La gravedad de este quebrantamiento de confianza radica, precisamente, en la dependencia de la sociedad actual respecto de las TICs para el desarrollo personal, económico y social de los individuos.

Se afirma que la tecnología de Internet es en sí misma un nuevo bien jurídico a proteger por el ordenamiento; un nuevo bien jurídico de primera magnitud.

Se ha destacado asimismo que mediante el delito informático se dañan bienes tanto personales como patrimoniales y que, sin reconocer con ello que estemos ante conductas que atenten contra un específico bien jurídico, nos encontramos por ello ante una categoría penal autónoma en la que el objeto de protección coincide no obstante con el de los tipos tradicionales que están siendo adaptados a las nuevas tecnologías.

2.6. Problemas de interpretación en la delincuencia informática

En las últimas décadas ha tomado cuerpo la eclosión del fenómeno informática en amplias parcelas de nuestra sociedad. La enorme expansión de que vienen gozando las nuevas tecnologías en una sociedad cada vez más receptiva a las posibilidades crecientes que ofrecen estos medios tiene consecuencias indudables para el mundo del Derecho y para el Derecho Penal en particular.

Hay una tesis que indican: "mientras que en la sociedad industrial la "lógica" de la producción de riqueza domina a la "lógica" de la producción de riesgos, en la sociedad del riesgo se invierte esta relación".

He elegido esta cita como inicio del presente tema por su eminente carácter revelador del tipo de sociedad en que se incardina y explica, no sólo el fenómeno, sino también el alcance de las nuevas modalidades delictivas. Parece existir un consenso generalizado en los autores a la hora de constatar la aparición de múltiples riesgos aparejados a la sociedad postindustrial, frente a los cuales la población está respondiendo con un sentimiento creciente de inseguridad.

Sin duda, la "delincuencia informática", "ciberdelincuencia" o "cibercrimen" constituye uno de los máximos exponentes de las nuevas realidades delictivas, como señala Jesús María Silva Sánchez, pues en ella concurren las notas de empleo de las nuevas tecnologías y la producción de riesgos anteriormente desconocidos (nuevas formas de ataque a la intimidad, defraudaciones de enorme cuantía, etc.), a la que se suman su carácter transfronterizo y susceptibilidad a la comisión por bandas organizadas.

Las nuevas realidades y formas de criminalidad deben encontrar una respuesta en diversas sedes jurídicas, entre las que han cobrado singular relevancia el Derecho penal sustantivo y el proceso penal.

Hasta tal punto es así, que ya se habla por la doctrina del fenómeno de la "expansión" del Derecho penal, caracterizado, según: "...la existencia de una tendencia claramente dominante en la legislación de todos los países hacia la introducción de nuevos tipos penales así como a una agravación de los ya existentes, que cabe enclavar en el marco general de la restricción, o la

"reinterpretación" de las garantías clásicas del derecho penal sustantivo y del derecho procesal penal. Creación de nuevos "bienes jurídico-penales", ampliación de los espacios de riesgos jurídico-penalmente relevantes, flexibilización de las reglas de imputación y relativización de los principios político-criminales de garantía no serían sino aspectos de esta tendencia general, a la que cabe referirse con el término "expansión". Un fenómeno que no es ni mucho menos ajeno al proceso penal, en que medios como "los controles policiales preventivos, la observación y vigilancia policial mediante instrumentos técnicos, que cada vez aparecen más perfeccionados, el uso de agentes provocadores, etc." (orientados a la lucha preventiva con el delito) y "la intervención creciente del principio de oportunidad, la promoción del acuerdo de entre las partes como modo de finalización del proceso, el oscurecimiento del principio de publicidad, la reducción de las posibilidades de prueba a instancia de parte, la eliminación de fases del proceso, etc.", "contribuyen a alejarlo de los principios liberales básicos y garantías tradicionalmente vigentes en este ámbito..."¹⁸

Éste es el contexto en que sitúo el fenómeno del ciber crimen y de la respuesta procesal al mismo, y el que tomaré como punto de partida para el presente estudio que, en consonancia con las indicaciones proporcionadas, persigue como objetivo señalar posibles líneas de investigación.

¹⁸ Silva Sánchez, Jesús-María. **La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales**. 2º. Ed., rev. y ampliada, Civitas, Madrid 2001. Pág. 167.

2.7. Efectos procesales del tema

Los autores consultados coinciden en señalar fundamentalmente las dificultades que el empleo de medios informáticos en la comisión de hechos delictivos reviste para la averiguación y persecución de la delincuencia informática (lo que sitúa las principales repercusiones para el proceso penal en la fase investigadora). Dichas dificultades vienen motivadas por una serie de propiedades que las especiales características del ciber crimen hacen posibles:

- a. En primer lugar, dichas conductas no dejan "huellas" tradicionales (vestigios materiales de la actividad delictiva como huellas dactilares, restos de ADN, etc.) sino "huellas electrónicas", que revisten gran complejidad y un carácter sumamente novedoso.
- b. Aunque el rastreo de los pasos seguidos en la comisión de la actividad ilícita es posible en muchas ocasiones, se ve entorpecido por su inserción en una amalgama de miles de procesos informáticos llevados a cabo diariamente y por la falta de visualización del iter criminis. Por otra parte, se trata de procedimientos de investigación de carácter muy técnico, necesitados de expertos en la materia y, en consecuencia, sumamente costosos.
- c. Por otra parte, la condición de especialistas de quienes cometen las conductas prohibidas les permite borrar o dificultar el seguimiento de las actuaciones practicadas para la consumación del delito , con lo que, a la ya tradicional complejidad de la investigación de ilícitos de corte "experto" (a saber, necesitados de conocimientos superiores o de una realización minuciosa y

concienzuda) se viene a añadir el plus de complicación que supone el carácter innovador de estos medios (necesitados de una respuesta igualmente técnica por parte de los responsables de la investigación y persecución de estos delitos, que sólo progresivamente y no siempre de modo satisfactorio se está proporcionando)

d. Todas estas notas (dificultad de rastreo, borrado de las huellas, etc.), a las que viene a añadirse el propio carácter impersonal que implica el recurso a los medios informáticos y, en particular, a Internet facilitan el anonimato del infractor, en ocasiones hasta el punto de hacer indeterminable su identidad.

e. Otra característica destacable, con indudables repercusiones para el proceso penal, es la presencia en múltiples actuaciones de un intermediario de carácter privado o administrativo (como son los proveedores de telecomunicaciones), sin cuyo concurso resulta imposible efectuar el intercambio de información preciso. La investigación de estos delitos topa por tanto con un tercero en discordia cuya colaboración, como se advertirá más adelante, deviene necesaria para la labor investigadora.

f. Igualmente trascendente se antoja el carácter transfronterizo de los procesos informáticos, consecuencia de la globalización y las nuevas tecnologías, que permite cometer los hechos delictivos en diversos países simultáneamente, a menudo por organizaciones delictivas radicadas en diferentes Estados y con cientos de integrantes. Este fenómeno no sólo obliga a una actuación solidaria por parte de las autoridades de los distintos países afectados (origen de la necesidad de una armonización legislativa o, al menos, de una cooperación policial y judicial articulada a un nivel supranacional) sino

que impone asimismo la perentoriedad de una revisión de los criterios competenciales y de las respuestas criminológicas al fenómeno de las bandas organizadas. En definitiva, la delincuencia informática presenta como rasgos añadidos a la complejidad técnica su carácter supranacional y favorable a la comisión por organizaciones criminales.

g. Eminentemente procesal es la problemática aparejada a la preservación de la prueba con vistas a su utilización en el juicio oral (la etapa procesal en que las mismas pueden romper la presunción de inocencia) La dificultad está motivada por el carácter volátil de los datos informáticos, que facilita enormemente su eliminación.

h. Finalmente (como aspecto de singular trascendencia) es necesario destacar los intereses ciudadanos en juego. La investigación de las conductas enmarcadas en la delincuencia informática roza con el derecho a la intimidad y al secreto de las comunicaciones de los/as ciudadanos/as (precisamente los/as usuarios/as de Internet claman constantemente por preservar la esfera de anonimato que el mismo comporta ante cualquier intento de limitarla) y obliga a observar un total cuidado en la realización de las indagaciones necesarias de forma que no se cuestione el respeto a los derechos fundamentales citados.



CAPÍTULO III

3. El derecho penal informático

3.1. Noción e ilustración del derecho penal informático

El Derecho ha ido encontrando nuevos desafíos a medida que evoluciona la sociedad, y más concretamente al verse enfrentado al vertiginoso desarrollo de las Nuevas Tecnologías de la Información (NTI). Es por lo anterior, que la gran mayoría de los juristas coinciden en el nacimiento de una nueva rama del derecho autónoma e independiente, cual es el Derecho Informático: No se debería dudar acerca de una verdadera autonomía en el Derecho Informático, haciendo la salvedad que esta ciencia constituye una rama jurídica atípica, que apenas nace.

Este nuevo contexto -donde ya hablamos ciertamente de la regulación del derecho informático como tal-, exige indagar las interrelaciones con otras ramas del derecho como lo son el derecho civil, el derecho administrativo y el derecho penal. Es de esta forma, que el tema de este ensayo se desarrolla sobre la base de la relación existente entre el derecho penal por un lado y el derecho informático por el otro. En la práctica, esta correlación jurídica la vemos materializada en dos aspectos clave que debemos considerar: La idea de proteger nuevos bienes jurídicos afectados como son la privacidad, la honra, la propiedad de datos, etc.; y un indispensable que hacer legislativo referido a la tipificación de ciertos delitos informáticos que nuestro ordenamiento contempla en el código penal.



A mi criterio puedo decir que el derecho penal informático, es una ciencia que apoyada en la informática forense, estudia todas las conductas nocivas e ilícitas es decir, al delito informático o criminalidad informática que se genera a través de sistemas informáticos y de internet, y que tiene como objeto principal tutelar a través de normas jurídicas, bienes jurídicos como la seguridad, la privacidad, la integridad informática y la protección de datos.

3.2. La elación entre el derecho penal y la informática

Actualmente el tema de la informática, ha cobrado gran significación para el mundo económico, cultural y educativo, principalmente, con el avance de la tecnología, y en este campo, que se toma tan amplio, se desenvuelve una gama compleja de actividades computarizadas o sistematizadas que escapan a la imaginación completa del hombre. Sin embargo, es evidente, que hace algunos años, no se hubiera podido imaginar el hombre que se afectarían diversos bienes jurídicos tutelados, con ocasión del uso de la tecnología informática, lo cual en la actualidad está sucediendo y ello, también debe ser objeto del campo de estudio y análisis de la ciencia penal moderna, aunque éstos conceptos difieren de la opinión de muchos tratadistas de la ciencia penal, en cuanto a que el estado debe cumplir los principios básicos de una ciencia penal moderna, que implica entre otros, el principio de la mínima intervención y dado el carácter fragmentario de la ciencia penal, no debe intervenir, y dejarlo a consideración de otras disciplinas como el derecho administrativo, por ejemplo, se difiere de esas conceptualizaciones, puesto que con el avance de la tecnología en la información, puede cometerse la mayoría de ilícitos penales que lesionan bienes jurídicos como el caso del patrimonio, el caso de la vida, con los homicidios, y otros.



La intervención de la ciencia penal moderna no sólo debe enfocarse en concepciones y teorías o doctrinas que garanticen los derechos humanos y que busquen su aplicabilidad, impulsando cambios sustanciales en las leyes existentes, sino también, debe centrarse en regular como ilícitas las actividades informáticas que perjudiquen a terceros, y derivado de ello pueden surgir nuevos bienes jurídicos tutelados brindando de esa forma protección a los ya existentes lo cual sería de trascendental importancia, como se decía, el caso del derecho a la vida, la libertad y a la integridad física y protección del patrimonio de las personas.

El problema podría parecer sencillo, si se considera que en un país, de acuerdo a su realidad como fuente real del derecho, crear nuevas figuras delictivas como podría ser el caso de regular actividades comprendidas dentro de la criminología informática, tal como se pretende demostrar, en el caso de la comisión de ilícitos a través del uso y programación del computador y de los demás medios accesibles. Pero el problema es más complejo, y allí podría adecuarse al principio de la extraterritorialidad de la ley penal, que tal como lo regula el Artículo 5 del código penal indica "este código también se aplicará: 1º.- Por delito cometido en el extranjero por funcionario al servicio de la República, cuando no hubiere sido juzgado en el país en el que perpetró el hecho. 2º.- Por delito cometido en nave, aeronave o cualquier otro medio de transporte guatemalteco, cuando no hubiere sido juzgado en el país en el que se cometió el delito. 3º.- Por delito cometido por guatemalteco en el extranjero, cuando se hubiere denegado su extradición. 4º.- Por delito cometido en el extranjero contra guatemalteco, cuando no hubiere sido juzgado en el país de su perpetración siempre que hubiere acusación de parte o del Ministerio Público y el imputado se hallare en Guatemala. 5º.- Por delito que,



por tratado o convención, deba sancionarse en Guatemala, aun cuando no hubiere sido cometido en su territorio. 6º.- Por delito cometido en el extranjero contra la seguridad del Estado, el orden constitucional, la integridad de su territorio, así como falsificación de la firma del Presidente de la República, falsificación de moneda o de billetes de banco, de curso legal, bonos y demás títulos y documentos de crédito.”.

En el caso que en la comunidad internacional, por ejemplo en un país se regula como ilícito una actividad relacionada con la informática, y en otro esté completamente aprobado y no constituya delito, existe conflicto de aplicación de la ley para el momento en que se determine que hubo un ilícito, en el caso del imputado, tomando en consideración que el avance de la información a nivel mundial, podría reducirse al uso de un computador, por medio del cual el operador puede conocer el mundo y con la habilidad y los programas necesarios no autorizados pirateados, puede provocar grandes perjuicios en el patrimonio de terceras personas, así como la afcción de otros bienes jurídicos tutelados existentes y que deben existir, a través de la tecnología de la cual es utilizada en la modernidad. Esta provoca nuevas formas de delinquir, como por ejemplo, la piratería en el uso indebido de programas, los juegos de azar a través del uso del computador, etc.

Es importante, de esta manera, poder establecer cuáles podrían ser las actividades relacionadas con la informática, que están ocasionando conflictos con la ley penal, es decir, producen daños y perjuicios a terceras personas, asimismo, determinar qué efectos produce el uso del Internet como un sistema de comunicación directa, el cual cobra día a día gran significación.

3.3. Acciones ilegales suscitadas con el uso de la informática

Existe un sinnúmero de actos o acciones que puede realizar una persona que pudiera considerárseles como un ilícito penal, mediante el uso inadecuado, indebido, no autorizado de un computador. El tratadista Ricardo Bría, enumera las siguientes:

- a. **Datos engañosos:** esta forma ilícita consiste en la manipulación de datos en la entrada y salida de la información de una computadora. Esto puede afectar a cualquier persona.
- b. **Cambios clandestinos de programas:** consiste en alterar los programas ya establecidos con un fin propio del operador, sin ninguna autorización de la fuente o el propietario del programa. A través de éstos puede perjudicar el patrimonio de las personas, por lo que el bien jurídico es el patrimonio.
- c. **Caballo de Troya:** constituye una variante de la técnica anterior que consiste en introducir rutinas que son activadas con una señal o al cumplirse una condición determinada, ejemplo: cuando produce el efecto de borrar los archivos maestros o inicializaciones de discos luego de producirse la baja de algún empleado, generalmente del Centro del cómputo, o con dolo, borrar la información que su existencia perjudicaba a determinada persona, es decir, a cualquier persona.
- d. **Puertas trampa:** dentro del campo de la informática estas actividades son conocidas como tal. Es un método ilícito que consiste en que putos débiles en un sistema de computación, diseñado con el propósito de tener acceso al mismo, eludiendo los controles normales. No es anormal encontrar sistemas cuyos

procedimientos de corrección de transacciones rechazadas por errores, permitan su reingreso al sistema de cómputo a través de rutinas que evitan los controles originales, lo que podría dar lugar a la introducción de datos falsos. Esta actividad no se encuentra regulada específicamente en el Código Penal.

e. **Modificación de documentos fuente:** Es una de las técnicas delictivas más utilizadas. Esta consiste en la comisión del ingreso de ciertas transacciones, la alteración de su contenido, la inclusión de transacciones no autorizadas o el procesamiento duplicado de transacciones. Estas formas de utilización ilícita del computador y programas no se encuentran reguladas en el Código Penal.

f. **Intercepción de documentos fuente** constituye una de las formas más elementales de cometer un delito por computadora, el teleprocesamiento, puede llegar a ser de los más complejos, pues determinar ese hecho es sumamente difícil y complejo, circunstancias que únicamente se han observado en países como Estados Unidos. A pesar de que en la Constitución Política de la República de Guatemala y en el código procesal penal, se encuentra prohibido, en la práctica a través del uso del computador, diariamente se ocasiona perjuicio en contra de los bienes jurídicos tutelados tanto de los particulares como a los estatales y nacionales.

3.4. Las innovadoras tecnologías de la informática

En la actualidad, el proceso acelerado de las formas de comunicación, ha hecho que surjan modernas tecnologías, las cuales deben considerarse como peligrosas, pues a través de tales formas de comunicación se puede dar lugar a la comisión de actividades

ilícitas propiamente dichas, que ocasionen un perjuicio a terceras personas, mediante el uso del computador, especialmente entre las cuales pueden citarse las siguientes:

a. Existe una modificación de los sistemas tradicionales de pagos e intercambio monetario en el sector bancario. Estos sistemas tradicionales se encuentran siendo sustituidos por las transferencias electrónicas de fondos, lo cual en el mundo financiero, se le denomina dinero electrónico. Este sistema realiza operaciones de giro y contabilidad, a través de formas electrónicas, lo cual evita que personalmente se acuda a un banco a realizar transacciones financieras, y que implique también la utilización de boletas que el mismo banco proporciona para realizar dichas transacciones. Algo novedoso de este sistema es el hecho de que las personas ya no portan el dinero, con el riesgo de que sufran un robo, asalto, etc., sino que se les facilita, por ejemplo, en el caso más sencillo, el pago de la luz, teléfono, etc.

b. Se prevé que muy pronto, se implementará el sistema de videotex, que permitirá a las personas la realización de múltiples operaciones desde sus hogares, tales como: servicios de televenta y telecompra, telebanca, transferencia electrónica de fondos etc., incluyendo el acceso de información a diferentes fuentes a nivel mundial, tal es el caso, como sucede en la actualidad con el sistema de Internet, correo electrónico.

c. Es importante tomar en cuenta que pueden existir infinidad de circunstancias por las cuales, mediante el uso del computador y de determinados programas, el operador puede ocasionar una serie de atropellos, aprovechándose de la exclusividad del uso del sistema o programa que las



víctimas ignoran y que difícilmente logren darse cuenta lo que en muchos casos ha hecho posible que quede tal actividad completamente ilícita e impune, y si en dado caso la víctima se enterara de los atropellos de que fue objeto, es difícil que pueda ejercitar su derecho, en virtud que en la legislación penal guatemalteca no se encuentra bien regulado el delito informático.

CAPÍTULO IV

4. La informática forense

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos.

Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos de especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así

como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En consecuencia, este breve apartado de mi investigación busca ofrecer un panorama general de esta especialidad técnico legal, para ilustrar a los lectores sobre los fundamentos generales y bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, unos nuevos científicos que a través de la formalidad de los procesos y la precisión de la técnica buscan decirle a los intrusos informáticos que están preparados para confrontarlos y procesarlos

4.1. Noción y definición

Existen múltiples definiciones a la fecha sobre el tema forense en informática. Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: Computación forense, digital forensics (forensia digital), network forensics (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

Es importante anotar, que al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asumen dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen como son: Identificación,



preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

Iniciemos con computer forensics, cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras: 1. Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o 2. Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de network forensics, forensia en redes, estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación

criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Finalmente, la digital forensics o forensia digital, trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Como hemos revisado, las definiciones abordan aspectos generales y específicos que convergen en todos los casos hacia la identificación, preservación, extracción, análisis, interpretación, documentación y presentación de evidencia digital para detallar, validar y sustentar las hipótesis que sobre un evento se hayan formulado. No obstante lo anterior, es pertinente anotar que aquellos dedicados a esta disciplina emergente como la informática forense, deben ser profesionales no con altos niveles de ética y respeto por las instituciones, sino con los más altos niveles, pues en ellos esta el soporte de las decisiones que sobre los hechos analizados se tomen.

4.2. La evidencia digital

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

En este sentido el documento mencionado establece que la evidencia digital puede ser dividida en tres categorías a saber:

- a. Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.)
- b. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
- c. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno.

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:

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

Estas características nos 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. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

4.3. Protocolo de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos

deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso bien sea legal u organizacional.

En este sentido, detallamos de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado:

a. **Esterilidad de los medios de informáticos de trabajo:** Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

b. **Verificación de las copias en medios informáticos:** Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. Adicionalmente, es preciso que el software u aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad



científica, para que conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

c. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados: El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

4.4. La cadena de custodia de las evidencias digitales

Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

4.5. Análisis de los medios informáticos

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

4.6. Reconocimiento de la evidencia digital

La evidencia digital en la administración de justicia en muchas partes del mundo continúa siendo una situación problemática por resolver. Dada las características mencionadas previamente, se hace un elemento que requiere un tratamiento especial, más allá de las características legales requeridas, pues éstas deben estar articuladas con los esfuerzos de seguridad de la información vigentes en las organizaciones.

4.7. La validación y confiabilidad de las herramientas forenses en la informática

Las herramientas utilizadas actualmente en investigaciones forenses en informática están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos.

Sin embargo, la fragilidad inherente del software, la vulnerabilidad presente en las mismas y las limitaciones propias de los lenguajes y prácticas de programación hacen que la comunidad académica y científica redoble sus esfuerzos para hacer de estos programas, herramientas más confiables y predecibles para los cuerpos de investigaciones judiciales y organizacionales.

La formación de especialistas en informática forense, que apoyen labores de peritaje informático tanto en la administración de justicia como en investigaciones organizacionales internas. Al ser la informática forense una ciencia aplicada naciente, se hace necesario iniciar las reflexiones sobre la formación de un especialista en informática forense.

Esta formación necesariamente deberá ser interdisciplinaria y para ello se requiere el concurso de los profesionales del derecho, la criminalística, las tecnologías de información y la seguridad informática, como mínimo, sin perjuicio de que otras disciplinas académicas puedan estar presentes en la estrategia de profesionalización de estos nuevos especialistas.

A lo largo de este documento hemos querido mostrar de manera básica y concreta una aproximación a la informática forense, no con el ánimo de sugerir un curso de acción sobre el tema, sino de ilustrar los diferentes escenarios y elementos que componen esta naciente disciplina auxiliar de la criminalística.

La informática forense es la respuesta natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en



medios informáticos y a través de medios informáticos) con el fin de enviar un mensaje claro a los intrusos: estamos preparados para responder a sus acciones y continuamos aprendiendo para dar con la verdad de sus acciones.





CAPÍTULO V

5. El manejo de la informática en el esclarecimiento de los casos de alto impacto en el ordenamiento jurídico penal guatemalteco

La teoría de la tipicidad relevante, es un contexto que abarca toda la justicia penal adjetiva, ya que la encontramos en los mecanismos de desjudicialización, así como en el procedimiento penal común. En la desjudicialización, resolverá ágilmente todos aquellos delitos de poca incidencia social, y en el proceso penal común, resolverá todos aquellos delitos de alto impacto social; así mismo, la teoría de la tipicidad relevante, permite la administración de una justicia pronta y cumplida, siendo en realidad parte de la conquista social, que el pueblo de Guatemala tiene para lograr la paz y la convivencia social. El camino de la tipicidad relevante en nuestro país, ha sido difícil, ya que algunos operadores de justicia, no han entendido del todo de cómo funciona, pero es de esperarse, que la capacitación y la experiencia constantes, permita lograr una correcta aplicación.

El jurista César Ricardo Barrientos Pellecer, En su libro Derecho Procesal Penal Guatemalteco, define la teoría de la tipicidad relevante de la siguiente manera: "Para permitir que los asuntos de menor importancia puedan ser tratados de manera sencilla y rápida, fue necesario replantear las teorías del derecho penal sustantivo, referente a los delitos públicos. Surgió así la Teoría de la Tipicidad Relevante, que obliga al estado a perseguir (prioritariamente) los hechos delictivos que producen impacto social."¹⁹

¹⁹ Barrientos Pellecer, César Ricardo. *Derecho procesal penal guatemalteco*. Magna Terra Ed.; Guatemala, 1995. Pág. 72.

5.1. Generalidades del fenómeno estudiado

La constante ola de criminalidad y organización criminal en Guatemala, el aprovechamiento de las fallas humanas al utilizar procedimientos tecnológicos para concertar los delitos, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con la manera de identificar a los responsables de tales ilícitos y resolver los casos en concreto utilizando como medio a la informática forense en el derecho procesal penal. A pesar del escenario anterior, la informática forense nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso de alto impacto social en Guatemala.

En consecuencia, este trabajo de investigación busca ofrecer un panorama general de esta especialidad técnico-legal, para ilustrar a los demás investigadores y lectores sobre los fundamentos generales y bases de actuación de aquellos que se han dedicado a procurar el esclarecimiento de los hechos en



medios informáticos, unos nuevos científicos que a través de la formalidad de los procesos y la precisión de la técnica buscan decirle a las organizaciones criminales que están preparados para confrontarlos y procesarlos.

Hoy en día las nuevas tecnologías de la comunicación se han convertido en una especie de arma para la justicia, debido a que el uso de la tecnología a mi criterio deja rastros, que después pueden ser utilizados como medios de prueba en procesos judiciales de orden penal.

En que en la actualidad jurídica guatemalteca se han creado nuevos juzgados del ramo penal, mismos que solo tienen competencia en casos de alto impacto social en Guatemala. Por lo que vale la pena, estudiar y determinar cuáles son los medios procesales en los cuales se basan estos Juzgados para resolver los casos con relevancia jurídica en Guatemala.

Los avances tecnológicos en esta área han abierto una brecha jurídica que debe afrontarse para evitar actos ilícitos con la tipificación de tales actos. Verbigracia, actualmente la Comisión Internacional Contra la Impunidad en Guatemala (CICIG), resaltó la importancia de los hallazgos en el tan sonado caso Rosenberg, obtenidos a través de la utilización de medios tecnológicos e informáticos, mismos que son un ejemplo de lo que se puede lograr con la complementación que tiene el derecho penal, procesal penal y la informática forense en el esclarecimientos de casos de alto impacto social en el orden penal de Guatemala.

Por lo que es necesario decir que en nuestro medio se debe de comenzar a utilizar la tecnología con responsabilidad, ya que el usuario debe tener presente que este beneficio tecnológico de comunicación rápida y económica tiene que emplearse con responsabilidad, sobre todo en la administración de la información.

5.2. Las tecnologías de la información y el proceso penal

“Las nuevas tecnologías de la información generan transformaciones en la sociedad. Es indudable que sus adelantos fraguan una nueva época en la historia de la humanidad, al decir de Ruperto Pinchote Olave, la de la sociedad de la información.”²⁰

La informática y las telecomunicaciones indistintamente facilitan el desarrollo de Internet, elemento más revelador de la nombrada “nuevas tecnologías de la información”. La informática “entendida”, permite almacenar y alternar grandes cantidades de información, mientras las telecomunicaciones enlazan a personas situadas en lugares alejados entre si, con sorprendente facilidad en breve tiempo.

De esa cuenta, como lo indica García Añón, “Las nuevas tecnologías de la información o tecnologías de la comunicación, cuya implementación se realiza por medio de Internet, exhiben diversas modalidades: el correo electrónico, la World Wide Web, el Chat,” “la Videoconferencia y la Telefonía. Todas se ejecutan a través de computadores

²⁰ Cobo del Rosal, Manuel y otros. **Curso de derecho penal español**. Parte Especial, tomo I, editorial Jurídicas y Sociales, Madrid, 1996. Pág. 98.

e implican una revolución que trastorna disímiles ámbitos de la cultura, entre ellos el jurídico.”²¹

Lucfa lo reafirma al expresar que: “...se consolidan en nuestras sociedades post industrializadas, como un instrumento imprescindible para una gran parte de su actividad...” y continua aseverando que “...su incidencia tiene que afectar, y afecta, a las distintas ramas del ordenamiento jurídico. Incluido, por supuesto, el Derecho penal.”²²

Con el objetivo de alcanzar una administración de justicia más eficaz y garantista, José Palomino nos ofrece en estas líneas el resultado de una investigación que afronta, sin los habituales prejuicios, la evolución y las perspectivas de futuro de las relaciones entre el Derecho penal y las nuevas tecnologías, señalando los límites que en este ámbito jurisdiccional se debieran respetar ante el inevitable progreso-de la informática jurídica.

“Fruto de la investigación y de su doble experiencia como jurista práctico y profesor de derecho penal, el autor ha podido formalizar una herramienta metodológica para asistir a los juristas, materializando en un sistema informático la que aquellos utilizan para aplicar el derecho penal. Inspirado en las características de los «sistemas expertos jurídicos», el modelo respeta las garantías, los contenidos y las particularidades del razonamiento judicial, dejando siempre a criterio del usuario la decisión final.”²³

²¹ García Añón, José. **Métodos y técnicas para la realización de trabajos de investigación**. Editorial Universidad de Valencia, Valencia, 1993. Pág. 78.

²² Gabaldón, Gerardo, Luis y P. Wilmer. **Usurpación de identidad certificación digital: propuestas para el control del fraude electrónico**. Sociologías, Porto Alegre, junio 2008. Pág. 145.

²³ Palomino Martín, José. **Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del derecho penal**. Editorial Tirant lo Blach, España, 2007. Pág. 3.

Un hecho trascendental ocurre cuando el Derecho viene a ser reforzado por la moderna Informática, que le imprime nueva fuerza, amplía su eficacia y le proporciona rapidez y un ámbito ampliado, que traspone toda clase de fronteras geográficas y tecnológicas.

En algunos países desarrollados existe ya la informatización del proceso jurídico, tanto en lo que se refiere a las soluciones de trámite, como a las que el juez elabora, tomando en cuenta modelos pre-formateados. La Informática permite, de modo automático y con ayuda de un banco de datos, la realización de demandas pre-formateadas, la contestación, la realización de actos y documentos y el seguimiento de procesos. En la fase probatoria, mediante la Informática existe la posibilidad de simular situaciones, se pueden verificar datos de identificación personal, compilar, organizar información durante el curso del proceso y efectuar comparaciones. La prueba documental comprende todos los objetos materiales existentes, entre los que se encuentran los documentos electrónicos. El documento electrónico es uno de los mejores instrumentos de la Informática, pues constituye una prueba de carácter documental. También se considera documento electrónico aquel que ha sido creado en una computadora, grabado en un soporte informático, producido y reproducido. La falta de firma de los documentos informáticos no los inhibe como material probatorio. Los medios de prueba informáticos consisten en: discos, cintas o cualquier clase de archivos magnéticos o de uso computacional, y en la reproducción por cualquier medio.

5.3. Las tecnologías de la información y la investigación criminal

El rápido desarrollo de las tecnologías de la información y de las comunicaciones ha producido también cambios en el proceso penal. Estos cambios son tanto cualitativos como cuantitativos. Cualitativos en la medida en que significan nuevos medios de investigación, más sutiles, más incruentos, más seductores, y en cuanto significan una dimensión nueva y particularmente peligrosa de lesión a los derechos fundamentales. En lo cuantitativo significan una mayor cantidad de herramientas en manos de las autoridades de la instrucción para efectos de realizar sus actividades. Estas herramientas van desde la observación de personas por periodos largos o cortos (incluso por medios audiovisuales) y el uso de agentes provocadores; pasando por la escucha de las conversaciones de los ciudadanos en vehículos y habitaciones, hasta el uso extensivo de medios de la tecnología de la información para comparar y escrutar datos personales.

Esta tendencia hacia la utilización de estas "nuevas" herramientas de control y vigilancia es particularmente clara en el desarrollo actual en el proceso penal en los países europeos, muy especialmente en la República Federal de Alemania, donde la discusión en torno a las problemas constitucionales y legales de este "nuevo estilo" de la investigación es más profunda.

En América Latina no ha habido hasta el momento una regulación del uso de estas nuevas tecnologías en el proceso penal, como tampoco ha habido una reflexión sobre sus posibles problemas de orden constitucional. De igual manera no hay

investigaciones que permitan aquilatar el grado de desarrollo y de utilización de equipos de cómputo y de conexiones telemáticas en una investigación criminal. Solo se tienen datos aislados de los esfuerzos de algunos poderes judiciales de la región por incorporar sistemas de cómputo para el manejo de incipientes proyectos informática jurídica documental y de gestión, y no existen datos sobre el poder informático en manos de la policía y del Ministerio Público. Cabe suponer que los avances en esta materia tarde o temprano serán utilizados ampliamente por el sistema de justicia penal, lo que generará, sin duda, la necesidad de reflexionar sobre el papel del proceso penal en una justicia penal que vela por un bien jurídico "novedoso" como lo es la "funcionalidad" o la "eficiencia" de la administración de justicia penal.

5.4. La administración de justicia y los retos del Estado ante la guerra frente a la criminalidad

No hace mucho se ha afirmado en nuestro país, pero también en América Latina y en Europa, que los Estados están enfrascados en una guerra contra la "criminalidad", una guerra sin cuartel, en donde la bandera de un proceso penal "eficiente" ondea con la fuerza de uno de esos bienes jurídicos intangibles y misteriosos, de los cuales nadie sabe de dónde vienen y de dónde se sustentan, pero que se sabe que pueden producir un cambio radical en el equilibrio entre las garantías individuales y las facultades del Estado al investigar los delitos, en todo caso a favor de estas últimas. Se trata de la llamada "funcionalidad de la administración de la justicia penal", concepto que fue desarrollado por el Tribunal Constitucional Federal Alemán en su jurisprudencia de inicios de los años ochenta, y que hoy incluso lleva a replantear una serie de derechos



y garantías fundamentales del acusado en el proceso, los cuales se hacen ceder con el fin de justificar una tarea del Estado, que más bien tiene el valor de una carta en blanco en favor del sistema de justicia penal.

La "funcionalidad de la administración de justicia penal" pertenece a ese grupo, cada vez más amplio, de bienes jurídicos sin contenido, que pueden ser llenados por vía de interpretación, y que tienen un papel importante a la hora de determinar el equilibrio entre los intereses del Estado (en este caso de la investigación de los delitos) y los derechos fundamentales del ciudadano.

En la forma en que ha sido utilizado este bien jurídico por el Tribunal Constitucional alemán, abre la posibilidad a que en los casos en que exista una posibilidad de limitar las facultades de investigación del Estado en razón de un derecho del acusado, este último se hace ceder a aquellas con el fin de que el interés público de realización de la justicia no se restrinja. Es cierto que hay un interés social importante en que se investiguen los delitos, y esto es en cierto sentido algo que se entiende por sí mismo, pero también es cierto que no existe en la ley fundamental de Bonn de 1949 o en la Constitución Política de la República Guatemala ninguna norma que establezca a la funcionalidad de la administración de la justicia penal como un bien jurídico con entidad propia, y aún cuando se pretenda derivar la misma del principio del Estado de Derecho, esta misma metodología interpretativa no permite que alguno de los derechos fundamentales, incluso aquellos que derivan directamente de la dignidad del hombre, puedan verse limitados para garantizar este interés social en la investigación satisfactoria de un delito.

La versión latinoamericana de esta idea del Tribunal Constitucional Federal Alemán la estamos empezando a ver nacer. Tanto en las discusiones en los parlamentos regionales, como en los medios de comunicación, se empieza a observar una preocupación sospechosa por la eficiencia. Se habla de que la guerra contra la criminalidad sólo la podrá ganar el estado si es eficiente, y para ello resulta necesario confiarle más herramientas y más posibilidades de acción, mayores facultades para escoger lo que persigue y más y mejores recursos para realizar esta tarea. En esta carrera por la "eficiencia" no se duda en potenciar la necesidad de reducir garantías clásicas en favor del imputado, cuando las mismas resultan sospechosas de reducir la "eficiencia" de la reacción estatal, o cuando un respeto de éstas acarree una disminución de las posibilidades de éxito frente a la criminalidad.

Quizá en una dimensión mucho menor a lo sucedido en Europa, también en América Latina el enfoque de la lucha contra la criminalidad organizada ha llevado en muchos países a reducir el marco de garantías del derecho penal clásico con la esperanza de que el impacto de la reacción del sistema de justicia penal sea más contundente, sin embargo, tanto las experiencias europeas, como las latinoamericanas, han demostrado que esta respuesta contundente no ha reducido el narcotráfico, ni ha podido incidir en las estructuras organizativas de este tipo de criminalidad.

Lo que queda por observarse es si en nuestro medio cultural serán asumidos los mismos discursos legitimadores que han permitido ampliar la utilización de herramientas tecnológicas para la investigación criminal, reduciendo en mayor medida las garantías en favor del acusado e incluso de aquellos ciudadanos sobre los que no

pesa sospecha de haber cometido delito. Una asunción de este discurso, llevaría, junto a la crisis evidente del sistema de justicia penal latinoamericano, a una ampliación de los poderes de las agencias represivas y a otorgar más y mejores herramientas que pueden ser utilizadas también para el control y vigilancia de la disidencia ideológica y para la mayor represión sectorial, típica de los sistemas del control penal latinoamericano.

En la República Federal de Alemania ha tenido gran importancia en la última década el seguimiento doctrinal, jurisprudencial y legislativo al equilibrio entre la funcionalidad de la administración de la justicia penal y del derecho a la autodeterminación informativa, toda vez que ahora la lucha contra la criminalidad organizada ha visualizado como una tarea primordial reducir este último derecho a su más mínima expresión, ya que se considera que es un muro y un obstáculo a una eficiente lucha contra la criminalidad.

5.5. El derecho a la autodeterminación informativa

Este derecho fundamental no es ningún nuevo derecho, sino que es la expresión de antiguos derechos como el derecho a la privacidad y al control del Estado, y a controlar que éste no limite los derechos de los ciudadanos de una manera insoportable, derechos que en alguna medida se han venido contaminando y reduciendo frente al avance constante y manifiesto de las tecnologías de la información y de la comunicación. Se trata de un derecho a saber y también un derecho a la transparencia del procesamiento de datos, el cual a su vez es una parte fundamental del concepto moderno de democracia.



Este derecho no sólo tiene validez para el almacenamiento de los datos, sino también a todo lo largo del proceso de obtención de la información, de tal manera que la forma de almacenamiento de los datos (manual o electrónica) no tiene un verdadero papel fundamental. Tampoco tiene importancia la clasificación de los diversos tipos de datos ya que no existen datos que por sí mismos carezcan de interés. En un procesamiento de datos que permite la rápida comparación, unión, listado y análisis de todos los datos posibles de una persona, ya no tendría interés hablar de datos de mayor o menor importancia, o de datos de mayor o menor privacidad, ya que la construcción de perfiles de personalidad se realiza con la ayuda de todos los datos posibles, por lo que el ámbito de protección de este derecho se encuentra fuertemente caracterizado por la índole especial de los intereses en conflicto en el procesamiento de datos, principalmente del interés del ciudadano de tener control sobre quién y en qué forma, con cuáles objetivos y bajo qué circunstancias, tiene acceso a sus datos personales.

El Tribunal Constitucional Alemán dedujo este derecho a la autodeterminación informativa al establecer una relación directa entre el derecho general a la personalidad y la dignidad del ser humano (artículo 2, párrafo 1 y el artículo 1 de la Ley Fundamental alemana). Esta línea interpretativa es clara si se entiende que este Tribunal meditó sobre la relación posible entre el control estatal de los datos de los ciudadanos y la posibilidad de una verdadera democracia compuesta por seres humanos que no tienen la posibilidad de auto-determinarse, muy especialmente en el ámbito del área más íntima de sus vidas.

Es indudable que una catalogación de los ciudadanos también era posible por medios manuales no electrónicos, sin embargo tal posibilidad no era viable sin una utilización masiva de recursos humanos, materiales y de tiempo. Con el procesamiento electrónico de datos tal meta es alcanzable con una precisión extraordinaria y sin un empleo ingente de recursos.

El riesgo de la construcción de perfiles de personalidad, a través de los cuales es posible catalogar a los ciudadanos y a los grupos sociales, y tomar medidas de prevención social así como otras medidas de control está en la base misma de la reflexión del tribunal. Cuando éste afirma que no existen ya más datos sin interés, se está refiriendo al hecho de que para la construcción de perfiles de los ciudadanos cualquier detalle, característica, circunstancia o evento en su vida, que de cualquier otra manera pasaría desapercibido, es de una importancia decisiva para los fines del control estatal. Estas personas, así catalogadas, verían reducidas totalmente sus posibilidades de cumplir un papel social activo, ya que de muchas maneras se les negaría un amplio acceso a los medios sociales, ya sea porque se les ha catalogado como grupos de riesgo, asociales, peligrosos, como sospechosos, como políticamente inconvenientes, como enfermos, como delincuentes o bien como deudores que no honran sus deudas o incluso como intelectuales comprometidos. El valor de este catálogo de características o de roles sociales tiene sentido en el contexto de una política estatal, y esto no es forma alguna una invención de un sueño descomunal y trágico perteneciente a una novela de fantasía, sino la trágica realidad a la que se enfrentan muchos ciudadanos en muchos lugares del mundo, en donde existen regímenes de carácter autoritario.



El Tribunal Constitucional Federal alemán observó este peligro y declaró que en los casos donde los individuos estén totalmente subordinados a la colectividad y sometidos a ella, de tal manera que sus derechos individuales queden prácticamente sin ningún vigor o validez, nos encontramos en presencia de un sometimiento de carácter inconstitucional.

Se configura de esta manera el "derecho a la autodeterminación informativa" como un derecho que pretende enfrentar el problema de "contaminación" a la que se enfrentan muchas libertades individuales consignadas en las Constituciones Políticas producto de los efectos provenientes de las nuevas tecnologías. Como un derecho fundamental de tercera generación es un derecho que tiene un valor de solidaridad, alcanzable por tanto a partir de un esfuerzo conjunto de la sociedad. En cuanto a su carácter de derecho fundamental, hay una discusión todavía presente en el ámbito doctrinario alemán, que apenas ha cedido paso al análisis de los problemas que enfrenta el datenschutz en relación con el desarrollo acelerado e inagotable de la tecnología de la información, que casi ha dejado atrás muchos de los principios y formas de garantía consignados en las legislaciones sobre la materia. Sin embargo, y a pesar de que la discusión doctrinal se mantiene, el mismo Tribunal Constitucional Federal Alemán se ha referido a él en una de sus más recientes sentencias como al derecho fundamental a la autodeterminación informativa. De igual manera, el Prof. Spiros Simitis, quien fuera Comisionado de la Protección de Datos del Estado de Hesse, y un crítico de su aceptación como derecho fundamental, ante la posibilidad de que se patrimonializará su protección y su interpretación, en un artículo reciente



propuso su incorporación constitucional como ya lo hicieran en Europa: España y Portugal, y en América Latina: Brasil, Colombia y algunas Constituciones provinciales en Argentina.

Un área interesante de preocupación para el derecho a la protección de datos lo constituye, evidentemente, el proceso penal. Es en esta zona donde se pueden detectar, en los últimos años, una creciente cantidad de cambios conducentes a una reducción de las posibilidades de control del ciudadano de los datos que pueden ser obtenidos y procesados por las autoridades de la investigación criminal. No se trata, como en otras épocas, de una mayor rudeza y crueldad en los métodos utilizados para la obtención de la "verdad real", sino ahora más que nunca de una serie de métodos altamente sutiles e incruentos, que muchas veces hasta son apetecidos por los ciudadanos, debido a que no se percibe en un primer momento su peligrosidad como herramienta de control y vigilancia sin límites.

Hoy en día se discute en la República Federal de Alemania como un tema central, en los diferentes proyectos legislativos dirigidos a adoptar medios electrónicos de obtención y procesamiento de datos personales en el proceso penal, la mayor o menor incidencia de estos instrumentos en el derecho a la autodeterminación informativa, a fin de que si se aceptan como medios de prueba, los mismos tengan limitaciones acorde con su carácter particularmente intrusivo en los derechos fundamentales del ciudadano, muy especialmente en su derecho a la privacidad.



5.6. Funcionalización del derecho penal en el estado de derecho

Se trata, hoy más que nunca, de hacer evidente cuál es la tendencia que reina en la actual política de la "funcionalización del derecho penal", en la cual existe bajo la bandera de un derecho procesal penal "eficiente", un caldo de cultivo para nuevos y más profundos ataques al derecho del ciudadano a controlar que tipo de informaciones sobre su persona existen en manos de las agencias del control penal.

El uso de nuevos medios de investigación en el proceso penal obliga a una serie de reflexiones sobre el papel del Estado de derecho en el "moderno" proceso penal, al cual le han correspondido una serie de cambios acordes con las nuevas tareas que se le han confiado en el campo de la seguridad interna del Estado y del combate de la criminalidad organizada.

El reto de la búsqueda de la verdad real por medio de herramientas cada vez más sofisticadas y el acomodo de la política criminal a metas y fines propias de un discurso populista ocasionan una crisis de garantías en el proceso penal. Esta crisis puede comprenderse aún mejor cuando se piensa en la forma vertiginosa en que éste se ha ido despidiendo de muchas de sus garantías tradicionales en favor del acusado, garantías que subrayaban su carácter de "derecho constitucional aplicado". El nuevo "poder informativo" en manos de las autoridades de la investigación significa para el ciudadano más lesiones a sus derechos en la sociedad de la información. De hecho el peligro de que la personalidad del ciudadano sea más transparente frente al Estado se

ha ido convirtiendo, mediante el uso de medios cada vez más modernos de tratamiento de los datos personales, en una realidad. El desarrollo y amplio uso de herramientas modernas para la grabación de audio y video y para la observación de todas las actividades de los ciudadanos, incluso de aquellas actividades desviadas que son de preocupación de la sociedad, han hecho posible que el procesamiento de datos en manos de las autoridades de la investigación represente un importante campo de trabajo para los protectores de datos.

Los peligros de este poder informativo en manos de las autoridades de la investigación aumentan en la misma medida en que aumentan también las justificaciones de orden jurisprudencial y legal que pretenden respaldar este rearme del Leviatán investigador y castigador, lo cual hace que cualquier tesis que sostenga lo contrario, y pretenda una reafirmación de los derechos del ciudadano en esta edad informativa signifique, de hecho, y a nivel ideológico, simplemente una forma de establecer una protección de delincuentes, y en construir defensas para los "enemigos de la libertad, de la eficiencia y de la seguridad".

Estas contradicciones revelan ciertos problemas en el marco de los fines simbólicos del proceso penal: El proceso penal se ha convertido en una herramienta para tranquilizar conciencias en la opinión pública y en la lucha electoral. Se trata de demostrar que los peligros de la criminalidad pueden ser controlados con el poder de choque del proceso penal. La criminalidad, mientras tanto, es presentada sin contornos ni colores como un fantasma que se pasea por todos los rincones de la sociedad, y en donde la única medida para su destrucción consiste en rearmar a las



autoridades de la investigación, especialmente a la policía y al Ministerio Público, reduciendo al mismo tiempo los derechos y garantías del acusado en el proceso penal. Es debido a este panorama que una criminalidad necesitada de definición, como lo es la criminalidad organizada, ha permitido que se produzcan "reformas urgentes" que en realidad sólo tienen que ver con reducciones de derechos, ampliación de prerrogativas y de ataques a derechos fundamentales, así como también como con un recrudecimiento del derecho penal. La pregunta acerca de la necesidad de estos cambios no suele plantearse. La política sólo muestra las nuevas direcciones en que la lucha contra este fantasma debe realizarse.

La característica fundamental de estos cambios se notan en mayores posibilidades para grabar y procesar datos personales de personas inocentes, sobre las cuales no pesa ninguna sospecha de haber cometido delito, incluso más allá de las usuales capacidades de la policía para reaccionar frente a peligros.

Sin bien es cierto la tendencia no es nueva, ya que la misma viene desde los años 50 en que se iniciaron las discusiones acerca de la utilización del detector de mentiras en el proceso penal, sí se nota un mayor enfoque hacia la eficiencia del funcionamiento del proceso penal y hacia una limitación exagerada del discurso garantista de una política criminal que podríamos llamar democrática.

Un ejemplo claro del moderno estado de la discusión puede notarse en las discusiones acerca de la utilización de las "huellas genéticas" en el proceso penal, el cual, a pesar de los evidentes problemas técnicos y de derechos fundamentales que

este medio de prueba ofrece, se ha pretendido utilizar a diestra y siniestra, incluso manejándose números realmente ilusorios sobre la supuesta precisión de las conclusiones que pueden derivarse de su utilización.

5.7. Procesos penales en boga en Guatemala donde se utilizo la informática

Para analizar este tema, necesariamente se tiene que hablar acerca de CICIG en Guatemala. CICIG, es un ente estructurado por la Organización de Naciones Unidas que busca facilitar el apoyo internacional a Guatemala en sus problemas de justicia y seguridad investigando los cuerpos ilegales y aparatos clandestinos de seguridad y colaborando en el desmantelamiento de los mismos. La CICIG realiza una labor de cooperación y no sustituye ni suplanta la actividad del Estado de Guatemala. Pero es este ente uno de los precursores de la implementación de la utilización de la tecnología para resolver casos de alto impacto social en Guatemala.

La CICIG persigue fundamentalmente apoyar la lucha contra la impunidad en el país y apoyar al sistema de justicia, en especial al Ministerio Público en la investigación de aquellos cuerpos ilegales y aparatos clandestinos de seguridad que más atentan contra la población y debilitan la justicia.

La CICIG tiene tres características fundamentales: a. Es un órgano internacional patrocinado por Naciones Unidas, cuyo marco legal es el Convenio de creación suscrito entre el Gobierno de Guatemala y la Organización de Naciones Unidas, en el marco de los Derechos Humanos y en cumplimiento de los Acuerdos de Paz. Es un

órgano autónomo (...) tendrá reconocimiento legal y personalidad jurídica en el país.

b. Es una Comisión con un mandato específico: aportar al sistema de justicia en Guatemala a través de la investigación de los CIACS y la asesoría al Gobierno y al sistema de justicia para el desmantelamiento de los mismos. c. En el momento en que la CICIG detecte la comisión de delitos por parte de los miembros de los CIACS hará la denuncia correspondiente a una Fiscalía Especial del Ministerio Público que se establecerá para coordinar el trabajo con la CICIG. La acción penal misma será responsabilidad del Ministerio Público, tal y como lo establece la ley, la CICIG podrá constituirse como Querellante Adhesivo, figura penal establecida en nuestro Código Procesal Penal. El Proceso Penal que se realice se regirá por lo establecido en la Constitución y en las leyes pertinentes.

a) Investigaciones

La CICIG y la Unidad Especial de Fiscalía de Apoyo a CICIG, -UEFAC- trabajan en investigaciones penales directas o propias con auxilio de la tecnología, con el fin de determinar la existencia de cuerpos ilegales de seguridad y aparatos clandestinos, su estructura, formas de operar, fuentes de financiamiento así como posible vinculación con entidades o agentes del Estado y otros sectores que atenten contra los derechos civiles y políticos en Guatemala. Las investigaciones que a continuación se resumen son aquellas cuya información puede ser publicada y que de alguna manera se ha utilizado la tecnología para su esclarecimiento. Todas las otras investigaciones en curso se mantienen bajo estricta confidencialidad.

- **Caso Bus de Nicaragua**

En este caso, un bus proveniente desde Nicaragua hasta la Ciudad de Guatemala, fue descubierto el 8 de noviembre de 2008 en el Departamento de Zacapa abandonado y envuelto en llamas. En el interior del bus se encontraron los cadáveres de dieciséis personas. El trabajo en la escena del crimen y peritajes posteriores, pudo determinar que en su mayoría habían fallecido a consecuencia de disparos por arma de fuego. La Fiscalía Seccional de Zacapa inició la investigación, que fue trasladada días después a la UEFAC, la cual con el apoyo de los Investigadores de la CICIG, la PNC, DINC-SAIA e INACIF realizó una serie de diligencias y pesquisas en coordinación con el Ministerio Público de Nicaragua. Adelantada la investigación, el 26 de marzo de 2009, se logró establecer la forma en que fueron asesinadas las personas mencionadas e identificar a la organización criminal que planeó, organizó y ejecutó los hechos: estructura dedicada al tráfico de cocaína, tráfico de armas, asesinato de personas por encargo, lavado de dinero, entre otros delitos. El 29 de junio de 2009, la UEFAC, presentó ante el Juzgado de Instancia Penal de la Ciudad de Zacapa, acusación en contra de Juan Carlos Policarpio Chinchilla, por los delitos de asesinato, conspiración y asociación ilícita y en contra de Rony Terraza, vinculado y detenido por encubrimiento impropio.

Posteriormente, la Cámara Penal de la Corte Suprema de Justicia accedió a la solicitud del Fiscal General, de trasladar el proceso al Tribunal que conoce los casos de alto riesgo en la Ciudad de Guatemala, a efectos de continuara con el trámite procesal y luego de abrir a juicio el siete de junio de dos mil diez, el Tribunal Primero de Sentencia



Penal, Narcoactividad y Delitos contra el Ambiente, dictó sentencia condenatoria en contra de Juan Carlos Policarpio Chinchilla y Rony Eduardo Terraza Hernández.

Así mismo, con posterioridad, siempre en el mismo caso, luego de continuar con la investigación, respectiva, determina que existían otras personas a las cuales se debía vincular al proceso, por lo que luego de realizar la solicitudes respectivas, se emiten ordenes de aprehensión, con lo cual, hasta la presente fecha, aún hay tres personas ligadas a proceso y contra las cuales, aún esta pendiente de determinar en audiencia de debate respectivo, si existe culpabilidad de los acusados y el grado de participación en el mismo.

- Caso Víctor Rivera

En este asunto, el 7 de abril de 2008, el ex asesor del Ministerio de Gobernación, Víctor Josué Rivera Azuaje, fue asesinado en el momento que conducía su automóvil en la Ciudad de Guatemala acompañado de su secretaria María del Rosario Melgar Martínez, quien resultó herida. La investigación fue trasladada a la UEFAC en el mes de octubre de 2008. Sin embargo, la Comisión estableció que en el trabajo de la escena del crimen, la cadena de custodia de las evidencias recuperadas, el manejo de los testigos e informantes y las prácticas de algunas diligencias, existió manipulación por parte de autoridades fiscales. Del estudio de los eventos criminales acaecidos con posterioridad al atentado, se ha establecido que varios de los informantes que trabajaban para el grupo antisequestros del Ministerio de Gobernación que asesoraba Víctor Rivera, fueron asesinados en fechas posteriores al hecho. La investigación

continúa, registrando importantes avances, de las cuales, es posible mencionar la reciente sentencia dictada en contra de diez personas más.

- **Caso Galindo**

Este caso, seguido en contra de Moisés Eduardo Galindo Ruíz y el ex coronel de infantería Luis Catarino Estrada Valenzuela, en su calidad de funcionarios del Ministerio de la Defensa Nacional durante el año 2001, durante el gobierno del presidente Alfonso Portillo, se les ligó a proceso por los delitos de peculado y falsedad ideológica en forma continuada. La investigación fue trasladada a la UEFAC en el mes de noviembre de 2008 y que además, se ha conexado al caso que se prosiguió contra Enrique Ríos Sosa, Luis Alberto Gómez Guillermo, Sergio Hugo Cárdenas Sagastume, Randolpho Leonel Chacón Álvarez, Miguel Ángel Salguero Torres, Pedro Adolfo Catalán Muñoz, por haber similitud entre los casos.

- **Caso Byron Vargas**

En este asunto, es de mencionar que el 20 de abril de 2008, en el municipio de Estanzuela, Departamento de Zacapa, fueron asesinadas tres niñas, iniciando la investigación en la Fiscalía Distrital de Zacapa y de la cual, se indicó que Byron Humberto Vargas Sosa, era el principal sospechoso del crimen. En el mes de octubre de 2008, la UEFAC conoció el caso, agilizándose así la investigación y lográndose la total y plena identificación del principal sospechoso. El 15 de febrero de 2009, Byron Vargas fue detenido por oficiales de la Policía Nacional Civil,



portando una cantidad importante de armas de fuego. Se procede por parte de la UEFAC a formularle cargos en la primera declaración a Vargas Sosa por el triple asesinato, siendo ligado a esta investigación por el Juez de Primera Instancia Penal, Narcoactividad y Delitos Contra el Ambiente del Departamento de Zacapa, por el delito de asesinato. En el curso de la investigación, se logra identificar a Esteban Bolvito Pérez y Mario Enrique Cojoc Quej, como las personas que participaron en los hechos con Vargas Sosa, siendo ligados por la comisión del delito de asesinato. En junio 2009, la Cámara Penal de la Corte Suprema de Justicia, accedió a la solicitud del Fiscal General de la Nación de trasladar el proceso al tribunal que conoce los casos de alto riesgo en la Ciudad de Guatemala donde se llevó a cabo la diligencia de apertura a juicio de la cual se remitieron las actuaciones correspondientes al Tribunal Octavo de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente, el cual dictó sentencia del 24 de octubre de 2011.

- Caso Rosenberg

El día 10 de mayo de 2009, en la Ciudad de Guatemala, fue asesinado el abogado Rodrigo Rosenberg Marzano. La Fiscalía de Sección de Delitos contra la Vida y la Integridad Personal inició la investigación con el Equipo de Escena del Crimen de la DICRI. El 14 de mayo de 2009, el expediente fue trasladado a la UEFAC. Adelantada la investigación el 11 de septiembre de 2009, se realizaron operativos en la ciudad con el apoyo de la Policía Nacional Civil y el Ejército Nacional, que permitió la captura de diez personas de la organización criminal vinculada al

asesinato. Estas personas fueron puestas a órdenes del Juzgado Décimo de Primera Instancia Penal, quien los ligó al proceso por los delitos de asesinato y asociación ilícita.

En este caso la Comisión Internacional Contra la Impunidad en Guatemala (CICIG) y su jefe en ese entonces, Carlos Castresana, indicó a los medios de comunicación, que el abogado Rodrigo Rosenberg Marzano, planificó su asesinato, mientras paseaba en una bicicleta, haciendo una exposición meticulosa de cómo ocurrió y quiénes planificaron y ejecutaron el asesinato, en este controversial caso. La conclusión a que llegó la CICIG luego de una exhaustiva investigación es que Rosenberg planificó su inmolación, simulando que era contra un extorsionista que quería matarlo. "El que dio la instrucciones (de su asesinato) fue el mismo Rosenberg", enfatizó el ex jefe de la CICIG.

El comisionado hizo ver que el equipo de investigadores estuvo en lugar de los hechos desde el día del crimen: "Se nos dijo de la trascendencia del asesinato, así que estuvimos ahí desde el propio 10 de mayo", puntualizó. Luego de varios meses de investigación, hay 11 personas detenidas vinculadas a este caso y 4 más permanecen prófugos, haciendo un total de 15 los implicados, entre éstos los que participaron en forma material y los intelectuales.

La CICIG expuso en la conferencia de prensa que organizó, que fue el mismo Rosenberg quien compró los celulares utilizados en el proceso de la planificación de su crimen y que él mismo se hacía las llamadas para simular que estaba

amenazado de muerte, todo ello con la ayuda de la informática.

Los investigadores analizaron los videos captados por las cámaras de seguridad de edificios cercanos al lugar del asesinato del abogado y lograron identificar a los tres vehículos vistos en ese lugar, días antes y el día del hecho, pues de uno de ellos descendió quien disparó contra Rosenberg. Fue así como se identificó a los autores materiales.

Finalmente, Castresana dijo que serán los Tribunales de justicia los que al final dictaminen la culpabilidad o inocencia de los sindicados, la CICIG sólo ha presentado las conclusiones a las que llegaron las investigaciones.

- **Caso Musa**

El día 14 de abril de 2009, cuando el señor Khalil Musa y su hija Marjorie Musa Maldonado, se conducían sobre la avenida Petapa, en la zona doce de la ciudad de Guatemala, en donde fueron interceptados por sujetos que se desplazaban en una motocicleta, quienes accionaron armas de fuego y segaron sus vidas. La investigación fue iniciada por la Fiscalía de Sección de Delitos contra la Vida y la Integridad Personal del Ministerio Público y trasladada a la UEFAC, el 15 de mayo de 2009, la cual continúa con ella. No obstante el tiempo transcurrido desde los hechos, se ha logrado recuperar información determinante de la escena del crimen y se adelantan labores para identificar a los individuos que ejecutaron los asesinatos.



- **Caso Amatitlán**

El 24 de abril de 2009, unidades del Servicio Antinarcóticos de la Policía Nacional Civil, acudieron a un complejo de bodegas ubicado en la ruta de la Ciudad de Guatemala, al Pacífico para una operación antidrogas. Al encontrar resistencia, se produjo un enfrentamiento y como consecuencia de ello hubo cinco muertos. Al requisar los vehículos abandonados por los asaltantes, encontraron en uno de los vehículos un lanzagranadas, fusiles y municiones. En otro vehículo se encontraron 370 kilos de cocaína. Registrada la bodega incautaron otros paquetes de cocaína listos para ser cargados, abundante armamento de uso militar y 13 vehículos, entre camiones y camionetas, algunos con placas de México y Estados Unidos de América. Las primeras diligencias fueron realizadas por la Fiscalía de Escuintla con apoyo de la Fiscalía de Sección contra Narcoactividad, donde se radicó la investigación. Posteriormente fue trasladado el expediente a la UEFAC. La investigación se adelanta para establecer la forma en que ocurrieron los hechos, la identificación de los miembros de la organización de narcotraficantes propietarios del estupefaciente y que ocasionaron la muerte a los policías de la PNC-SAIA.

- **Caso twitter**

En el presente caso, se puede apreciar el actuar de una personas en las redes sociales, tal como lo hiciera Jean Anleu Fernández, quien mediante la red social llamada Twitter, publicara “Primera acción real “sacar el pisto de Banrural Quebrar al banco de los corruptos”, el 12 de mayo de 2009, a las 14 horas, por lo que el 14 de



mayo de ese mismo año, fue capturado en la empresa donde trabaja por agentes de la Policía Nacional Civil (PNC) bajo la acusación de promover el pánico financiero.

Luego de la detención de Jean Anleu Fernández, durante un allanamiento en su residencia de la zona 8 de Guatemala la policía decomisó su computadora por solicitud de la fiscalía de bancos del Ministerio Público. Según la ley en Guatemala que juzga a Jeanfer, él está acusado de cometer delito de pánico financiero. La Ley sanciona con 5 mil quetzales y 50 mil quetzales más prisión de uno a tres años. Jeanfer es el primer usuario de Twitter detenido en Guatemala por el delito de pánico financiero. Pero según el contexto en el que se encuentra el país, muchos usuarios en Twitter opinan que esto no es más que una forma de represión para la libertad de expresión porque un mensaje o dos para un usuario con menos de 300 seguidores, no podría causar un pánico financiero.

Genaro Pacheco, fiscal a cargo del caso, indicó que le dieron seguimiento a lo que salió publicado en Internet y se giró la orden de captura. "El acusado confesó haber escrito el mensaje."

Días atrás Edgar Barquín, superintendente de Bancos, explicó en conferencia de prensa que se tomarían todas las acciones legales a quienes provocaran pánico financiero.

El decreto 64-2008 que crea el delito de pánico financiero, expresa que elaborar, divulgar o reproducir por cualquier medio o sistema de comunicación, información falsa



o inexacta que menoscabe la confianza de los clientes, usuarios, depositantes o inversionistas de una institución sujeta a la vigilancia e inspección de la Superintendencia de Bancos deberá ser procesado.

Según el artículo 342.B, el responsable será sancionado con prisión de uno a tres años y una sanción económica de entre Q5 mil y Q50 mil. Las penas se incrementan si se comprueba que quien cometió el delito conocía los daños que podría causar a la institución o bien, trabajaba en el banco.

b) CICIG como querellante adhesivo

Entre los casos que la CICIG es querellante adhesiva, se destacan los siguientes:

- Masacre del 25 de marzo de 2008 en el departamento de Zacapa

Enfrentamiento entre dos grupos armados ilegales en el municipio de Rio Hondo, departamento de Zacapa, que dejó como consecuencia nueve personas asesinadas, tres heridas y seis capturadas. Investigaciones posteriores permitieron detener a otras cinco personas. El 9 de julio de 2009 se celebró la audiencia de ofrecimiento de prueba y se está a la espera de que se fije fecha y hora para la iniciación del debate. Asumiendo la función de querellante adhesivo por primera vez en su mandato en el caso de la masacre de Zacapa, CICIG puso de manifiesto su compromiso con el Ministerio Público de Guatemala para reforzar su posición procesal en aquellos supuestos en que la capacidad de violencia y corrupción del grupo delictivo acusado, podría llegar a generar impunidad.

- **Caso Portillo**

Alfonso Antonio Portillo Cabrera, Presidente de la República en el período comprendido del 2000 al 2004, fue entregado por las autoridades mexicanas a su homólogos guatemaltecos el 7 de octubre del 2008, en razón a una solicitud de extradición iniciada en el año 2005 por el delito de peculado. La acusación se fundamenta en que en el año 2001 fueron sustraídos del presupuesto asignado al Ministerio de la Defensa Nacional ciento veinte millones de quetzales, de los cuales al menos treinta millones fueron invertidos por el ex presidente Alfonso Portillo a título personal y para beneficio propio. La investigación vincula al procesado con otros altos funcionarios de su gobierno en la apropiación de más de cuatrocientos millones de quetzales. El proceso se encuentra en la fase intermedia pendiente de la apertura a juicio.

Eduardo Arévalo Lacs, Ministro de la Defensa Nacional del gobierno del Presidente Portillo en el año 2001, refrendó el Acuerdo Gubernativo número 16-2001 que permitió la modificación del presupuesto del Ministerio de la Defensa Nacional por la cantidad de ciento veinte millones de quetzales. Por estos hechos se encuentra procesado y bajo detención.

Se indicó que en los hechos participaron también los militares en retiro Napoleón Rojas Méndez y Jacobo Esdras Salán Sánchez, en calidad de Asesor de Seguridad y como persona de confianza del Presidente Alfonso Antonio Portillo Cabrera, respectivamente. El 25 de junio de 2009, el Juzgado Octavo de Instancia Penal de Guatemala emitió órdenes de captura en contra de los tres acusados, por el delito de peculado. Sólo fue

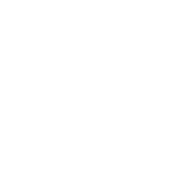
posible ejecutar la orden de captura de Eduardo Arévalo Lacs quien quedó ligado a proceso por el delito de peculado, además de imponerle una fianza de cuarenta millones de quetzales, rebajada en dos oportunidades a cinco millones y luego a cuatro millones. Sobre los otros imputados, se encuentra pendiente su captura y se ha dado información a la Interpol.

El ex general Enrique Ríos Sosa, junto con Miguel Ángel Salguero Torres, Luis Alberto Gómez Guillermo, Sergio Hugo Cárdenas Sagastume, Randolpho Leonel Chacón Álvarez y Pedro Adolfo Catalán Muñoz son procesados de tomar parte directa en la sustracción de diferentes cantidades de dinero que suman cuatrocientos cuarenta y un millones de quetzales del erario nacional durante los años 2001 y 2002 en su calidad de funcionarios del Ministerio de la Defensa Nacional. El 25 de marzo de 2009, el Juez de Instancia Penal de Turno de la Ciudad de Guatemala, emitió las órdenes de captura en contra de los ex funcionarios citados imponiéndoles medida cautelar de arresto domiciliario.



CONCLUSIONES

1. La sociedad del conocimiento ha dado lugar al derecho informático, con sus propias leyes, su propia autonomía y sus relaciones con otras ramas fundamentales del mundo jurídico, como el derecho penal. De manera que la informática y el derecho son dos nuevos aliados al servicio de las sociedades, de los negocios y de la justicia.
2. El crimen informático incluye la conducta antijurídica, no ética o no autorizada, relativa con el procesado automático de datos y/o transmisiones de datos. Es así que existen muchas conductas ilícitas que se producen día a día en la red o en sistemas informáticos y resultan difíciles de descubrir, denunciar y probar debido a la falta de regulación para una efectiva sanción penal.
3. Referirse a informática forense, es mencionar un contexto teórico de operaciones y formalismos legales. Los instrumentos informáticos son base para analizar las evidencias digitales en los medios informáticos. Pero, hay ausencia de una formalidad adicional que valide la seguridad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza.
4. La organización criminal en Guatemala, y el aumento de ésta, así como el aprovechamiento de las fallas humanas al usar procedimientos tecnológicos para concertar delitos, son la razón de existencia de la informática forense, ya que es una disciplina auxiliar de la justicia moderna, para enfrentar al delito informático y garantizar la veracidad de la evidencia digital que pudiese aportar en un proceso de alto impacto social.





RECOMENDACIONES

1. Debe ser estudiada y normada adecuadamente por el legislador guatemalteco la era de la Internet, ha surgido toda una serie de nuevos delitos penales, a través de cambios en la contratación electrónica, propiedad intelectual, medios de pago, sistema registral, teletrabajo y comercio, la banca e industria mundial; mismos que constituyen un promisorio campo de acción jurídica, que.
2. Es necesario que el Organismo Legislativo, haga la creación y aplicación de una nueva herramienta jurídica, como lo es la informática forense, para ser usada para esclarecer los hechos considerados como delitos; puesto que junto al avance y desarrollo tecnológico de los países, surgen nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir; por lo que.
3. Es esencial que el Ministerio Público de Guatemala ingrese al mundo de la ciencia, específicamente informática forense; para que, con ello pueda, de manera concreta y eficiente, basar sus acusaciones con mayor credibilidad para el juzgador.
4. La sociedad guatemalteca debe tomar conciencia respecto a la manera de usar las nuevas tecnologías de información, ya que el usuario debe tener presente que este beneficio tecnológico de comunicación rápida y económica tiene que emplearse con responsabilidad; sobre todo en la administración de la información.





BIBLIOGRAFÍA

BARRERA LÓPEZ, Horacio Mauricio. **Derecho informático en la curricula universitaria.** Universidad de San Carlos de Guatemala, Guatemala.(s.f)

BARRIENTOS PELLECCER, César Ricardo. **Derecho procesal penal guatemalteco.** Magna Terra Ed.; Guatemala, 1995.

BRAÑAS, Alfonso. **Manual de derecho civil.** Universidad de San Carlos de Guatemala, Guatemala: Ed. estudiantil Fénix, 1998.

CABANELLAS, Guillermo. **Diccionario de derecho usual.** Editorial Heliasta: S.R.L. 1981.

CALSAMIGLIA, **Ciencia Jurídica. El derecho y la justicia.** Madrid: Editorial Trotta, 1996.

CASTILLO GONZÁLEZ, Jorge Mario. **Derecho administrativo guatemalteco.** Guatemala: Editorial Impresiones Gráficas. 2005.

CLARO SOLAR, Luis. **Explicaciones de derecho civil chileno y comparado.** Santiago: Editorial Jurídica de Chile, 1978.

COBO DEL ROSAL, Manuel y otros. **Curso de derecho penal español.** Parte Especial, tomo I, editorial Jurídicas y Sociales, Madrid: 1996.

CRUZ OCHOA, Ramón de la. **El delito de estafa.** Ediciones ONBC. La Habana, Cuba: 2001.

DAMIANOVICH de CORREDO, Laura. **Delitos contra la propiedad.** 3ra edición catalizada, Buenos Aires, Argentina: editorial Universidad S.R.L, Septiembre 2000.

DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de derecho informático.** Pamplona, España: Ed., Aranzadi. 1997.



Diccionario jurídico Espasa. Madrid España: Editorial Espasa Calpe, S.A. 1999.

Diccionario enciclopédico Larousse. México D.F.,: Agrupación Editorial, S.A. 1996.

Diccionario de ciencias jurídicas, políticas y sociales. Buenos Aires, Argentina: Ediciones Heliasta, 2001.

Diccionario hispánico universal. Tomo I. de W.M. Jackson Editores. México: 2001.

Diccionario de la lengua española. Vigésima edición. Ed. Espasa-Calpe. Madrid, España: 1984.

Diccionario de la Real Academia de la Lengua Española. Editorial RAE; España: 1992. Pág. 553.

HUERTA M., Marcelo y Líbano M. Claudio. **Delitos informáticos.** Editorial Cono Sur, Chile: 1996.

GABALDÓN, Gerardo, Luis y P. Wilmer. **Usurpación de identidad certificación digital: propuestas para el control del fraude electrónico.** Porto Alegre, Brasil: Ed., Sociologías, junio 2008.

GARCÍA AÑÓN, José. **Métodos y técnicas para la realización de trabajos de investigación.** Editorial Universidad de Valencia, Valencia: 1993.

MORGAN SANABRIA, Rolando. **Material de apoyo para el curso planeación del proceso de la investigación científica.** Tesorería de la Facultad de CIENCIAS Jurídicas y Sociales, EDIFICIO s-7 Universidad de San Carlos de Guatemala.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas políticas y sociales.** Editorial Helista: S.R.L. 1979.



PALOMINO MARTÍN, José. **Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del derecho penal.** Editorial Tirant lo Blach, España: 2007.

PESCIO, V. **Manual de derecho civil.** Tomo I. Santiago: Editorial Jurídica de Chile: 1978.

QUEZADA TORUÑO, Fernando José. **La informática jurídica y el notariado en Guatemala.** Boletín No. 8 del Instituto Guatemalteco de Derecho Notarial. Guatemala: 2004.

STREETER PRIETO, Jorge. **Ensayo la ciencia del derecho.** Universidad de Santiago de Chile, Chile: 2002. Pág. 286.

SILVA SÁNCHEZ, Jesús-María. **La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales.** 2º. Ed., rev. y ampliada, Civitas, Madrid: 2001.

TOCORA, Fernando Luís. **Derecho penal especial.** Librería del profesional, editorial ABC, 8va edición, Bogotá, Colombia: 2002.

VODANOVIC, Antonio. **Tratado de derecho civil: Parte preliminar y general.** Tomo I. Santiago: Editorial Jurídica de Chile: 1998.

Legislación.

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

Código Civil. Decreto Ley 106. Promulgado en el gobierno de Enrique Peralta Azurdia, en 1963.

Código Procesal Civil y Mercantil. Decreto Ley 107. Promulgado en el gobierno de Enrique Peralta Azurdia, en 1963.

Código Procesal Penal. Congreso de la República de Guatemala, Decreto 51-92



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

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