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

¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?

LUISA INÉS ORTÍZ

GUATEMALA, JUNIO 2015

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

¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

LUISA INÉS ORTÍZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, junio 2015

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	MSc.	Avidán Ortiz Orellana
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Licda.	Rosario Gil Pérez
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Mario Roberto Méndez Alvarez
VOCAL V:	Br.	Luis Rodolfo Aceituno Macario
SECRETARIO:	Lic.	Daniel Mauricio Tejeda Ayestas

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 08 de noviembre de 2013.

Atentamente pase al (a) Profesional, OMAR RICARDO BARRIOS OSORIO, para que proceda a asesorar el trabajo de tesis del (a) estudiante LUISA INÉS ORTÍZ, con carné 200140937, intitulado ¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?.

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

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

Adjunto encontrará el plan de tesis respectivo.

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

DR. BONERGE AMILCAR MEJÍA ORELLANA
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción ____/____/____. f) _____
Asesor(a)

Licenciado Omar Ricardo Barrios Osorio

Abogado y Notario
Colegiado 7138 No. Teléfono 22519234
Dirección 14 Calle 3-17 zona 1 Segundo Nivel Oficina 205 Ciudad Capital.

Guatemala, 14 de julio de 2014

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
24 JUL. 2014
UNIDAD DE ASESORÍA DE TESIS
Hora:
Firma:

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

Distinguido Licenciado:

En cumplimiento del nombramiento recaído en mi persona, procedí a asesorar el trabajo de tesis de la estudiante Luisa Inés Ortiz, titulado, **"¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?"**; y para lo cual emito el siguiente dictamen:

Al analizar el trabajo de tesis de la bachiller Luisa Inés Ortíz, se hace constar que el contenido científico y técnico de la tesis, se ajusta al tema desarrollado y en virtud de haberse satisfecho las exigencias del suscrito asesor, en realizar las modificaciones de forma y de fondo para mejorar la investigación, el mismo constituye un aporte al contenido científico y técnico al Derecho de nuestro país.

El tema abordado en la investigación de tesis **"¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?"**, hace al principio la descripción de la doctrina general de las disciplinas de la criminalística y entre ellas se menciona la informática forense; posteriormente una exposición del delito de informática forense, así como casos concretos de hechos ilícitos cometidos en la banca electrónica en el país. Asimismo, se describieron las acciones típicas del delito informático establecidas en Colombia, Costa Rica, República Dominicana, Perú comparando con lo descrito en el Código Penal guatemalteco y la iniciativa de ley 4055 proyecto de ley de delitos informáticos. Finalmente se determinó el estado actual de los servicios de banca en línea, la importancia y la implementación adecuada para la aplicación de la Informática Forense

Omar Ricardo Barrios Osorio
ABOGADO Y NOTARIO

Licenciado Omar Ricardo Barrios Osorio

Abogado y Notario
Colegiado 7138 No. Teléfono 22519234
Dirección 14 Calle 3-17 zona 1 Segundo Nivel Oficina 205 Ciudad Capital.

en la investigación de delitos cibernéticos en el sistema bancario guatemalteco, tomando en cuenta a las instituciones que deben de participar en la investigación como en la prevención de dichos hechos delictivos.

La bachiller Luisa Inés Ortíz, desarrolló una investigación utilizando los métodos sintético-analítico, inductivo-deductivo y jurídico, lo que permitió entrelazar la historia, partiendo de los principios generales de la disciplina del derecho objeto de estudio a la realidad actual; fueron aplicadas las reglas de redacción y ortografía correctamente, siguiendo las normas estipuladas de la Real Academia de la Lengua Española; trabajo de tesis que constituye un aporte científico a esta facultad, contribuyendo doctrinaria y jurídicamente en materia de investigación y prevención de hechos ilícitos cibernéticos, tomando como punto de referencia la banca en línea; la conclusión discursiva, las bases legales en cada uno de los temas desarrollados dentro de la investigación y al haberse cumplido con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales del Examen General Público; concluyo, en virtud de haberse satisfecho las exigencias del suscrito asesor, derivadas del examen del trabajo y por las razones expuestas resulta procedente emitir **DICTAMEN FAVORABLE**, a efecto que el presente trabajo sea aprobado y discutido posteriormente en revisiones tanto de forma, de fondo y finalmente en el examen general público correspondiente. Así mismo expresamente declaro no ser pariente de la estudiante dentro de los grados de ley.

Atentamente,

Omar Ricardo Barrios Osorio
ABOGADO Y NOTARIO

Lic. Omar Ricardo Barrios Osorio
ASESOR

"ID Y ENSEÑAD A TODOS"

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 03 de octubre de 2014.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante LUISA INÉS ORTÍZ, titulado ¿CÓMO SE DEBE APLICAR LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE DELITOS CIBERNÉTICOS EN EL SISTEMA BANCARIO GUATEMALTECO?. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

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

BAMO/srrs.

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

Lic. Avidán Ortiz Orellana
DECANO

DEDICATORIA

A DIOS: Por su infinita bondad y misericordia, por permitirme luchar por mis objetivos, porque a pesar de todo siempre está a mi lado.

A MI MADRE: Desde el cielo te has encargado de enviarme tus bendiciones, siempre vives en mis pensamientos, gracias por darme la vida.

A MIS ABUELOS: Por su amor, su ejemplo de trabajo y su entrega hacia nosotros; principalmente a mi abuelita María Luisa Pérez, por enseñarme que con esfuerzo y dedicación alcanzo mis objetivos.

A MIS HERMANOS: Porque a pesar de las circunstancias y momentos difíciles hemos aprendido a salir adelante.

A MI HIJO: Diego Alejandro, porque desde el primer día que te vi una cosa entendí, quiero predicarte con mi ejemplo y verte convertido en un hombre de bien.

A LA UNIVERSIDAD: De San Carlos de Guatemala, la Tricentenaria, Alma Máter que permitió que me formara como profesional.

A LA FACULTAD: De Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, de cuyas aulas tengo privilegio ser egresada.

PRESENTACIÓN

La presente investigación pertenece a la rama del derecho público, al describirse los delitos del derecho informático y su investigación a través de métodos de la criminalística, contenidos dentro del derecho penal, es una investigación de tipo cualitativa porque se establecieron fenómenos sociales y la aplicación de la hermenéutica jurídica; que permitió un análisis comparativo interpretativo del derecho nacional e internacional acerca del problema planteado.

Se realizó aproximadamente en seis meses, su objeto fue determinar cómo debe utilizarse la informática forense en la investigación de delitos cibernéticos en el sistema bancario guatemalteco, los sujetos de estudio fueron casos de delitos cometidos dentro de la banca electrónica en el país.

El aporte académico que da la investigación es dar a conocer a la comunidad estudiantil, los problemas jurídicos presentados dentro del comercio electrónico especialmente en el servicio e-banking, así como, la solución a través de los elementos científicos jurídicos que provee la criminalística y participación que el Estado de Guatemala debe tener en este fenómeno socio-jurídico.

Aunado a lo anterior la presente investigación estableció la falta de participación estatal en la resolución de delitos, así como las deficiencias legales para prevenir dichos hechos ilícitos. La inexistencia de coordinación interinstitucional, entre el Instituto Nacional de Ciencias Forenses y la Superintendencia de Bancos. En consecuencia a ello se describió la forma de aplicar la informática forense dentro de nuestro ordenamiento jurídico, observando legislación latinoamericana acerca del tema y técnicas aplicadas a la seguridad informática en general, así como sistemas de prevención.

HIPÓTESIS

La informática forense debe aplicarse en el sistema bancario guatemalteco para adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, que determinen la compensación de los daños causados por los criminales o intrusos.

COMPROBACIÓN DE LA HIPÓTESIS

La propuesta de solución anticipada que se dio al problema planteado, fue comprobada en el desarrollo de la investigación, al establecer que no existe participación estatal en la investigación y prevención de los delitos informáticos, cometidos dentro de la banca en línea.

En cuanto a la investigación no existe un laboratorio especializado dentro del Instituto Nacional de Ciencias Forenses, asimismo en la Superintendencia de Bancos no se encuentra dotada de un marco legal adecuado, que les permita coadyuvar tanto con el instituto, como con las entidades bancarias del país en la prevención del delito.

Por lo que debe aplicarse la informática forense en el sistema bancario guatemalteco para adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente; guardados en un medio computacional, que determinen la compensación de los daños causados por los criminales o intrusos. Respecto a la metodología utilizada para el desarrollo de la presente investigación fueron los métodos: sintético-analítico, inductivo-deductivo y jurídico.

ÍNDICE

Pág.

CAPÍTULO II

CAPÍTULO III

Pág.

CAPÍTULO IV

Pág.

INTRODUCCIÓN

Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, es mucho más fácil la comisión de delitos por estas vías. Actualmente, en Guatemala, los ataques a los sistemas bancarios en línea son uno de los métodos más utilizados para robar dinero de los usuarios comunes. El número de delitos cometidos en esta área crece rápidamente en todo el mundo, a pesar de todas las medidas técnicas adoptadas; demostrándose de esta manera que la delincuencia organizada es cada vez más especializada.

Por otro lado, la informática forense es el análisis de la información digital contenida en dispositivos digitales, en servidores externos utilizados por una empresa, en algunos casos, en un sistema de información de terceros su objetivo es encontrar, por medio de distintas técnicas de análisis y clasificación, elementos con la fuerza probatoria suficiente para establecer la culpabilidad de un imputado por el delito.

El objetivo general que se alcanzó en la investigación fue la descripción de la forma de aplicación de los métodos de la informática forenses en los delitos cometidos en el sistema bancario guatemalteco, para la deducción de responsabilidades civiles, penales, etc., a quienes resulten culpables que sea el resultado de la adquisición, preservación y obtención de pruebas a través de esta técnica de la criminalística.

Los objetivos específicos de la presente investigación fueron desarrollados al describir: el establecimiento del estado actual de los servicios de banca electrónica en Guatemala, las consecuencias de la inseguridad de la banca electrónica, análisis comparado de delitos informáticos con énfasis en el e-banking, los métodos de la informática forense para combatir los delitos en internet, lo anterior para proponer la implementación de métodos y medidas de prevención dirigidas a las entidades

correspondientes que velan por la banca en Guatemala y coadyuvan a la administración de justicia.

El presente estudio está conformado por cuatro capítulos: el primero, describe doctrina general de las disciplinas de la criminalística y entre ellas se mencionara la informática forense; en el segundo, se realizó una exposición del delito de informática forense, así como casos concretos de hechos ilícitos cometidos en la banca electrónica en el país los cuales fueron: la piratería informática, el robo de identidad utilizando medios informáticos y el phishing; en el tercero, se describieron acciones típicas del delito informático establecidas en Colombia, Costa Rica, República Dominicana, Perú comparando con lo descrito en el Código Penal guatemalteco y la iniciativa de Ley 4055 proyecto de ley de delitos informáticos; finalmente el cuarto capítulo, determinó el estado actual de los servicio de banca en línea, la importancia y la implementación adecuada para la aplicación de la Informática Forense en la investigación de delitos cibernéticos en el sistema bancario de Guatemala, tomando en cuenta las instituciones deben tener participación tanto en la investigación como en la prevención de dichos hechos delictivos.

Para la realización de la presente investigación los métodos de investigación utilizados fueron el sintético-analítico, inductivo-deductivo y jurídico. En cuanto a las técnicas estas fueron fichas de trabajo, análisis, bibliográfica, reproducciones y dispositivo de almacenamiento.

El desarrollo del presente trabajo de investigación permite dar a conocer la necesidad y falta de interés que existe dentro del ámbito gubernamental, en apoyar y controlar delitos realizados por nuevas tecnologías, al no tener una legislación y reglamentación apropiada para que las entidades del Estado que correspondan puedan actuar con un mejor conocimiento en la investigación y prevención de hechos ilícitos cibernético, tomando como punto de referencia la banca en línea.

CAPÍTULO I

Dentro del presente capítulo, se hará una descripción teórica del origen, significado, características y otros temas relevantes sobre la criminalística forense, a la vez se abordara sobre la institución que fue creada para la aplicación de esta ciencias en la resolución de casos dentro de la República de Guatemala, mencionando su historia, definición, finalidad y principios, que son la base de la razón de existir y actuar de la ente estatal Instituto Nacional de Ciencias Forenses (INACIF). Por último se expondrá que métodos criminalísticos son utilizados por el Instituto de Ciencias Forenses en la resolución de delitos cibernéticos.

1. Criminalística

1.1. Antecedentes

La primera disciplina precursora de la criminalística fue lo que en la actualidad se conoce como dactiloscopia, es decir la ciencia que estudia las huellas dactilares[1]. El ilustre experto en investigación B.C. Bridges, en una de sus obras refiere lo siguiente: "(...) algunos de los primeros usos prácticos de la investigación mediante las impresiones dactilares son acreditados a los chinos, quienes las aplicaban diariamente en sus negocios y empresas legales, mientras tanto el mundo occidental se encontraba en el período conocido como la edad oscura"[2].

---

[1] Montiel Sosa, Juventino. **Criminalística.** Pág. 10
[2] http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm; (14 de septiembre de 2013)

Sostiene el autor Montiel Sosa que Kia Kung-Yen, historiador chino de la dinastía Tang, en sus escritos del año 650, hizo mención a la identificación mediante las impresiones dactilares, en un comentario sobre un antiguo método en la elaboración de documentos legales. De aquí se deduce que para el año 650 los chinos ya utilizaban las impresiones dactilares en sus tratos comerciales y en ese mismo año, hacían mención al método anterior al uso de las impresiones consistentes en la utilización de placas de madera con muescas iguales recortadas en los mismos sitios de los lados las que conservaban las partes del contrato e igualadas dichas tablas se podía constatar la autenticidad o falsedad de los contratos de referencia. Montiel, citado por los autores Castellanos y Ceballos, señalan: "el significado de muescas era el mismo de la identificación mediante las impresiones dactilares (hua-chi), de la actualidad".[3]

"Muchos años después, en 1575 surge otra ciencia precursora de la criminalística: la medicina legal, iniciada por el francés Ambrosio Paré y desarrollada por Paolo Sacchias en 1651. En 1665, Marcello Malpighi observaba y estudiaba los relieves dactilares de las yemas de los dedos y palmas de las manos. Una de las primeras publicaciones en Europa acerca del estudio de las impresiones dactilares apareció en Inglaterra en 1648, realizada por el doctor Nehemiah Grew, perteneciente al colegio de físicas y cirujanos de la Real Sociedad de Londres".[4]

"En 1686, nuevamente Malpighi hacía valiosas aportaciones al estudio de las impresiones dactilares tanto que una de las partes de la piel humano lleva el nombre de capa de Malpighi en 1753; otro ilustre estudioso y precursor es el doctor Boncher, quien

---

[3] **Ibíd**
[4] Montiel Sosa, Juventino. **Ob. Cit.** Página 10

realizo un estudio sobre balística, disciplina que a la postre se llamaría balística forense, también precursora de la Criminalística."[5]

Para la investigación criminalística uno de los métodos con mayor antigüedad y de gran utilidad en la actualidad fue la balística que "en 1809 el célebre francés Vidoc, fue incluido en las filas de la policía francesa y pronto se convirtió en el primer director de la seguridad nacional (Sûreté Nationale). A él se le atribuye el registro y creación de expedientes con las pesquisas de los casos y la introducción de los estudios (...) Fue el primero en utilizar moldes para recoger huellas de la escena del crimen, definiendo la otoscopia. Sus técnicas antropométricas tendrían gran repercusión"[6].

Otros métodos de investigación criminalística para coadyuvar a la investigación de hechos ilícitos se dan en el año "...1823 un tratado escrito por anatomista, fisiólogo y botánico checo Jan Evangelista Purkyně describe los tipos de huellas dactilares y las clasificó en 9 grupos. Durante ese mismo año, Huschke descrubrió los relieves triangulares, conocidos como deltas, de las huellas dactilares de los dedos. En 1835, aparece otro de los primeros precursores de la balística, Henry Goddard".[7]

"En 1840, con el español Mateo Orfila nace la Toxicología, ciencia que estudia los efectos de las toxinas o venenos vegetales, animales y minerales, tanto como tratamiento o intoxicación. El aporte de esta ciencia a la reconstrucción de homicidios y suicidios es enorme. William Herschel, en 1858, adoptó el uso de las impresiones dactilares para evitar la suplantación. En 1872 era una ciencia que auxiliaba a los

---

[5] http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm; **Ob. Cit.** (14 de septiembre de 2013)
[6] Montiel Sosa, Juventino. **Ob. Cit.,** Pág. 10
[7] **Ibíd.,** Pág. 10

jueces a esclarecer ciertos tipos de delitos, en donde los venenos eran usados con muchas frecuencias. Esta ciencia o disciplina también es considerada como precursora de la Criminalística".[8]

"En 1866, Allan Pinkerton, ponía en práctica la fotografía criminal para reconocer a los delincuentes, disciplina que posteriormente seria llamada fotografía judicial y actualmente se le conoce como fotografía forense."[9]

"Alfonso Bertillón creó en París el Servicio de Identificación Judicial en 1882, dado a conocer en 1885 y se adoptó de forma oficial en 1888. Este método antropométrico se basaba en el registro de las diferentes características óseas métricas y cromáticas de las personas mayores de 21 años en 11 diferentes partes del cuerpo. En esa época Bertillón publicó una tesis sobre el retrato hablado. Desde 1884, Bertillón tomó fotografías de los lugares de los hechos con todos sus indicios. Fue en 1886, cuando Alan Pinkerton, puso en práctica la fotografía criminal para reconocer a los delincuentes. En Londres, Sir Francis Galton, en 1885 instaló los fundamentos para la solución del problema, que representaba hacer una clasificación de las impresiones dactilares."[10]

En 1888, el inglés Henri Faulds en Tokio, Japón, contribuyo a la dactiloscopia ya que logro precisar los tipos arco, presilla y verticilo en los dibujos papilares de yemas de los dedos.

---

[8] **Ibíd.,** Pág. 10
[9] http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm; **Ob. Cit.** (14 de septiembre de 2013)
[10] Montiel Sosa, Juventino. **Ob. Cit.,** Pág. 10

"En agosto de 1891, en Argentina, Jaun Vucetich, inaugura la oficina de identificación y utiliza la antropometría y las huellas digitales de ambas manos y crea así la ficha decadactilar. Lo anterior permite establecer que las investigaciones policíacas se empezaban a guiar científicamente, pero con un porcentaje considerable de empirismo, donde se usaba la intuición y el sentido común y lógicamente no se obtenían resultados muy satisfactorios. Pero todos estas investigaciones y pesquisas empíricas, adquirieron u nombre propio que les dio el más ilustre y distinguido criminalista de todos los tiempos, el Doctor en derecho Hanns Gross, denominándole Criminalística, en Graz, Austria. En 1892 dada a conocer mediante su obra conocida con el nombre de: Manual del Juez, todos los Sistemas de Criminalística".[11]

"El Doctor Hanns Gross nació en Graz Austria en 1847, fue juez de Instrucción en Stejermark y Profesor en Derecho Penal en la Universidad de Graz, y por primera vez fue quien se refirió a los métodos de investigación criminal como Criminalística. La elaboración del Manual del Juez, le tomo veinte años de experiencia e intensos trabajos, en donde hizo orientaciones que debe reconocer la instrucción de una averiguación para aplicación de la técnica del interrogatorio, el levantamiento de planos y diagramas, utilización de los peritos, la interpretación de escrituras, conocimiento de los medios de comunicación entre los participantes de un mismo delito para el reconocimiento de las lesiones, etcétera, siendo en general un manual útil para los jueces en el esclarecimiento de cualquier caso penal".[12]

---

[11] **Ibid.,** Pág. 10
[12] **Ibíd.,** Pág. 10

"El contenido científico del Manual del Juez, se desprende que el Doctor Hanns Gross, en su época constituyo a la Criminalística con las siguientes materias: antropometría, argot criminal, contabilidad, criptografía, dibujo forense, documentoscopia, explosivos, fotografía, grafología, hechos de transito ferroviario, hematología, incendios, medicina legal, química legal e interrogatorio".[13]

"En 1896, Juan Vucetich logró que la policía de la provincia de Buenos Aires (en la ciudad de La Plata), Argentina, dejara de utilizar el método antropométrico de Bertillón y redujo a cuatro los tipos fundamentales de Dactiloscopia, determinados por la presencia o ausencia de los deltas. Ottrolenghi y Alongi, en 1899 fundaron una revista llamada Polizia Scientifica. Lombroso, Ferri y Alongi solicitaron una policía judicial científica en Italia".[14]

1.2. Definición

De acuerdo con el autor Gisbert citado por Montiel, Castellanos y Ceballos como: "una disciplina científica que estudia los indicios dejados en lugar del delito, con el propósito de descubrir la identidad del criminal y las circunstancia que concurrieron en el hecho delictuoso."[15]

---

[13] http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm; **Ob. cit.** (14 de septiembre de 2013)
[14] Montiel Sosa, Juventino. **Ob. Cit.,** Pág. 10
[15] **Ibíd.,** Pág. 10

"Desde un punto de vista amplio, mencionan los anteriores autores se puede considerar como el conjunto de procedimientos aplicables a la investigación y el estudio de un crimen para llegar a sus pruebas".[16]

"En un sentido más restringido se define a la Criminalística como la disciplina que mediante la aplicación de los principios de las ciencias naturales y sus técnicas tienen como objeto el reconocimiento, la identificación e individualización de las evidencias físicas o materiales con el fin de determinar si un hecho es delito, cómo se cometió y quién lo cometió".[17]

Castellanos y Ceballos mencionan que "tanto en el sentido amplio como en el restringido la Criminalística está íntimamente ligada con el fenómeno crimen y tiene como base el hecho de que el criminal deja huellas en el lugar." [18]

La evaluación y la obtención de información son las tareas principales de las investigaciones sin importar su propósito final. "El proceso de investigación se debe considerar en términos del obtenido y no de la evidencia, esta evidencia puede ser física o indiciaria material. Gran parte de la información que se consigue no es aceptable desde el punto de vista legal, sin embargo, los rumores, informes confidenciales y similares son de gran valor ya que indican el modo de conocer la evidencia aceptable".[19]

---

[16] **Ibíd.,** Pág. 10
[17] **Ibíd.,** Pág. 10
[18] **Ibíd.,** Pág. 10
[19] **Ibíd.,** Pág. 10

También se le define como "la ciencia que estudia los indicios encontrados en el lugar de los hechos, con el fin de identificar al delincuente, determinar las circunstancias en que se produjo el hecho delictivo y establecer las relaciones de participación de los individuos y factores que intervinieron en el crimen. Parte de la base de que el criminal, por muy astuto que sea, siempre deja en el lugar algún elemento, biológico o no, que delata su presencia. Encontrar y analizar esos indicios es el objetivo de la Criminalística."[20]

Los autores José Carlos Fuentes Rocañin; José Cabrera Forneiro; Carlos Fuertes Iglesias en su "Manual de Ciencias Forenses", define a la Criminalística como: "...la profesión y disciplina científica dirigida al reconocimiento, individualización y evaluación de la evidencia física, mediante la aplicación de diversas ciencias a las cuestiones legales. En el área de la investigación criminal, la ciencia multidisciplinaria denominada criminalística ha emergido con fuerza e impacto en prácticamente todos los elementos del sistema judicial. Esta ciencia puede suministrar información objetiva, de otra manera inalcanzable para el investigador y para el sistema judicial, a través del examen de la evidencia física." [21]

El criminalista debe observar, describir, plantear el problema, hipotetizar, experimentar y obtener un resultado convertido en teoría, principio general o en un elemento útil para el área en que trabaja, según los anteriores autores. El estudio y análisis de los indicios facilitan el conocimiento para establecer la forma y mecanismos de los hechos con todos sus fenómenos. El criminalista estudia desde el inicio de la primera maniobra

---

[20] Forneiro, José Cabrera y Carlos Fuertes Rocañin, Calixto Plumed Moreno, **Enfermería Legal.** Pág. 15
[21] **Ibíd.,** Pág. 15

hasta el último movimiento que se puso en juego para realizar el acto investigado, incluyéndose las formas de uso de los instrumentos u objetos de ejecución y el registro de sus manifestaciones, así como las posiciones y situaciones de los participantes, movimientos, manipulación y desplazamiento de cuerpos y objetos efectuados durante la comisión del hecho.

Además, mencionan los autores ya citados, que dicha ciencia estudia una extensa variedad de agentes mecánicos, químicos, físicos y biológicos, y toda la gran variedad de evidencias materiales. Su análisis identificativo, cuantitativo, cualitativo y comparativo, necesitará de metodología, tecnología y conocimientos universales de las disciplinas científicas que constituyen la criminalística general, como son la balística forense, química y biología forense, antropología, psicología, documentología, dactiloscopia, fotografía, planimetría, etcétera.

El agente de la autoridad o el investigador que llega al lugar de los hechos debe ser un experto recolector de evidencias, dado que su función es de vital importancia y va más allá de lo que comúnmente se cree. De su actividad científica, observadora y creadora en el escenario del suceso depende en gran parte el funcionamiento de casi todas las secciones del laboratorio de criminalística.

Dentro de sus múltiples actividades deben saber solicitar con propiedad los estudios y análisis de las evidencias físicas, de acuerdo con las circunstancias del hecho que se investiga. Asimismo deben conocer las técnicas forenses que se aplican en el laboratorio y dentro de estos requisitos destaca con especial significación, el

conocimiento necesario para el resguardo, la custodia y el almacenaje que posibilite la conservación de la evidencia hasta su análisis en los respectivos laboratorios.

La Criminalística, auxilia a cualquier rama del derecho general y a cualquier institución del Estado; "...cuenta con objetivos perfectamente definidos, con principios científicamente establecidos y prácticamente comprobados. Asimismo, ha creado una metodología propia de acuerdo a sus actividades, a través del método científico para formular sus teorías, leyes o principios y para razonarlos deductivamente mediante las proposiciones del silogismo universal."[22]

1.3. Características

Se extiende a tres áreas características:

1) "La búsqueda de los indicios;

2) Transformación de estos en prueba consecuencia de su objetivo; y,

3) Demostrar la culpabilidad o inocencia de un sujeto determinado".[23]

1.4. Finalidad

Los autores Castellanos y Ceballos mencionan cumple con una triple finalidad:

A. "Auxilio de inmediato, con asesoría en el lugar de los hechos, a la policía judicial y al agente de la fiscalía, a fin de tomar nuevas decisiones de acción para la consecución de las investigaciones.

---

[22] **Ibíd.,** Pág. 18

[23] http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm; **Ob. Cit.,** (14 de septiembre de 2013)

B. Emite dictámenes periciales en cualquiera de sus disciplinas científicas, para auxiliar a los órganos investigadores y jurisdiccionales, cuyos elementos pueden ser útiles para el ejercicio o desistimiento de la acción penal o para tomar las resoluciones judiciales respectivas.

C. Participa en diligencias ministeriales y judiciales, tales como inspecciones, (...) reconstrucciones de hechos y juntas de peritos e interviene con terceros peritos de discordia a efecto de opinar parcialmente sobre caso concreto".[24]

1.5. Instituto Nacional de Ciencias Forenses (INACIF)

El Instituto Nacional de Ciencias Forenses de Guatemala -INACIF- es creado con el Decreto 32-2006 del Congreso de la República de Guatemala, del ocho de septiembre de dos mil seis, como resultado de la necesidad de contar con medios de prueba válidos y fehacientes en los procesos judiciales. Cuenta con la cooperación de expertos y peritos en ciencias forenses que aplican los avances tecnológicos, metodológicos y científicos de la medicina legal y criminalística, como elementos esenciales en la investigación criminal y de cualquier otra naturaleza.

El Presidente del Organismo Judicial y de la Corte Suprema de Justicia, juramenta al director del Instituto Nacional de Ciencias Forenses de Guatemala.

"INACIF inicia sus funciones el día 19 de julio de 2007, y nace como institución auxiliar de la administración de justicia, con autonomía funcional, personalidad jurídica,

[24] **Ibíd**

patrimonio propio y con toda la responsabilidad en materia de peritajes técnico-científicos."[25]

El Instituto Nacional de Ciencias Forense, es una entidad independiente, técnica científica con autonomía legal para su funcionamiento que coadyuva al sistema de justicia en Guatemala, en la resolución de casos concretos mediante la utilización de métodos científicos multidisciplinarios, que a través de dictámenes produce prueba para la resolución de hechos ilícitos.

1.5.1. Funciones

El Artículo 29 del Decreto 32-2006 menciona que el INACIF suministrará sus servicios a requerimiento o solicitud de:

a) Los jueces o tribunales competentes en materia penal;

b) Los auxiliares y agentes fiscales del Ministerio Público;

c) Los jueces competentes de otras ramas de la administración de justicia;

d) El Instituto de la Defensa Pública Penal, la defensa técnica privada y las partes procesales en el ramo penal, por medio del Ministerio Público o el órgano jurisdiccional competente;

e) La Policía Nacional Civil en el desarrollo de investigaciones preliminares en casos urgentes, dando cuenta inmediatamente al Ministerio Público quien también deberá recibir el resultado de las mismas para dirigir la investigación correspondiente. Por ningún motivo podrá la Policía Nacional Civil, solicitar en forma directa informes o

[25] http://www.inacif.gob.gt/, (13 de diciembre de 2013)

peritajes sobre evidencias obtenidas en allanamientos, aprehensiones, detenciones o secuestros judiciales; y,

f) Las personas o entidades a quienes se les encomiende la investigación en los procedimientos especiales de averiguación.

1.5.2. Principios aplicables a la función del Instituto

Los principios aplicables a la función del INACIF los regula el Artículo cuatro del Decreto número 32-2006, del Congreso de la República describiéndolos de la siguiente manera:

A) Objetividad

En el ejercicio de sus funciones mantendrá objetividad e imparcialidad y observará el más escrupuloso respeto y acatamiento a la Constitución Política y Leyes de la República de Guatemala, y en lo atinente a los tratados y convenios internacionales reconocidos y ratificados por Guatemala.

B) Profesionalismo

Sujetará sus actuaciones a los más altos niveles de rigor técnico, científico y ético, teniendo como metas la eficiencia y la efectividad de aquellas.

C) Respeto a la dignidad humana

Respetará la dignidad inherente al ser humano, cumpliendo, sin discriminación ni privilegios, con la aportación de estudios y dictámenes objetivos e imparciales.

D) Unidad y concentración

El INACIF sistematizará y clasificará toda la información que procese, facilitando la consulta de la misma a las personas interesadas.

E) Coordinación interinstitucional

Los organismos e instituciones del Estado deberán cooperar con el INACIF, cuando éste lo requiera para el cumplimiento de los fines que le asigna la presente Ley.

F) Publicidad y transparencia

Los procedimientos y técnicas periciales que se apliquen serán sistematizadas y ordenadas en protocolos o manuales, los cuales serán públicos y accesibles para los interesados, debiendo realizar actualizaciones periódicas.[26]

G) Actualización técnica

Incorporará, con base a sus posibilidades económicas, las innovaciones tecnológicas y científicas para mejorar sus actuaciones y actualización para su personal técnico.

H) Gratuidad del servicio

"Los servicios prestados por el INACIF en materia penal serán gratuitos, sin perjuicio de la condena en costas que establezca el órgano jurisdiccional. Además podrá prestar servicios en otros procesos judiciales, notariales, administrativos o arbitrales mediante el previo pago de honorarios, conforme el arancel que para el efecto se apruebe. Podrá

[26] **Ibíd**

concederse exoneración de pago de honorarios en los casos señalados en el reglamento."[27]

1.6. Métodos de investigación criminalística

Es importante conocer cuáles son los servicios que actualmente presta el Instituto Nacional de Ciencias Forenses para demostrar que actualmente no cuenta con un método o bien un laboratorio para la investigación de delitos informáticos, las normas que utiliza el INACIF, para el desarrollo de la investigación a través de las técnicas criminológicas están basados en los siguientes:

1.6.1. Clínica forense

Efectúa pericias relacionadas con evaluaciones médicas a personas vivas,

a) Dictamina sobre lesiones personales.
b) Dictamina sobre embriaguez.
c) Establece edad cronológica.
d) Determina responsabilidad profesional.
e) Determina salud física y mental.

1.6.2. Odontología forense

A través de la odontología establece:

a) Lesiones físicas en cavidad oral.
b) Dictamina edad cronológica

[27] **Ibíd**

c) Realiza carta dental en identificación de personas o cadáveres no identificados o de dudosa identificación.

1.6.3. Patología forense

Realiza necropsias médico-legales, para establecer la causa de muerte y circunstancia relacionadas y ha cadáveres exhumados por autoridad competente.

1.6.4. Antropología forense

Realiza análisis e interpretación de restos óseos con fines de:

a) Identificación;

b) Restauración;

c) Reconstrucción cráneo facial; y

d) Análisis arqueológico de restos para determinar edad.

1.6.5. Psiquiatría y psicología

"Emite dictámenes en relación con el estado mental de personas involucradas en procesos ilícitos de cualquier índole".[28] Así como la secuela que un hecho pudo causar en víctimas de distintas agresiones.

---

[28] **Ibíd**

1.6.6. Dactiloscopia forense

Laboratorio encargado de realizar:

a) "Identificación de cadáveres XX a través del cotejo de las fichas necrodactilares tomadas en su momento, con los registros dactilares en documentos aportados por la Fiscalía.
b) Revelación de huellas latentes en diferentes elementos.
c) Realización reseñas dactilares y necrodactilares, a partir de recuperación y tratamiento de pulpejo, en cadáveres quemados o en avanzado estado de descomposición.
d) Revelación fragmentos de huellas latentes o visibles y determina su utilidad.
e) Realización de Cotejo de fragmentos dactilares útiles, con impresiones dactilares proporcionadas por el ente investigador.
f) Comparación de impresiones dactilares que obran en documentos de identificación, -sospechosos de ser alterados-, con impresiones dactilares indubitadas o que sean proporcionadas por archivos criminales o civiles a petición de autoridad competente." [29]

1.6.7. Fisicoquímica forense

a) "Análisis comparativo de pinturas y rastros de pintura.
b) Identificación y análisis comparativo de fibras textiles.
c) Análisis instrumental por absorción atómica, técnica para determinar la concentración de un elemento metálico determinado en una muestra.

[29] **Ibíd**

d) Análisis para la identificación de combustible.

e) Análisis de acelerantes en residuos de incendio.

f) Análisis comparativos entre elementos materia de prueba.

g) Análisis de plagicidad, herbicida, raticidas o tóxicos en aguas, alimentos y otros indicios de origen no biológico (ropa, contenedores, etcétera).

h) Otros estudios químicos específicos."[30]

1.6.8. Sustancias controladas

Otro de los métodos de investigación criminalística es el de sustancias controladas el cual consiste en: "análisis de material vegetal sospechoso de ser marihuana o amapola; de sustancias que producen dependencias psíquicas o físicas y sometidas a control por la ley; sustancias sometidas a control, por el Ministerio de Salud Pública y Asistencia Social, a través del Departamento de regulación y control de medicamentos y productos afines". [31] Finalmente de sustancias precursoras, sólidas y líquidos, que intervienen en el procesamiento de estupefacientes que son sometidos a control por la ley y otras normativas.

1.6.9. Toxicología

Este servicio prestado por el Instituto Nacional de Ciencias Forenses en Guatemala, realiza: "análisis sobre material orgánico: tejidos, fluidos tomados de personas vivas o

[30] **Ibíd**
[31] **Ibíd**

cadáveres; con el fin de determinar la presencia de sustancias, que pudieran causar daño o la muerte."[32]

1.6.10. Documentoscopía

El laboratorio de documentoscopia del Instituto Nacional de Ciencias Forenses, realiza análisis y estudios de los siguientes documentos:

a) "Manuscritos para establecer autenticidad o falsedad.
b) Cheques, papel moneda, billetes de loterías, sellos fiscales o postales, etiquetas, pasaportes, cédulas de ciudadanía, tarjetas de crédito, de vehículos, carnés personales o cualquier otro documento con el fin de establecer si son auténticos o falsos.
c) Elementos de reproducción gráfica empleados en la fabricación de documentos.
d) Textos mecanográficos y sistemas de impresión, para determinar las características de clase como: tipo de máquina, impresora o impresión y los aspectos de individualidad que permitan establecer la fuente impresora en que se elaboró el documento.
e) Cotejo de impresiones con el fin de determinar si provienen de una misma matriz o no. Estudio de alteración de documentos por supresión o adición de contenido.
f) Papel carbón, con el fin de establecer el contenido impreso a través de él.
g) Estudios de papeles en blanco, para revelar escritos latentes, dejados por la huella de un elemento escritor." [33]

---

[32] **Ibíd**
[33] **Ibíd**

1.6.11. Identificación de vehículos

Este laboratorio es el encargado de "determinar alteraciones en identificaciones de serie, chasis, motor de vehículos. Ubicación en números confidenciales en vehículos que por su naturaleza y marca lo poseen".[34]

1.6.12. Balística

a) El laboratorio de balística realiza:
b) Dictámenes periciales relacionados con balística interior y exterior.
c) Estudio de armas, proyectiles, vainas, cartuchos, perdigones, postas, pistones de potencia, esquirlas y fragmentos de proyectil.
d) Revelado de números seriales de armas de fuego.
e) Cotejo de lesiones y microlesiones en proyectiles y casquillos (dubitados, indubitados a fin de establecer autenticidad).
f) Determinación de distancias de disparo, sobre prendas de vestir portadas por la Víctima. Determinación de orificios de entra y salida en prendas de vestir.[35]

1.7. Métodos que utiliza actualmente el Instituto Nacional de Ciencias Forenses, para investigar los delitos cibernéticos

El actual Director del Instituto Nacional de Ciencias Forenses, (INACIF), en abril del año 2012, comento a un medio de comunicación de prensa escrita, que: "...uno de sus proyectos a la vista es la creación de laboratorios de informática forense, ya que la

---

[34] Ibíd
[35] Ibíd

institución no cuenta con ello y que el portafolio de servicios son los mínimos: medicina forense, clínica forense, toxicología, balística, documentoscopía, grafología, sustancias controladas, trayectoria y vehículos. Estaba por implementarse el laboratorio de lingüística y acústica."[36]

En noviembre de ese mismo año el director comento que: "...el presupuesto asignado para el 2013 no es suficiente para invertir y poner al servicio los laboratorios que hacen falta entre ellos, informática forense..."[37] Por lo que actualmente en su guía de servicios todavía no está implementado dicho laboratorio.

Asimismo, al momento de realizar una comparación en publicaciones oficiales de los servicios de criminalística que presta el Instituto Nacional de Ciencias Forenses hasta el año 2014, se puede verificar que la propuesta del Director no se ha concretado; demostrándose, que actualmente el instituto no cuenta con un laboratorio de informática forense, que permita el examen de evidencia en casos de robos cometidos a través del uso de comunicaciones informáticas; por lo tanto, la seguridad de la banca electrónica es vulnerable y solamente está a merced de la seguridad que presta las entidades bancarias.

[36] http://www.elperiodico.com.gt/es/20121104/pais/220128, (22 de enero de 2014)
[37] **Ibíd**

CAPÍTULO II

2. Casos de hechos ilícitos cometidos en la banca electrónica en la República de Guatemala

En Guatemala han ido en aumento los delitos cometidos a través de la utilización de la Internet, estos son producto del conocimiento especializado que poseen algunas personas para manipular información y obtener ganancias ilícitas de ello. Uno de estos hechos ilícitos son los fraudes a través de la banca electrónica, para poder debitar de las cuentas bancarias de los cuentahabientes de bancos del sistema cantidades de dinero a favor del delincuente.

"El ámbito espacial en los delitos tecnológicos es sumamente importante, en especial por las múltiples formas de comunicación que establece Internet; al respecto el Código Penal establece el principio al territorio de Guatemala: Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción, (Artículo 4). El problema en el ambiente de las Tecnologías de la Información y la Comunicación (TIC); es que la comunicación y relaciones no son solo de carácter nacional, también son internacionales, es decir fuera de las fronteras de Guatemala y por ende algunos hechos ilícitos son cometidos en un lugar distinto al territorio de Guatemala (en el ciberespacio)".[38]

[38] Barrios Osorio, Omar Ricardo. **Introducción de las nuevas tecnologías en el Derecho.** Pág. 147

Este tipo de hecho también pertenece a un nuevo hecho ilícito moderno que el autor Barrios Osorio, describe: "...los términos ciberdelitos, delitos informáticos, delitos electrónicos, delitos cibernéticos, computer crime; en principio pueden considerarse como sinónimos pero existen diferencias las cuales parten de determinar las acciones que estos conceptos describen como delitos".[39]

En virtud de lo anterior y antes de hacer referencia a los casos de hechos ilícitos cometidos en la banca electrónica en Guatemala es necesario conocer y comprender conceptos generales del origen, definición, clases y elementos de los delitos informáticos.

2.1. Breve reseña histórica

Los antecedentes históricos de estos delitos tienen un origen muy cercano, la creación de la computadora y el sistema de conexión mundial a través de la Internet, permitieron nuevas formas de realizar delitos; aunque al final su consecuencia sea la misma (en caso de robos a través de la banca electrónica); el modo de operar para llegar al fin ha sido realmente innovador.

Es por ello que "los avances tecnológicos y dentro de estos los de orden informático determinan imperativamente necesidades de orden social, que impulsan la obligación de tutela estatal a través de la reforma o creación de leyes específicas".[40]

"El Derecho Penal no constituye la excepción, y se ha visto en la necesidad de normar ámbitos de protección a bienes jurídicos tutelados que anteriormente no existían o no

[39] Barrios Osorio.**Derecho e informática, aspectos fundamentales.** Pág. 377
[40] Noriega Salazar, Hans Aarón. **Delitos Informáticos**. Pág. 21

se consideraban merecedores de defensa estatal. En ese sentido se puede ubicar cronológicamente el siglo veinte, como el origen y evolución de los delitos de carácter informático".[41]

"Los ataques al programa o sistema operativo de un computador pueden ser considerados como las primeras conductas merecedoras de regulación y sanción de carácter penal".[42]

"Debe reconocerse que uno de las primeras acciones de este tipo se da a manera de juego, documentándose en el año de 1959 el caso de Robert Thomas Morris, Douglas McIlory y Víctor Vysottsky, tres programadores de la compañía Bell Computer quienes en una competencia idearon un sistema al que denominaron Corewar, consistiendo este en crear programas que paulatinamente disminuían la memoria de la computadora, ganando el mismo quien lograse la eliminación total de ésta".[43]

"Uno de los primeros virus que afecta los sistemas informáticos aparece en el año de 1972, y se le denominó Creeper (enredadera en idioma inglés), que afectó a las computadoras de la compañía IBM e hizo necesaria la aparición del primer antivirus conocido como cegadora".[44]

"Posteriormente en el año 1980 el Arpanet, (sistema de comunicación vía computadoras usado por el departamento de defensa de los Estados Unidos y

---

[41] **Ibíd.,** Pág. 21
[42] **Ibíd.,** Pág. 21
[43] **Ibíd.,** Pág. 21
[44] **Ibíd.,** Pág. 21

precursor de Internet), experimentó ataques a través de un virus informático que necesitó de tres días de trabajo para eliminarlo".[45]

"En el plano internacional al año de 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio para aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas de computadoras. Fruto de ello en el año 1986, se publica el documento titulado: Delitos de Informática análisis de la Normativa Jurídica en el que se recopilan detalles de normas penales vigentes y propuestas de reforma de legislación en sus países miembros así como las conductas que era necesario sancionar penalmente, en lo que se denominó lista mínima".[46]

Con respecto a la legislación guatemalteca, es en el año de 1996 que se regula los delitos informáticos entre los que se puede mencionar la destrucción de registros informáticos, alteración de programas y la reproducción de instrucciones o programas de computación entre otros.[47]

2.2. Definición

Según el autor Barrios Osorio define "...de forma básica como delito informático las acciones prohibidas por la ley, cometidas en contra de uno o varios de los elementos que integran un sistema de información o los derechos que del mismo se deriven (protección de datos, intimidad o privacidad, derechos de autor)".[48]

---

[45] **Ibíd.,** Pág. 22
[46] **Ibíd.,** Pág. 22
[47] **Ibíd.,** Pág. 22
[48] Barrios Osorio. **Ob. Cit.**, Pág. 377

Gabriel Andrés Cámpoli citado por Barrios Osorio define como Delitos Informáticos Electrónicos "en los cuales el autor produce un daño o intromisión no autorizada en aparatos electrónicos ajenos... pero que poseen como bien jurídico tutelado en forma específica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios".[49]

La informática es definida en el Diccionario de la Real Academia de la Lengua Española como "el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".[50]

Tiedemann señala: "Con la expresión criminalidad mediante computadoras se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente dañosos y por eso penalizables en el futuro) realizados con el empleo de un equipo automático de procesamiento de datos".[51]

La Organización de las Naciones Unidas al referirse a la delincuencia informática lo hace de la siguiente manera: "A menudo, se le considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos".[52]

---

[49] **Ibíd** Pág. 377
[50] http://www.rae.es/ (22 de febrero de 2014)
[51] Noriega Salazar, Hans Aarón. **Ob. Cit.,** Pág. 21
[52] http://www.onu.org.gt/, (22 de febrero de 2014)

"Los delitos contra bienes informáticos (TIC) y los delitos cometidos por medio de las Tecnologías de la información y la comunicación son aquellos que atentan contra bienes creados por la Informática y las Tecnologías de la información y la comunicación; en sentido amplio se consideran a los delitos informáticos los cometidos contra los bienes de origen informático así como aquellos en los que se haga uso indebido de los sistemas de información y que se encuentran regulados en otros capítulos del Código Penal e inclusive algunos que no están regulados pero que pueden ser considerados delito. (spam, fraude informático, subasta ilícitas, publicaciones obscenas en línea)".[53]

La comisión de hechos ilícitos realizados a la banca electrónica tienen como ámbito de actuación la *t*ecnología de la información y de comunicación, dentro del ciberespacio, esto implica que realizan ataques con la intencionalidad de daño en la intromisión o acceso a bases de datos o archivos que las mismas contengan, o bien la utilización de aparatos tecnológico y de comunicación con información personal para su acceso para la comisión de los delitos, para obtener una ganancia económica ilícita; esto demuestra que pertenecen al ámbito de los delitos informáticos.

2.3. La responsabilidad en la comisión de un delito

"La persona que participa en la comisión de un hecho ilícito debe de asumir las consecuencias de lo realizado contra Derecho; la responsabilidad que asume el sujeto activo del delito son: la responsabilidad penal y civil".[54]

---

[53] Barrios Osorio. **Ob. Cit.**, Pág. 378
[54] **Ibíd.,** Pág. 378

"La responsabilidad penal se deduce a través de ejercitar la acción penal en contra del sujeto activo por el ente acusador del Estado que es el Ministerio Público o en su caso el querellante y que busca en representación de la sociedad afectada, deducirle la responsabilidad penal al delincuente, para lo cual solicita al órgano jurisdiccional la aplicación de una pena u otra forma o mecanismo alternativo de solución al conflicto penal. La pena es la forma con la cual el estado rehabilita al delincuente y lo prepara para su reincorporación a la sociedad. En el caso de los delitos informáticos establecidos en el Código Penal vigente se contempla la pena de prisión y la pena de multa".[55]

"La responsabilidad civil comprende el resarcimiento económico que debe de realizar el responsable del hecho ilícito (imputado o condenado) o la persona que la ley determine (tercero civilmente demandado), a la víctima o agraviado".[56]

2.4. Clasificación de los delitos y las tecnologías de la información y la comunicación

"Para analizar cada uno de los delitos en cuanto al bien jurídico tutelado que éstos protegen es necesario describir un Sistema de Información y este es el conjunto de elementos que tiene por objeto procesar datos e información para facilitar la toma de decisiones o proporcionar un servicio".[57]

"Los elementos que compone ese sistema de información (automatizado) son: el hardware (equipo de computación), software (los programas de ordenador), usuarios

[55] **Ibíd.,** Pág. 378
[56] **Ibíd.,** Pág. 378
[57] **Ibíd.,** Pág. 378

(personas que accedan al sistema), información (el conjunto de datos) y documentación técnica (manuales y guías de utilización y referencia)".[58]

2.5. Bien jurídico tutelado

En el entendido que el bien jurídico tutelado lo "constituyen todos aquellos derechos, valores o atributos de la persona que el Estado encuentra merecedores de protección a través del Derecho Penal, se puede afirmar que en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro."[59]

"Por un lado las acciones que van dirigidas al sabotaje, el daño, la destrucción o pérdida de equipos de computación afectan, lesionan o ponen en peligro el bien jurídico patrimonio. ...Por otro lado, los delitos que se sirven o utilizan de un equipo informático para su realización pueden de igual manera afectar diversos bienes, como lo serían la indemnidad sexual (caso de la pornografía infantil)".[60]

Asimismo la reproducción no autorizada de libros, películas música, etc., afecta valores de propiedad intelectual acciones que tienen una motivación económica por lo que a su vez redundan en la afectación al bien jurídico patrimonial.

"Es por eso que al hablar de delitos informáticos es válida la afirmación que los mismos afectan una diversidad de bienes legalmente tutelados por lo que puede considerarse pluriofensivos".[61]

---

[58] **Ibíd.,** Pág. 378
[59] Noriega Salazar. **Ob. Cit.,** Pág. 22
[60] Barrios Osorio. **Ob. Cit.**, Pág. 379
[61] **Ibíd.,** Pág. 379

Respecto a los delitos realizados en la banca electrónica de los bancos del sistema, pueden considerarse que van dirigidos afectar el patrimonio de los cuentahabientes que depositan su dinero dentro de las entidades bancarias, por ende el bien jurídico tutelado es el patrimonio. Siendo una forma de hurto mediante la utilización de herramientas y conocimientos de sistemas informáticos para facilitar su acceso.

2.6. Los sujetos del delito

Los sujetos de los delitos informáticos son cometidos por personas ya sean individuales y físicas; el autor Barrios Osorio menciona que estos en la doctrina se clasifican como: sujeto activo y sujeto pasivo.

"El sujeto activo es la persona que incurre o realiza la prohibición que le ha establecido la ley. En el caso de los delitos que atentan contra los programas de ordenador, tienden a tener un alto grado de conocimiento y recursos en el área de informática y TIC en general, en virtud que estos delitos no pueden ser cometidos por cualquier persona. Siendo las más comunes: Hacker, Cracker, Pirata informático..."[62] por lo que son "...sujetos que violan o rompen los niveles de seguridad de acceso o de utilización de los programas".[63]

"El Hacker: Este término proviene del uso del vocablo del idioma inglés hack que traducido significa cortar, tajar, hachazo. La acción de cortar los niveles de seguridad

[62] Barrios Osorio. **Ob. Cit.**, Pág. 379
[63] **Ibíd.,** Pág. 379

de un sistema informático se denomina hacking. Al sujeto responsable se le llama hacker".[64]

El hacker es definido como"...una persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos"[65]. Esta acción de cortar los procedimientos de seguridad en doctrina se puede describir desde varios 'niveles' de gravedad. Al respecto Gabriel Cámpoli citado por Barrios Osorio los clasifica en: Intrusión simple, daño electrónico simple, intrusión agravada por la finalidad".[66]

"El primero denominado Intrusión Simple (hacking simple), es la acción consistente en el acceso no autorizado a un equipo informático ajeno una página web propiedad de un tercero, por cualquier medio, cuando el sujeto activo no produjere con ella ningún daño o fuere motivado por fines que puedan considerarse incluidos en otro tipo penal más grave, como tampoco produjere algún detrimento en derechos intelectuales del sujeto pasivo. // Este nivel de ilícito lo realiza el hacker, en los otros niveles se ha utilizando el término cracker".[67]

Otro de los sujetos que participan en los delitos informáticos es el Cracker este: "...término proviene del vocablo inglés crack que traducido significa romperse, restallido, grieta..."[68], o romper "...se utiliza para referirse a las personas

---

[64] **Ibíd.,** Pág. 379
[65] https://www.google.com.gt/search?q=hacker, (19 de junio de 2014)
[66] Barrios Osorio. **Ob. Cit.**, Pág. 379
[67] **Ibíd.,** Pág. 379
[68] **Ibíd.,** Pág. 379

que rompen algún sistema de seguridad. (...) pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío".[69]

"En este caso se encuentran los otros niveles descritos anteriormente. El segundo es el Daño Electrónico Simple (cracking), que es la acción en la cual el sujeto activo, luego de introducirse de forma no autorizada en equipo electrónico o página web ajena, produce algún detrimento patrimonial mediante el menoscabo de la integridad física o lógica de cualquier de ellos, sin más motivo que la producción misma del daño".[70]

"El tercer nivel denominado Intrusión agravada por la finalidad (Hacking económico o agravado) se define como la acción consistente en el acceso no autorizado a un equipo informático ajeno o una página web de propiedad de un tercero, por cualquier medio, cuando el sujeto activo lo hiciere a fin de obtener un beneficio económico de cualquier otro tipo para sí o un tercero".[71]

Otro sujeto del delito informático se encuentra los piratas informáticos, las acciones cometidas por ellos esta ligados a los delitos de propiedad intelectual y son definido como: "...quien adopta por negocio la reproducción, apropiación o acapararían y distribución, con fines lucrativos, y a gran escala, de distintos medios y contenidos (software, videos, música) de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador".[72]

---

[69] http://es.wikipedia.org/wiki/Cracker, (29 de junio de 2014)
[70] Barrios Osorio. **Ob. Cit.**, Pág. 380
[71] **Ibíd.,** Pág. 380
[72] http://web.archive.org/web/20050313113824/http://www.persystems.net/sosvirus/general/hackers.htm, (29 de junio de 2014)

"...por la influencia que tienen en el ambiente informático las grandes empresas de computación, en especial las titulares de los programas de ordenador más comerciales, se acuño el concepto pirata informático..."// "Los términos descritos anteriormente se utilizan para el sujeto que ejecuta la acción de forma directa, pero es importante establecer que pueden existir otra clase de responsables como el autor intelectual. El ejemplo surge cuando un sujeto que no tiene el conocimiento en informática encarga a un hacker para cometer el hecho ilícito". [73]

El sujeto pasivo por ser el titular del bien jurídico tutelado y quien es el lesionado por el hecho ilícito cometido, dentro de los delitos informáticos, según Barrios Osorio, afecta a: "...a) La sociedad, y; b) la víctima o agraviado. Las persona jurídicas (colectivas son las principales víctimas de estos, delitos, en especial aquellas consideradas en doctrina como sociedades especiales (bancos, financieras, aseguradores, casas emisoras de tarjetas de crédito y débito), en virtud que estas manejan un considerable volumen de información y datos, estos últimos representativos de valores o moneda administrada de forma electrónica".[74]

"Además se encuentran afectadas por los delitos informáticos las personas que se dedican específicamente a prestar servicios relacionados con las TIC como proveedores de Internet y sus aplicaciones (correo electrónico), servidores de información, portales, etcétera. Las personas individuales también sufren los embates de delitos relacionados con sus sistemas informáticos, siendo el más común el delito de introducir programas destructivos (virus) en sus sistemas, el acceder a su información

[73] **Ibíd.,** Pág. 380
[74] **Ibíd.,** Pág. 380

(hacking). La administración tributaria también es un sujeto pasivo, en virtud que se alteran los programas de ordenador de los sistemas de control tributario de los obligados o responsables (contribuyentes) para cometer delitos relacionados con el incumplimiento de los tributos (Manipulación de la información)".[75]

2.7. Clases de delitos informáticos

La clasificación que a continuación se describirá es según el bien jurídico afectado, iniciando con un la argumentación siguiente: "Al definir los delitos informáticos se hacía referencia a acciones antijurídicas con una finalidad que podría ser el ataque, daño o acceso no autorizado a un aparato o sistema de computadoras o sus programas, o bien se sirve de éstas como medio operativo para realizar actos ilícitos; además de acuerdo a la real afectación al bien jurídico tutelado estos pueden ser dirigidos a vulnerar el patrimonio, propiedad intelectual o bien la privacidad o indemnidad de las personas. Estas reflexiones sirven de base para proponer por parte del autor (Noriega Salazar), la siguiente clasificación de los delitos informáticos, distinguiéndose entonces dos tipos a saber: // a) Delitos Informáticos contra el patrimonio y la propiedad intelectual. b) Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual".[76]

Como podrá corroborarse en títulos siguientes, los delitos cometidos a la banca electrónica, al sistema bancario guatemalteco su bien jurídico tutelado está dirigido a la protección al patrimonio, en el caso de piratas informáticos que también cometen

---

[75] **Ibíd.,** Pág. 381
[76] Noriega Salazar. **Ob. Cit.,** Pág. 22

delitos en los sistemas informáticos bancarios, crear programas que violentan la propiedad intelectual, además de vulnerar la privacidad de las personas.

Este delito está muy ligado al primer tipo de delitos en la clasificación anteriormente mencionada; sin embargo también tiene una relación parcial con el segundo, respecto a la privacidad e intimidad, en la obtención de datos confidenciales, sin embargo por ser un delito que su bien jurídico protegido es el patrimonio; la libertad e indemnidad sexuales no tienen relación alguna con la comisión del hecho delictivo.

2.8. Caso de phishing en banca electrónica

"El término phishing proviene de la palabra inglesa 'fishing', que significa pesca y hace alusión al intento de que los usuarios 'piquen el anzuelo' para dar información confidencial; se trata de un crimen cibernético por el cual los estafadores roban la información y las contraseñas de las cuentas bancarias o tarjetas de crédito de sus víctimas".[77]

"El estafador, conocido como phisher, se hace pasar por una empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, para luego redireccionarlo a un sitio web que simula ser el portal del banco".[78]

Se puede establecer que el delito de Phishing, es una serie de maniobras para engañar a los usuarios de la red, con ello lograr la obtención de datos que permitan el acceso a cuentas bancarias, números de tarjetas de crédito o debito y poder obtener una

[77] http://www.elperiodico.com.gt/es/20110628/economia/197413/, (23 de febrero de 2014)
[78] **Ibíd**

ganancia patrimonial ilícita; al respecto se ha impulsado información en diferentes medios, (ejemplo entidades bancarias), acerca del cuidado que el cuentahabiente debe tener con sus datos personales; siendo uno de los participes importantes en la lucha contra este delito.

Los usuarios del sistema bancario guatemalteco que han sido afectados por este delito se da cuando: "...a un cuentahabiente le vaciaron su cuenta por medio de la banca en la Red; cuando este revisó su estado de cuenta por medio de su computadora, un phisher copió su contraseña desde otra computadora".[79] Suplantando páginas de bancos para poder realizarlo.

Otro caso los describe "...Un asistente de gerencia de Banrural, afirmó que 'se trata de una técnica de estafa muy usada en el país y que la única forma de impedir estos fraudes es por medio de la prevención y la educación de los clientes".[80] Esta experiencia la obtuvo porque el mismo cliente llamó a la entidad bancaria para saber si la información enviada fue la correcta.

El gerente del Banco Industrial, expresa que: "la mejor manera de prevenir las estafas es informarle a los clientes que los bancos no requieren información por medio de correo electrónico. En la página de la Internet se colocan ventanas indicándoles a los clientes que no den información. Este problema es muy difícil de resolver, debido a que son bandas internacionales, ya que para la tecnología no existen fronteras. // El representante de Banrural explicó "...que el sistema bancario nacional recibe un

[79] **Ibíd**
[80] **Ibíd**

servicio de protección que bloquea las páginas de phishing. En este sentido no hay competencia y se ataca en forma conjunta; para prevenir este problema la banca guatemalteca es una sola".[81]

En cuanto a las entidades estatales: "fuentes del Ministerio Público reconocieron que existen varios casos de estafas por phishing que están siendo investigadas. Unos de los problemas es que no está tipificado el fraude cibernético en la legislación nacional y que no se cuenta con la tecnología para dar con los estafadores. A pesar de que en el Congreso aún se discute una iniciativa de ley sobre el tema de delito cibernético, el Código Penal en su Artículo 274 reconoce violaciones a los Registros Prohibidos, Manipulación de Información y uso indebido de la misma, las cuales contemplan penas de 6 meses a 5 años de prisión así como multas monetarias".[82]

2.9. Casos de robo de identidad

El robo de datos personales para cometer hechos ilícitos, a través de la internet, también es un medio para cometer delitos dentro del sistema bancario guatemalteco; aunque no siempre es un debito a cuentas bancarias; siempre va ligado al fraude dentro de este tipo de entidad. Por lo que se observara a continuación de qué forma afecta la economía de los cuentahabientes con el uso de sistemas de información tecnológica, robo de datos y finalmente la forma de operar en conjunto.

Respecto a este delito se dice que: "algunas personas se apoderan de documentos como cédulas, pasaportes o licencias de conducir, y también perfiles en las redes

---

[81] **Ibíd**
[82] **Ibíd**

sociales. La mayoría de veces lo hacen para obtener beneficios económicos mediante estafas. // Otros se ven afectados de diferente manera: quienes les roban sus documentos personales los utilizan para obtener tarjetas de crédito y financiamientos en bancos. Gastan a placer y luego dejan a sus víctimas con una fuerte deuda. // Existen casos de usurpación de identidad en las redes sociales. Consiguen herramientas de hackeo o sustracción de cookies (información digital que queda grabada en las computadoras) y contraseñas".[83]

Respecto a casos realizados dentro del territorio guatemalteco: "se han dado casos de personas que emplean sniffers y keyloggers, programas que capturan los datos que circulan en internet y que graban las pulsaciones que se generan en un teclado. Es así como amenazan o sobornan, además de sustraer fuertes sumas de dinero al clonar tarjetas de crédito con los datos obtenidos".[84]

Otras de las formas de la comisión del hecho ilícito es: "el riesgo de conectarse a redes inalámbricas de restaurantes, hoteles o cafés. Un usuario podría estar conectado al mismo sistema y vigilar lo que otro hace en su computadora. Un administrador de redes con malas intenciones podría estar controlando, sin que nadie se dé cuenta, por medio de programas especiales. Hay herramientas que monitorean lo que alguien más escribe en los chats, en tiempo real".[85]

Una de las peculiaridades del robo de identidad con respecto a los demás casos, este es un delito que ha sido cometido antes de la existencia de la Internet, ya que con

---

[83] http://especiales.prensalibre.com/revistad/2012/04/22/reportajecentral.shtml, (02 de marzo de 2014)
[84] **Ibíd**
[85] **Ibíd**

anterioridad su comisión más frecuente era la usurpación del nombre de otro, ya sea con fines lucrativos o bien para dañar el honor de una persona, falsificando documentación original, por lo que la obtención y la utilización de los datos personales era más complejo. En la actualidad lo común es asociarlo con la obtención de datos por medios informáticos personales y luego utilizarla de forma ilegal, siendo en la mayoría de casos con un fin patrimonial que moral.

La adquisición de datos es mucho más fácil, que en el pasado, la digitalización y automatización de datos permite un constante movimiento de datos personales dentro de la red y una fuente constante para la proliferación de delitos; por ello es que existe diversidad de formas en su comisión.

La protección de los datos debe reforzarse aun mas, hoy en día la deducción de responsabilidades deber ir dirigida a varios actores dentro de la sociedad, no solo quien ha utilizado la información directamente, sino a entidades públicas y privadas, que no garantizan una protección adecuada; asimismo de forma preventiva, el cuidado de cada usuario debe tener con la información personal.

La legislación guatemalteca con relación a la comercialización de datos personales nada menciona al respecto, según Omar Barrios, Director de la Unidad de Derecho y Tecnología del Centro de Estudios de Derecho. Sigue manifestando el anterior autor que: "tal es el caso de algunas outsourcing, como agencias de empleo en línea. Estas recopilan información de la gente para mantener actualizadas sus bases de datos y luego, vendérselas a otras firmas que las comercializan, las cuales, a su vez, la

comparten con instituciones financieras, para evaluar el perfil de una persona que, por ejemplo, solicita crédito".[86]

En cuanto a la participación de personas jurídicas públicas y privadas describen expertos en la materia que "empresas como Informes en Red, Sociedad Anónima (Infornet) y Trans Union violan la Ley de Acceso a la Información Pública al vender datos personales sin que los afectados lo sepan y sin que hayan dado su consentimiento. // El secretario ejecutivo de la Comisión de Acceso a la Información de la Procuraduría de Derechos Humanos, afirmo que esas empresas manejan información pública, y por eso no infringen la ley."[87]

En el caso de la empresa Trans Union la información que maneja proviene de una concesión de servicio de digitalización que realizo al Registro Civil de la Municipalidad de Guatemala, durante el año 2002, por lo que no existe autorización de las personas que se encuentra dentro de su cartera de clientes.

En cuanto, a la protección legal que puede brindar la legislación guatemalteca actual; puede mencionarse como ejemplo la sentencia de la Corte de Constitucionalidad del "11 de octubre del 2006, (...) en el expediente 1356-2006, se examinó la sentencia que meses antes una persona había promovido contra Infornet. La Corte de Constitucionalidad reconoce el 'derecho a la intimidad' y el 'respeto a un ámbito de vida privada personal y familiar'. Prosigue en que la base de datos de la firma no tiene controles que permitan determinar la veracidad y actualización de su información, y que, por tanto, pueden causar la 'afectación del entorno personal, social o profesional',

[86] **Ibíd**
[87] **Ibíd**

y el consecuente 'agravio de los derechos a la intimidad y honor' de un individuo. // Al final del expediente, la Corte de Constitucionalidad le ordenó a esa empresa que excluyera de su base de datos toda la información del acusador".[88]

En relación a los delitos dentro de la banca electrónica, esta sentencia demuestra que es posible dentro del orden jurídico guatemalteco existente, evitar el uso inadecuado de datos personales, si bien es cierto estas empresas de crédito la realizan para ver el perfil financiero de la personas, es probable que la información sea vendida, robada o cedida para utilizar la identidad y causar un daño patrimonial en usuarios del e-banking; al no brindarle a su cartera de clientes la protección de datos personales que administran.

Los delitos establecidos que tienen cierta relación con el robo de identidades se encuentra tipificados dentro de los Artículos 274 "F", "D", del Código Penal, según el análisis siguiente pueden vincularse, sin embargo el vacío legal continua.

El Decreto Número 33-96 en el Artículo 18 adiciona el Artículo 274 "F" el cual establece: Artículo 274 "F". Uso de información. Se impondrá prisión de seis meses a dos años y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

El autor Barrios Osorio menciona que: "en este caso, la redacción del Artículo denota la confusión o el poco conocimiento que se tenía en el año 1996 sobre esta materia, en

---

[88] **Ibíd**

virtud que en un mismo Artículo se quieren regular dos situaciones diferentes. Se puede determinar que se protegen dos bienes jurídicos o derechos: los registros informáticos (en cuanto a su utilización no autorizada) y el acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos".[89]

La primera posición es el "...caso de los registros informáticos, la persona que crea una base de datos (lícita), dispone de quienes van a tener autorización para hacer uso de ellos. La utilización autorizada de los registros puede ser directa del computador que los tiene almacenados, en línea (red interna y externa), o pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas, incluso, un usuario autorizado para acceder al sistema, pero no para utilizar en forma distinta los registros informáticos. Cuando un sujeto sin la autorización del titular de ese registro informático hace uso de él, estaría incurriendo en el delito establecido",[90] generándole lucro o no.

Del análisis realizado por el Autor Barrios Osorio, puede observase que trata de desarticular cada elemento del delito, como bien lo señala, hay una confusión en la redacción; porque en esa época existía muy poco conocimiento sobre los delitos informáticos y que actualmente, se puede determinar con más claridad, razón por la cual se menciono en este apartado, esta opinión doctrinaria; de manera que permita encuadrar esta conducta con el robo de identidad, estando de acuerdo totalmente con la posición de dicho autor.

---

[89] Barrios Osorio. **Ob. Cit.**, Pág. 147
[90] **Ibíd.,** Pág. 147

La segunda posición es "cuando el acceso al sistema lo realiza una persona que no está autorizada, se encuadra esa acción a este delito. Es importante señalar que el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, incluso si no realiza ninguna acción con la información. Esto se conoce en doctrina como el delito de hacking".[91] Este es el proceso que se utiliza para conocer los limites de seguridad de un programa, con el fin de obtener un beneficio o comprobar inmunidad de un sistema.

A su vez; otro delito donde puede encuadrase el robo de información para cometer hechos ilícitos dentro de la banca electrónica lo establece el Decreto Número 33-96 en el Artículo 16 adiciona el Artículo 274 "D" el cual establece: Artículo 274 "D". Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

El autor Barrios Osorio describe que: "para poder definir el bien jurídico que protege el Artículo 274 "D" (la intimidad de la persona), es importante recordar las definiciones de datos personales y de intimidad, así como los derechos que resultan de ellos".[92]

Con respecto a los delitos tipificados dentro del Código Penal, uso de información autorizada, puede relacionarse con los delitos informáticos de robo de identidades en el sistema bancario, para la comisión de hechos ilícitos, en virtud de que los bancos del país poseen datos de sus clientes debidamente autorizados; que pueden ser desviados a otros sistemas o bien sus empleados realizar una extracción de los mismo; para

[91] **Ibíd.,** Pág. 149
[92] **Ibíd.,** Pág. 149

proveerle a otro la información, sin la debida autorización y con una finalidad lucrativa. En cuanto al otro delito contenido dentro de la legislación penal que es registros prohibidos, este tiene una vinculación con los robo dentro del e-banking, respecto a que la información proporcionada al banco debe ser categorizada como un registro que afecta la intimidad de la persona; por lo tanto la utilización de la misma debe tener mayores niveles de seguridad.

Es importante mencionar que a partir de la aprobación de la Ley de Acceso a la Información Pública, dio lugar a una nueva modalidad de acción constitucional esta denominada en habeas data, donde el Estado tiene el deber de proteger los datos personales de sus ciudadanos para evitar cualquier manipulación, usurpación, violación a la intimidad patrimonial de las personas.

En resumen, el robo de datos personales mediante medios informáticos requiere del acceso a una base de información y que mediante el uso de información confidencial, robada de varios recursos electrónicos, por ejemplo datos dentro de correos electrónico, facebook, etcétera; como ya se señalo con anterioridad, con esto acceder a sistemas regularmente de entidades bancarias; con un fin meramente lucrativo y en detrimento del patrimonio del titular de la información personal.

2.10. Caso de piratas informáticos

Este tipo de delito de los casos que ha afectado la banca electrónica en Guatemala, ya que el modo de operar es robar información confidencial a través de la creación de

programas que simulan un entidad oficial, lo que permite lograr el acceso a cuentas bancarias y de esta manera realizar acreditaciones o compras a su favor.

Para ilustrar de mejor manera este delito, proceso a indicar casos concretos, así como relatos de victimas y opiniones por parte del Ministerio Público.

En uno de los casos que se ha realizado por investigadores del Ministerio Público en Guatemala "...los piratas informáticos ingresan en bases de datos de usuarios de bancos y crean cuentas paralelas, y de esa manera verifican el estado financiero de cuentahabientes". // La Fiscalía indicó que la modalidad es reciente, y que consiste en plagiar datos de cuentahabientes y trasladarlos a su propia base. Cuando el usuario ingresa con su clave, ellos la pueden copiar. Además, tienen una alerta para cuando se depositan altas cantidades de dinero, y esas cuentas son las que mejor aprovechan".[93] Una víctima de este tipo de delitos expreso que cuando "...quiso verificar su saldo, y se sorprendió cuando observó que en cinco segundos efectuaron el mismo número de transacciones. Inmediatamente llamo al banco, pues el sistema le alertó acerca de una transacción internacional en dólares con su tarjeta de débito".// "En el sistema bancario bloquearon la cuenta de manera inmediata, y dos días después se presentó a una agencia para aclarar su situación y llenar formularios que posteriormente presentó en el Ministerio Público."[94]

En cuanto a "el Ministerio Público tiene un caso en juicio contra dos capturados en noviembre del 2010. El proceso se lleva en el Tribunal Primero de Sentencia Penal en Mixco, contra Salvador Alejandro Pineda Urbina y Heidy Mercedes Jordan Godínez.

[93] http://eticauvg.wordpress.com/2012/05/22/analisis-de-casos/, (04 de marzo de 2014)
[94] **Ibíd**

Ambos efectuaron varias transferencias por pagos y servicios por medio de cuentas de otras personas que oscilaban entre Q10 mil y Q90 mil. La investigación comenzó en el 2009, cuando tarjetahabientes recibían correos para actualización de datos. Varias personas recibieron correos falsos de páginas virtuales de entidades bancarias. En estas les solicitaban que de conformidad con la Ley de Lavado de Dinero y otros Activos debían confirmar sus datos".[95]

Posteriormente, "los clientes reportaron transferencias que nunca habían realizado. La Fiscalía cree que las cuentas desde donde copiaron las bases de datos fueron creadas en otros países. Se sospecha esto, pues las cuentas tienen terminaciones de otros países en las últimas letras, como España y Alemania. Ambos capturados no tenían antecedentes, pero por ese delito la Fiscalía los sindica de estafa propia en forma continuada, manipulación de la información en forma continuada y conspiración".[96]

[95] **Ibíd**
[96] **Ibíd**

CAPÍTULO III

3. Comparación del delito informático regulado en Guatemala y países de América Latina

La conducta que conlleva una acción u omisión que se ajusta a los presupuestos establecidos como delito o falta en un ordenamiento jurídico de orden penal, son consideradas acciones típicas.

Estas pueden ser cometidas de diversas formas siempre con el fin de dañar un bien jurídico tutelado por el Estado. A partir de ello en la actualidad legislaciones de todo el mundo han tenido que añadir otra figura delictiva que tiene como plataforma una ciencia tecnológica reciente, pero con gran crecimiento tanto en la utilización para el desarrollo y convivencia diaria, (transacciones monetaria, compras, compartir información, etc.), lográndolo a través de la informática.

Ahora bien "la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales. Los sistemas informáticos deben contar con la capacidad de cumplir tres tareas básicas: entrada (captación de la información), procesamiento y salida (transmisión de los resultados). El conjunto de estas tres tareas se conoce como algoritmo".[97]

"La informática reúne a muchas de las técnicas que el hombre ha desarrollado con el objetivo de potenciar sus capacidades de pensamiento, memoria y comunicación. Su área de aplicación no tiene límites: la informática se utiliza en la gestión de negocios,

[97] http://definicion.de/informatica/#ixzz2tWQKILCz, (03 de marzo de 2014)

en el almacenamiento de información, en el control de procesos, en las comunicaciones, en los transportes, en la medicina y en muchos otros sectores"...// también abarca "...los principales fundamentos de las ciencias de la computación, como la programación para el desarrollo de software, la arquitectura de las computadoras y del hardware, las redes como Internet y la inteligencia artificial. Incluso se aplica en varios temas de la electrónica".[98]

La utilización de esta tecnología ha permitido el nacimiento de nuevas figuras delictivas, denominados delitos informáticos, aunque ya se estableció en el capítulo anterior su base teórica; pero recapitulando estos son: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos"[99] que en diversos estados han sido abordadas de diferente manera.

A continuación se hará un breve análisis del contenido de algunas leyes latinoamericanas, respecto a la forma de incorporación dentro de la legislación penal de cada país, sobre delitos informáticos, en relación con lo legislado en Guatemala y especialmente con los delitos cometidos en la banca electrónica.

3.1. Los delitos informáticos contenido en el Código Penal de Guatemala

En el año 1996, fue cuando se adicionaron los delitos informáticos al Código Penal en Guatemala, a través de una reforma contenida en el Decreto Número 33-96 del Congreso de la República, publicado el veinticinco de junio de mil novecientos noventa

---

[98] http://definicion.de/informatica/#ixzz2tWQKILCz, (03 de marzo de 2014)
[99] **Ibíd**

y seis y que entró en vigencia el tres de julio del mismo año. No todos los tipos legales incorporados están íntimamente ligados a los ilícitos cometidos en la banca electrónica, en virtud que algunos pertenecen a otras áreas que se encuentran fuera del ámbito de acción de los delitos cometidos en el ciberespacio dirigidos al robo o defraudación de bancos.

Por lo anterior el estudio estará dirigido solo aquellos tipos penales que tienen relación intima con los delitos que por sus elementos y el bien jurídico tutelado han sido utilizados para robo en bancos y usuarios del mismo utilizando herramientas informáticas para su comisión.

"En virtud de la naturaleza del bien jurídico que protege el Estado a través de regular los denominados Delitos Informáticos, estos fueron ubicados dentro del Título VI De los delitos contra el patrimonio. El legislador los ubica en este apartado en virtud que se protegen creaciones de la propiedad intelectual (propiedad industrial y derechos de autor), así como derechos humanos intrínsecos de las personas (intimidad personal), que para algunos doctrinarios no tiene carácter de patrimonio".[100]

El autor Barrios Osorio señala que: "es importante establecer que el Decreto no contempla los casos de delitos culposos, es decir debe de existir dolo (Artículos 10, 11, 12 del Código Penal). // Los delitos informáticos regulados en el Código Penal protegen los elementos de los sistema de información en determinados hechos, en otros pueden ser un delito común y/o puede darse la situación de un concurso de delitos".[101]

---

[100] Barrios Osorio. **Ob. Cit.**, Pág. 390
[101] **Ibíd.,**Pág. 390

Los delitos informáticos establecidos en el Código Penal pueden clasificarse según el elemento del sistema que protegen, en:

A. "Delitos que protegen los programas de computación: alteración de programas (Artículo 274 "B"); reproducción de instrucciones o programas de computación (Artículo 274 "C"); programas destructivos (Artículo 274 "G").

B. Delitos contra las bases de datos: destrucción de registros informáticos (Artículo 274 "A").

C. Delitos contra la información contenida en los sistemas: uso de Información (Artículo 274 "F"); manipulación de información (Artículo 274 "E").

D. Delitos de la información contenida en los sistemas cuando afectan la intimidad de las personas: registros prohibidos (Artículo 274 "D")".[102]

Los delitos informáticos regulados en el Código Penal se analizarán siguiendo el criterio del autor Barrios Osorio por el bien jurídico protegido en normas tipo y solamente aquellos que tengan relación según sus elementos e interpretación doctrinaria con los delitos cometidos en la banca electrónica en base a casos expuestos en el capítulo anterior del presente trabajo de tesis.

3.1.1. Reproducción de instrucciones o programas de computación

El Decreto Número 33-96 en el Artículo 15 adiciona el Artículo 274 "C" al Código Penal donde describe: "Reproducción de instrucciones o programas de computación. Se

[102] **Ibíd.**, Pág. 390

impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación".

En el Artículo 274 "C" el bien jurídico tutelado está dirigido a proteger: "...los derechos de autor y conexos del creador del programa de ordenador (se le denomina comúnmente el programador cuando es una persona individual) o la persona a quien cedió sus derechos".[103]

"En materia de programas de ordenador la persona (individual o jurídica) titular de los derechos de autor (morales, pecuniarios o patrimoniales, conexos) o sus herederos, tienen el derecho exclusivo a su reproducción distribución, importación y exportación de copias acceso, traducción, entre otros derechos. Lo anterior queda establecido en la ley especial y determinado en los contratos que celebre con quien ceda algunos de los derechos de que goza en su calidad de autor".[104]

Los bancos para la automatización de sus servicios, han necesitado de la colaboración de expertos en sistemas informáticos, con el tiempo han implementado departamentos especializados de expertos en tecnología informática; estas son las personas individuales contratadas por el banco para la realización de sistemas que permita prestar a sus cuentahabientes de manera computarizada sus servicios. Los desarrolladores de estos sistemas, a su vez, ceden los derechos de propiedad intelectual a estas entidades financieras, (regularmente a través de un contrato laboral o mercantil en caso de persona jurídica independiente); por lo que ellas tienen el uso

[103] **Ibíd.**, Pág. 392
[104] **Ibíd.**, Pág. 392

exclusivo de su reproducción, distribución, importación y exportación de copias, accesos y demás derechos que le asignen las leyes de la materia.

En caso de los delitos cometidos en la banca electrónica, como los piratas informaticos, que infringe este bien jurídico tutelado, al entrar a un sistema sin autorización, permite que el titular del derecho de autor (los bancos del sistema por cesión), tenga la asistencia de la tutela estatal para procesamiento de los culpables.

El autor Barrios Osorio, aclara que "en la jerga informática, en el lenguaje comercial, en la publicidad de las empresas afectadas y en las campañas de prevención, se le denomina a este delito 'piratería', pero en la legislación penal guatemalteca el delito de piratería se encuentra como un delito contra la seguridad colectiva (libro II, Título VII, Capítulo III, Artículo 299, 230)".[105] Sin embargo, comparando los elementos del delito anteriormente expuesto y los piratas informáticos, encuadran dentro del tipo penal analizado, dentro de los párrafos anteriores.

El riesgo que corren las entidades bancarias al contratar desarrolladores expertos de sistemas, es cuando "el acceso a equipo de computación y su tecnología, facilitan la comisión de este delito; a ello se le suma la falta de conocimiento en materia informática en aspectos técnicos y legales, el alto costo de algunos programas de ordenador y los errores en la redacción de los contratos de desarrollo y de licencia, aunque en principio ninguno de los aspectos indicados es causa de justificación para la comisión de este delito cuando la conducta del sujeto activo encuadra en la norma

[105] **Ibíd.**, Pág. 392

tipo."[106] Sin embargo, existen casos en que los administradores de redes que trabajan en la misma entidad bancaria, participan en colaboración con agentes externos para la comisión del hecho.

Como ya se menciono, un ejemplo de este tipo es donde se sindican responsables por delitos de Piratería o Reproducción de Instrucciones o Programas de Computación. La relación con los delitos anteriores al caso de piratería presentado en la banca electrónica en Guatemala, está en la forma de operar de estos delincuentes cibernéticos, porque crearon páginas web idénticas a las de los bancos, con el propósito de desviar información a su base de datos de esta manera obtener datos personales, contraseñas, etc.; asimismo, estar pendientes de las salida y entrada de efectivo que se encuentra en movimiento a causa de las diversas actividades que se dan dentro del uso del sistema bancario en línea. Esto les permitía hacer transferencias a sus propias cuentas bancarias y de esta manera realizar una forma de defraudación y hurto a los cuentahabientes utilizando la reproducción de un programa sin autorización.

3.1.2. Delito contra la información contenida en los sistemas

Dentro de la clasificación propuesta por el autor Barrios Osorio el delito que tiene relación con los hechos ilícitos cometidos a la banca electrónica, es el Uso de información.

Dicho delito fue regulado por el Decreto Número 33-96 en el Artículo 18 adiciona el Artículo 274 "F" del Código Penal el cual establece: "Uso de información. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin

[106] **Ibíd.,** Pág. 393

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

El autor Barrios Osorio determina que se protegen dos bienes jurídicos o derechos:

a) "Los registros informáticos (en cuanto a su utilización no autorizada).
b) El acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos".[107]

Este delito fue analizado dentro del capítulo anterior, al exponer el robo de identidades; aunque expresamente no se encuentra regulado, tiene estrecha relación con el mismo, cuando estos registros automatizados esta bajo la responsabilidad de una entidad bancaria y agentes externos hacen uso del sistema sin autorización. Es por ello que el primer bien jurídico es infringido, en la comisión de hechos ilícitos en la banca electrónica especialmente en el robo de datos personales, porque las personas utilizan datos de acceso de cuentahabientes para poder debitar de cuentas bancarias cantidades de dinero.

Ahora con el segundo, la relación que tiene con los delitos cometidos en la banca electrónica, es cuando personas autorizadas que tienen a su cargo la administración de la información, dentro de los sistemas bancarios, utilizan dichos registros para la comisión de hechos ilícitos, es el caso de trabajadores del banco que tienen acceso a información confidencial.

[107] **Ibíd.,** Pág. 393

Respecto a lo anterior el autor Barrios Osorio, establece que: "la persona que crea un registro informático (de datos lícitos), dispone de quienes van a tener autorización para hacer uso de los mismos. La utilización autorizada de los registros pueden ser directa del computador que los tiene almacenados, en línea (red interna y externa) e inclusive pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas e inclusive un usuario autorizado para acceder al sistema, pero no para utilizar de forma distinta los registro informáticos".[108]

"Cuando un sujeto sin la autorización del titular de ese registro informático hace uso del mismo estaría incurriendo en el delito establecido. La redacción es muy limitada y puede hacer incurrir al operador de justicia en errores. En el caso de utilizar esos registros informáticos en otro sistema de información automatizado, se estaría incurriendo en el delito establecido, le genere ese uso lucro o no. Se puede dar la situación que sea una persona quien 'extrae' el registro y otra persona la que lo utilice en un sistema. Esto puede estar en concurso con otros delitos".[109]

Los trabajadores de un banco tienen diferentes niveles de acceso al sistema cada uno está limitado según la tarea que le corresponde dentro de la entidad, el que infringe el límite de lo que le compete manejar, si lo realiza una persona que no está autorizada se encuadra esa acción a este delito; resalta el autor Barrios Osorio que "...el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, inclusive si no realiza ninguna acción con la información. Esto se conoce en doctrina como el delito de hacking"; asimismo // "si el acceso fue casual, es decir no

[108] **Ibíd.,** Pág. 393
[109] **Ibíd.,** Pág. 393

existe intención, no constituirá delito en virtud que no están regulados delitos informáticos culposos (ver segundo párrafo Artículo 12 Código Penal)".[110]

El uso de información que establece este hecho ilícito informático, respecto a los delitos cometidos a la banca electrónica en Guatemala, está relacionado con los registros informáticos (en cuanto a su utilización no autorizada), esto como ya se ha reiterado en varias ocasiones dentro del presente trabajo de investigación, se describió en los casos de robo de identidades, ya sea, defraudando al banco o bien para poder acceder cuentas bancarias y con ello extraer cantidades de dinero.

Entre los casos de robo de identidades expuesto dentro del presente estudio, referente a la defraudación o robo dentro de la banca electrónica en Guatemala, están el ingreso de redes sociales con herramientas de hackeo o sustracción de cookies, para obtener la información digital que queda grabada en la computadores como contraseñas, cuentas bancarias o de tarjetas de crédito. Esto les permite el acceso no autorizado a la base de datos del cuentahabiente en los bancos del sistema mediante banca electrónica y extraer cantidades de dinero dentro del sistema de banca en línea.

La diferencia fundamental que tiene este tipo penal es que no concursa con el delito de reproducción de instrucciones o programas de computación analizando anteriormente, pero si con el delito de registros prohibidos que se describirá en el próximo apartado.

[110] **Ibíd.,** Pág. 393

3.1.3. Delitos de la información contenida en los sistemas cuando afecta la intimidad de las personas

Dentro de esta clasificación se encuentra como único delito el de registros prohibidos, contenido en el Decreto Número 33-96 en el Artículo 16 adiciona el Artículo 274 "D" del Código Penal el cual establece: "Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas".

El autor Barrios Osorio describe que: "los datos personales se definen en la ley de protección de Datos Personales de Argentina como: Artículo segundo: ...Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". Doctrinariamente son clasificado como Privados o Íntimos y públicos, los primeros se subdividen en sensibles y no sensibles, los primero revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Asimismo, "...define como intimidad o privacía el derecho del individuo a ejercer el control de aquella información de sí mismo, que desee compartir con otros, de la cantidad que de la misma facilite a otros y del momento en que desee hacerlo".[111]

"El Artículo 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del Congreso de los Estados Unidos Mexicanos establece: Como información confidencial: I. La entrega con tal carácter por los particulares a los sujetos obligados... y // II. Los datos personales que requieran el consentimiento de los

[111] **Ibíd.,** Pág. 393

individuos para su difusión, distribución o comercialización en los términos de esta ley".[112]

"No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público"[113].// En el caso "...de Guatemala no cuenta con una Ley de Protección de Datos, que determine de forma expresa que datos se consideran públicos y cuales privados (íntimos); eso ha dado el problema que se crean base o banco de datos, así como toda clase de compilación de datos de las personas, que al ser administrados de forma inadecuada o bien los datos fueron adquiridos por un procedimiento ilegal y que entren en la esfera de la intimidad de las personas, se estaría cometiendo el delito de registros prohibidos".[114]

La relación principal con el delito cometido en la banca electrónica esta en los casos de robo de identidad descrito en el capitulo anterior con fines de uso ilícito, esto conlleva como ya se analizo con anterioridad a un concurso delitos con los delitos de hurto, estafa, caso especial de estafa y uso de información. Porque, al no existir una definición clara sobre datos personales dentro de la legislación del país y el límite de su protección, todos los datos sustraídos en cualquier forma conforman el delito de Registros prohibidos por lo tanto encuadra como un elemento de los robos de identidad para poder cometer delitos en la banca electrónica; además, el Uso de esta información y la posterior obtención del dinero a través de ardid o engaño (hurto, estafa y caso especial), dentro del sistema de banca electrónica, conforman cada uno de los

[112] **Ibíd.,** Pág. 395
[113] **Ibíd.,** Pág. 395
[114] **Ibíd.,** Pág. 395

elementos que permiten consumar una de las formas de defraudar o hurtar ganancias ilícitas en el servicio de banca en línea que presta el sistema bancario guatemalteco.

3.2. Ley 1273-2009 de la protección de la información y de los datos de la República de Colombia

En la República de Colombia se público el cinco de enero de 2009, en el Diario Oficial la Ley numero 1273-2009, por medio de la cual se modifica el Código Penal, creándose un nuevo bien jurídico tutelado - denominado "De la protección de la información y de los datos"-, adicionando mediante su Artículo uno el Título VII BIS, con el cual se pretende preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El decreto creo dos capítulos el primero describe "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", el segundo "De los atentados informáticos y otras infracciones".

El primer capítulo está conformado por los Artículos 269A hasta el 269H, donde regula los siguientes delitos:

a) Acceso abusivo a un sistema informático
b) Obstaculización ilegítima de sistema informático o red de telecomunicación
c) Interceptación de datos informáticos
d) Daño Informático
e) Uso de software malicioso
f) Violación de datos personales

g) Suplantación de sitios web para captura datos personales

h) Circunstancias de agravación punitiva

El segundo capítulo que describe de los atentados informáticos y otras infracciones se encuentran contenido en los Artículo 269I al 269J del cuerpo legal antes mencionado, que contiene los siguientes delitos:

a) Hurto por medios informáticos y semejantes

b) Transferencia no consentida de activos

Los delitos dentro del Estado de Colombia tienen una mejor descripción técnica de la comisión de hechos delictivos cometidos en el ciberespacio en comparación con Guatemala. La razón fundamental del porque esta regulación legal es mejor que la nacional, es precisamente por el año de su incorporación en el país, ya que los tipos penales informáticos en el Estado guatemalteco fueron introducidos a la legislación penal en 1996; mientras que la legislación colombiana fue en el año 2009, lo que hace una diferencia 13 años, que marca el conocimiento en los particulares y legisladores del uso de la tecnología por medios informáticos y las nuevas formas de operar para la comisión de nuevos hechos ilícitos a través del ciberespacio.

Se ha reiterado a lo largo de la presente investigación que los delitos cometidos en la banca electrónica en Guatemala pueden estar dentro de un concurso con otros delitos, porque es necesario la realización de diversas estrategias y técnicas de la informática para lograr su comisión final, la que es defraudar o disminuir el patrimonio ya sea de una persona física (cuentahabiente) o jurídica (entidad bancaria).

Respecto a la relación que la tipificación de delitos informáticos que el país colombiano tiene con los robos generados en la banca electrónica en Guatemala, a los casos expuestos en el Capítulo II del presente trabajo de tesis son: el caso de robo de identidades para poder facilitar el acceso al sistema de banca en línea presenta características similares con varios delitos informáticos colombianos.

Como primera forma para iniciar el camino para la comisión del delito informático en cuanto al robo de identidades y posterior uso en la banca electrónica; puede mencionarse el Artículo uno de la ley objeto de estudio y comparación; que adiciona el Artículo 269F al Código Penal de Colombia que establece: "Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes..."

Como se menciono con anterioridad el delincuente cibernético o persona física acceden a cuentas de correo electrónico, redes sociales, etc., para la obtención de datos informáticos, posterior a ello se utiliza para acceder a la base de datos que el sistema bancario brinda a sus cuentahabientes para sus transacciones personales, aquí es donde se cumple lo contenido en el Artículo uno de la ley 1273-2009 de la República de Colombia que adiciona el Artículo 269A al Código Penal de ese mismo país que establece: "...Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema

informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo..."

Otro caso que también se encuadra en los casos expuestos en el capitulo anterior del presente estudio donde describe "piratas informáticos" y "Phishing". El primero trata de que los delincuentes ingresan a bases de datos de usuarios de bancos creando cuentas parales para verificar el estado financiero de los cuentahabientes y de esta manera trasladar a sus propias cuentas cantidades de dinero. El segundo, se da mediante la circulación de correos electrónicos solicitando actualizar información de banca en línea por parte de estafadores cibernéticos. El enlace adjunto le direcciona a una página web que aparenta ser legítima, pero el usuario está siendo víctima de un intento de estafa.

Estos dos casos encuadran perfectamente en el delito informático establecido en el Artículo 269C, del Código Penal de Colombia porque describe: "Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".

Además también tiene mucha relación con el Artículo 269G, del mismo cuerpo legal mencionado que describe: "Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.... // asimismo establece "...el que modifique el sistema de resolución de

nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave...". Dato importante es mencionar que la ley también creo circunstancias de agravación punitiva, donde aumenta de la mitad a las tres cuartas partes si la conducta se comete contra redes o sistema informáticos o de comunicaciones en el sector financiero (Artículo 269H Código Penal Colombiano).

Otros delitos íntimamente relacionadas con los casos expuesto donde existe defraudación y robo dentro de la banca electrónica y que puede considerarse el adecuado a la forma de operar sin que exista algún concurso de delito son los dos delitos contenidos en el Capítulo II de la Ley 273-2009 de la República de Colombia ya que menciona el objetivo final que es apropiarse de cantidades de dinero que se encuentra en las entidades bancarias, que pueden manipulares mediante diversas herramientas de tecnología informática, estos delitos están contenido en el Artículo uno y adiciona los Artículos 269I y 269J al Código Penal colombiano, que a continuación se describen.

El primer delito expresa: "...Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el Artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el Artículo 240 de este Código".

El segundo establece: "...Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero... asimismo el Artículo mencionado expresa: "...a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa..."

3.3. Ley 9048 de los Delitos Informáticos en Costa Rica

La Asamblea Legislativa de la República de Costa Rica en el año dos mil doce sancionó y publicó la reforma de varios Artículos y la modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal a través del Decreto Número 17.613 siendo los Artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Número 4573, Código Penal, de 4 de mayo de 1970. Este decreto legislativo introduce los siguientes delitos:

a) Corrupción
b) Violación de correspondencia o comunicaciones
c) Violación de datos personales
d) Extorsión
e) Estafa informática
f) Daño informático
g) Espionaje
h) Daño agravado
i) Sabotaje informático

j) Delitos informáticos y conexos dentro de ellos se encuentra: Suplantación de identidad, Espionaje informático, Instalación o propagación de programas informáticos maliciosos, Suplantación de páginas electrónicas, Facilitación del delito informático, Narcotráfico y crimen organizado, Difusión de información falsa.

Las reformas contenidas del Decreto Número 17.613 de la República de Costa Rica además de ser recientes ya que se realizaron en el año 2012, incorpora delitos comunes que también son cometidos mediante el uso de la tecnología de información que en otras legislaciones las clasifican como delitos de contenido.

En comparación con la legislación guatemalteca se puede apreciar que de igual manera que en Colombia, los delitos informáticos tipificados en Costa Rica son más específicos, técnicos y con una redacción más precisa a los hechos ilícitos informáticos que se están cometiendo en la actualidad, esto también es a causa de la época en que se están implementando en comparación con Guatemala que datan del año 1996. Respecto a los casos expuestos en el capítulo anterior que describen las formas en que se defrauda el sistema bancario (tanto la entidad como sus usuarios), en la República los delitos que se relacionan son los siguientes:

En el caso de robo de identidades para poder defraudar o robar dentro de la banca electrónica en Guatemala, son varios los delitos que encuadran en este comportamiento.

Uno de ellos está contenido en el Artículo 196 bis del Código Penal de Costa Rica que establece: "Violación de datos personales: ...quien en beneficio propio o de un tercero,

con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos..."

Estafa informática (Artículo 217 bis): este delito se comete "...quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro."

El otro precepto legal relaciona con el anterior caso se encuentra establecido en el Artículo 230, que describe: "...Suplantación de identidad. Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero..."

Con relación a los casos de "piratas informáticos" y "Phishing", descritos en el titulo anterior, los delitos relacionados en la legislación costarricense se encuentran los siguientes:

A. Violación de correspondencia o comunicaciones (Artículo 196): este delito se comete cuando "...con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona". También establece un aumento en la pena y respecto a los delitos de banca electrónica los relacionados son: "a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.//b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores y electrónicos, ópticos o magnéticos..."

B. Instalación o propagación de programas informáticos maliciosos (Artículo 232): este delito conlleva la instalación de programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, en general y especialmente establece los casos que tienen compatibilidad con los ilícitos cometidos a la banca electrónica en Guatemala los siguientes: "...a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.//

...e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos". Asimismo establece que: "La pena será de tres a nueve años de prisión cuando el programa informático malicioso: i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal //...iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi. // iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero..."

C. Suplantación de páginas electrónicas (Artículo 233): Este delito lo comete "quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet. La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero".

La legislación costarricense, en comparación con la de Guatemala, se puede apreciar que el órgano legislador de ese país, tiene un idea clara de la identificación y del aumento de delitos, con la utilización de datos personales en medios informáticos, en cambio Guatemala, su regulación en algunos tipos penales es confusa y conlleva a concurso de delitos, para encuadrar los hechos ilícitos cometidos en la banca electrónica. En cuanto a los demás casos expuestos (phishing, piratas informáticos); no establece expresamente dichos actos ilícitos, de igual manera que el código penal

guatemalteco; pero la diferencia radica que en la ley costarricense describen los elementos que la producen, aunque el nombre no sea exacto puede encuadrarse con más facilidad a dichos hechos delictivos.

3.4. Ley 53-07 sobre delitos de alta tecnología de República Dominicana

La República Dominicana dentro de su legislación se diferencia en comparación con los otros países latinoamericanos analizados en cuanto a cómo han incorporado los delitos informáticos, este se caracteriza por crear una ley especial bajo el Número 53-07, sancionada el mes de enero de 2007, donde detalla Crímenes y Delitos de Alta Tecnología.

La ley de Crímenes de Alta Tecnología de República Dominicana es muy completa, su estructura contenida en dos títulos tiene disposiciones generales y conceptuales como objeto, ámbito y principios, definiciones que permiten conocer conceptos técnicos respecto que conforman los elementos de los delitos informáticos.

Dicha ley describe en el Artículo numeral romano uno, el Objeto del instrumento legal y establece que es para "la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales...La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos

comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos".

Dentro de su Título segundo, forma una estrategia nacional para el combate de dichos delitos que van desde la descripción de los delitos como parte sustantiva, dividiéndolos en: crímenes y delito contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información, delitos de contenido, delitos de propiedad intelectual y afines, delitos de propiedad intelectual y afines, crímenes, delitos contra la nación y actos de terrorismo.

Dentro de la primera clasificación contenida en los Artículos del cinco al 11, de la mencionada ley, se encuentran los siguientes delitos:

a) Códigos de acceso
b) Acceso ilícito
c) Acceso ilícito para servicios a terceros
d) Beneficio de actividades de un tercero
e) Dispositivos fraudulentos
f) Interceptación e intervención de datos o señales
g) Daño o alteración de datos
h) Sabotaje

En la segunda clasificación que son los delitos de contenido, se diferencia de los anteriores, en virtud que, su comisión se da porque el contenido ya sea de las paginas dentro de la internet presentan delitos ya tipificados pero se utiliza como herramienta la

alta tecnología. Se encuentra regulado en los Artículos del 12 al 24 de la ley mencionada en este apartado, siendo los siguientes:

a) Atentado contra la vida de la persona
b) Robo mediante la utilización de alta tecnología
c) Obtención ilícita de fondos
d) Estafa
e) Chantaje
f) Robo de identidad
g) De la falsedad de documentos y firmas
h) Uso de equipos para invasión de privacidad
i) Comercio ilícito de bienes y servicios
j) Difamación
k) Injuria pública
l) Atentado sexual
m) Pornografía infantil

En cuanto a los delitos relacionados a la Propiedad Intelectual y afines, describen cuando contravenga la ley de la materia. Respecto a los ilícitos cometido contra telecomunicaciones, estos se encuentran dirigidos a crímenes que se cometen en la interceptación o uso de redes físicas, por último los crímenes contra la nación y actos de terrorismo en relación con la alta tecnología se encuentran dentro de los Artículos 27 y 28 los cuales denominan: crímenes y delitos contra la nación y actos de terrorismo.

Otra característica importante de la presente ley es porque trata de abarcar todo el ámbito de comisión, investigación, castigo y sanción de los delitos informáticos con la creación de una ley especifica que contiene: objetivos, principios, aplicación y una clasificación amplia sobre las diferentes formas de comisión de los delitos, también, establece una estrategia interinstitucional para el combate del mismo; describiendo a los organismos competentes y reglas de derecho procesal contenida en los Artículos del 29 al 50 de la Ley de Crímenes de Alta Tecnología de la República Dominicana.

Los organismos encargados y competentes son dependientes del Ministerio Público especializados en la investigación y persecución de los delitos y crímenes contenidos en la ley anteriormente mencionada. También dicho precepto legal crea una comisión interinstitucional, un Departamento de investigación de crímenes y Delitos de Alta Tecnología (DICAT) y una División de investigaciones de delitos informáticos (DIDI), estableciendo entre otras ordenanzas: su organización, comunicación, funciones y presupuesto.

Por otro lado establece medidas cautelares y procesales que describen la aplicación del Código Procesal Penal, conservación de los datos, facultades del Ministerio Público; prácticas de recopilación de evidencia, proveedores de servicios entre otras directrices para la correcta persecución penal.

También describe las formas en que se impondrá la responsabilidad civil y penal de las personas moral, las acciones administrativas, pago de indemnizaciones, leyes la complementan, la forma de acción pública y finalmente el tribunal competente, (Artículos 60 al 65).

La peculiaridad más importante de esta ley es la implementación de una estrategia específica para el combate, persecución y sanción de hechos ilícitos dentro de la ciberespacio. Su estructura y la forma en que pretende abarcar cada espacio, tanto sustantivo como procesal, sobre la comisión de los hechos delictivos dentro de la alta tecnología o la tecnología de comunicación es un avance en la creación de la materia. La limitación encontrada es que no menciona a entidades financieras solamente generaliza comportamientos delictivos con el uso de la informática.

Respecto a la vinculación de los hechos ilícitos cometidos en la banca electrónica guatemalteca, específicamente los casos expuestos en el capitulo anterior del presente trabajo de tesis, los delitos que son compatibles son los siguientes:

El robo de identidad para la comisión de hechos ilícitos en la banca electrónica puede relacionarse con varios delitos contenidos en la Ley de Crímenes de Alta Tecnología de República Dominicana el primero de ellos es el contenido en su Artículo 17, que expresa: "Robo de identidad. El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones..."; Sin embargo los elementos de este delito no complementa la comisión de los hechos delictivos realizado en el servicio bancario en línea, por lo que es necesario agrupar otros delitos regulados en la ley mencionada.

Una de las formas de poder obtener datos personales como ya se estableció, es a través de la redes sociales, correos electrónicos y bases de datos privados, para ello es necesario usar equipos que permitan la invasión de esa privacidad y precisamente es un delito dentro de la Ley mencionada que en su Artículo 19 establece: "...El uso, sin

causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas..."

De los anteriores delitos se puede determinar que el delincuente ya ha cometido dos delitos para la obtención de datos personales según la ley especial de la República Dominicana, pero es necesario que participen dos delitos más para la consumación de delitos cometidos en la banca electrónica estos son:

El primero es el denominado Códigos de Acceso (Artículo 5) "El hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo..."; en este delito lo aplicable a los casos de hechos ilícitos contra la banca electrónica es copiar, generar y utilizar códigos de acceso para acceder a un sistema y especialmente a un sistema bancario.

El segundo delito es el Acceso Ilícito (Artículo 6) "El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización...". Respecto a los delitos con robo de identidades realizados en el sistema bancario en línea es aplicable el acceder al sistema utilizando identidad ajena.

Con relación a los casos de **piratas informáticos y Phishing,** aplicando la legislación para delitos informáticos de la República Dominicana los delitos que tienen compatibilidad son los siguientes:

A. Dispositivos Fraudulentos, (Artículo 8). Esta dirigido a la creación de herramientas de sistema o electrónicas para la comisión de hechos ilícitos dentro del ciberespacio.

B. Interceptación e Intervención de Datos o Señales, (Artículo 9). Este va dirigido a obtener datos en diferentes formas perteneciente a otra persona; sin autorización de autoridad competente, por cuenta ajena o propia a través de cualquier sistema informático y sus derivaciones, voluntaria e intencionalmente para violar la intimidad y la privacidad de las personas físicas o morales.

3.5. Capítulo X del Código Penal peruano (parte referida a delitos informáticos)

La legislación peruana al igual que Guatemala, Colombia y Costa Rica incorporaron los delitos informáticos a través de una reforma contenida en la Ley Número 27309, publicado el 17 de julio del año 2000, el contenido capitular es pequeño solamente tres Artículos del 207A al 207C. Los cuales son:

a) Delito Informático
b) Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras
c) Delito informático agravado

El único delito que tiene relación con los delitos cometidos en la banca electrónica es el contenido en el Artículo 207-A, que expresa: "...Delito Informático. El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos..."

Puede apreciarse que dentro de los casos expuestos en el presente estudio este delito solamente se asemeja a los delitos de **Piratas Informaticos y Phishing**. En caso de robo de identidad o bien de establecer un agravante cuando es cometido al sistema bancario nada describe al respecto.

3.6. Diferencias en los tipos penales de otras legislaciones y el delito informático en Guatemala

Las diferencias principales entre las leyes de Guatemala y las de la República de Colombia, Costa Rica y República Dominicana son:

A. Los delitos informáticos contenidos en Código Penal de Guatemala no son compatibles con la realidad de las diversas formas de comisión de hechos ilícitos en el ciberespacio porque fueron incorporados con una falta evidente de conocimiento de los sistemas de comunicación informática en comparación con los otros países.

B. La época en que se incorporaron los delitos informáticos a la legislación penal guatemalteca data del año 1996, en comparación con los demás países que han sido recientemente incorporados ya que el más cercano a nuestro país son los

delitos informáticos contenidos en el Código Penal del Perú, (incorporado en el año 2000) y presentan deficiencias al igual que Guatemala en su contenido respecto a la realidad de casos ocurridos de hechos ilícitos cometidos en la banca electrónica.

C. En la República Dominicana existe una ley especial mientras que en Guatemala, Colombia y Costa Rica fueron adicionadas mediante reformas a los códigos penales de cada país.

D. Los delitos dentro del Estado de Colombia tienen una mejor descripción técnica de la comisión de hechos delictivos cometidos en el ciberespacio en comparación con Guatemala.

E. Las Leyes de Colombia y Costa Rica son las únicas que regulan circunstancias de agravación punitiva si la conducta se comete contra redes o sistemas informáticos o de comunicaciones en el sector financiero o bancario.

F. La ley colombiana es la única ley que regula expresamente el hurto a entidades bancarias.

G. Respecto al caso de robo de identidad para realizar hechos ilícitos dentro del servicio en línea bancario la legislación penal de Costa Rica y República Dominicana son los únicos que tiene una definición concreta sobre datos personales y su violación mediante la creación de un tipo penal

H. De todos los ordenamientos analizados la ley más completa en cuanto a la clasificación de delitos y estratega para la persecución es la Ley de Crímenes de

Alta Tecnología de la República Dominicana la deficiencia que presenta es que no menciona delitos dirigidos específicamente a la banca electrónica, sistema financiero o bancario.

3.7. Iniciativa 4055 Ley de delitos informáticos en Guatemala

"El partido de Acción de Desarrollo Nacional (ADN), creó la iniciativa 4055 de Ley De Delitos Informáticos, a través de los diputados ponentes: Francisco José Contreras Contreras, Mario Roderico de León Mazariegos, Félix Adolfo Ruano de León. la cual tiene por objeto la protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información. Así como la prevención y sanción de los delitos cometidos relativos a fraude Informático, daño informático, acceso ilícito, falsificación informática, espionaje informático, violación de la disponibilidad, reproducción de equipos, etc."[115]

Esta iniciativa pretende crear una ley especial de delitos informáticos; su estructura la compone cinco títulos el primero establece las disposiciones generales y de definiciones de las palabras técnicas contenidas en el documento, el segundo describe delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos contenidos en los Artículos cuatro al siete los cuales son:

a) Acceso sin autorización
b) Daño informático
c) Posesión de equipos o prestación de servicios para daño informático

[115] http://www.transdoc.com.gt/assets/images/users/dani/file/, (23 de enero de 2014)

d) Espionaje informático

En el Título tres establece los delitos informáticos relacionados con la propiedad y autenticidad, que se describen en los Artículos del 8 al 13, siendo los siguientes:

a) Fraude informático
b) Uso fraudulento de tarjetas inteligentes o instrumentos análogos
c) Provisión indebida de bienes o servicios
d) Posesión de equipo para falsificaciones
e) Falsificación Informática
f) Invitación de acceso

Por otro lado dentro del Titulo cuatro se encentra los delitos relacionados con el contenido, que se establecen dentro de los Artículos 14 al 15 de la iniciativa de ley mencionada los cuales son:

a) Pornografía infantil
b) Alteración de imágenes

En el quinto y último título establece la creación de una Unidad de Investigación, establecida en el Artículo 16 de la iniciativa de ley mencionada que expresa: "El Ministerio Público, en un plazo no mayor de sesenta (60) días, creará y organizará una Unidad de Investigación especializada en delitos informáticos..."

Esta iniciativa tiene una semejanza solamente en la creación de una clasificación de delitos con la Ley de Crímenes de Alta Tecnología de República Dominicana, pero no contiene estrategias de persecución penal, ni coordinación interinstitucional.

La iniciativa mencionada solo contiene la parte sustantiva como lo es el establecimiento de una nueva clasificación de delitos informáticos en Guatemala; la creación de una unidad dentro del Ministerio Público que acertadamente se propone. Evidentemente el contenido de la ley es limitado, no abarca agravantes punitivos en caso de que se cometan contra entidades bancarias y sus usuarios, ni refiere tampoco delitos de la banca electrónica. Por lo que dentro del desarrollo de aprobación para ley debe ser ampliado y modificado para abarcar la totalidad de hechos ilícitos que se presenta en el ciberespacio.

En comparación con los casos expuestos los delitos de la iniciativa y lo casos de hechos delictivos en la banca en línea descritos en el presente estudio en el caso de robo de identidades, no tiene tipificado dicho delito expresamente, todo es en referencia a los casos de **piratas informáticos y phishing**, como podrá apreciarse en los siguientes delitos:

A. Acceso sin autorización (Artículo 4): "El que sin plena autorización, acceda, intercepte, interfiera o utilice un sistema o dato informático, de naturaleza privada o pública, y de acceso restringido..."

B. Espionaje informático (Artículo 7): "El que, ilegítimamente, se apodere, obtenga, revele, transmita o difunda el contenido, parcial o total, de un sistema o dato

informático, de carácter público o privado..." // asimismo describe "...quien creare un sistema o datos informáticos que puedan afectar la intimidad o privacidad de las personas".

C. Fraude informático (Artículo 8): "El que para obtener algún beneficio para sí o para un tercero, mediante cualquier artificio tecnológico o manipulación de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonio en perjuicio de otro..."

D. Falsificación informática (Artículo 12): "Quien a través de cualquier medio, cree, altere, modifique o elimine, total o parcialmente, un sistema, documento o dato informático y simule su autenticidad..." // asimismo describe: "...el que, por cualquier medio, conduzca, enlace o remita a un sitio o sistema informático falso o fraudulento" // la pena se aumenta para quien procura, "...un beneficio propio o ajeno".

E. Invitación de acceso (Artículo 13): "El que de manera deliberada e ilegitima, a través de mensaje de datos o de cualquier otro medio, atraiga o invite a ingresar a un sitio o sistema informático falso o fraudulento..." // la pena se aumenta para quien procura, "...un beneficio propio o ajeno".

3.8. Acciones contra bienes las tecnologías de la información y la comunicación no tipificadas en la legislación guatemalteca

"Existen una serie de acciones que cometen las personas que no son delitos en Guatemala por no estar expresamente prohibidas, en virtud del principio de legalidad;

en otros Estados estas conductas se encuentran tipificadas como delitos. Algunas de las conductas anómalas en la Internet que afectan a los sujetos (usuarios, PSI y Servidores), se describen a continuación":[116]

a) "El delito de Spam que consiste en enviar correos electrónicos no solicitados de forma masiva.
b) El delito de Spyware que consiste en introducir programas que posteriormente enviarán la información sustraída del sistema al sujeto que lo instaló.
c) El delito de phishing por la idea de "pescar" información en la Internet a través de correos electrónicos o formularios y que en muchos casos tiene por objeto "robar la identidad" de las personas.
d) Una variante del phishing se ha denominado pharming que puede ser definido como una nueva forma de fraude en la Internet al intervenir las comunicaciones entre el usuario y los Servidores y que tiene como objeto re direccionar la comunicación del usuario a un sitio falso para que ingrese sus datos.
e) Otra conducta prohibida en otros Estados surge cuando una persona mayor de edad permite a un menor de edad (niño o adolecente) tener acceso a sitios de categoría XXX."[117]

"Además el fraude informático, robo informático, subastas ilegales, publicaciones obscenas en la Internet, pornografía en la Internet, entre otros"[118]. Tampoco establece agravantes de fraude o robo informático cuando van dirigidas a entidades bancarias y sus usuarios.

---

[116] Barrios Osorio.**Ob. Cit.**, Pág. 411
[117] **Ibíd**
[118] **Ibíd**

CAPÍTULO IV

4. Aplicación de la informática forense en la investigación de delitos cibernéticos en el sistema bancario guatemalteco

Los delitos cometidos en la banca electrónica tienen su origen a partir del uso del comercio electrónico, este dio "...un nuevo enfoque al comercio internacional y al uso de documentos mercantiles, para la celebración de los actos de comercio, porque ahora la empresa multinacional más grande o cualquier persona o comerciante, pueden celebrar la transacción internacional más común: La compraventa mercantil internacional y para identificar la operación cuando se utiliza la Internet como medio para celebrarla, se denomina Comercio Electrónico, aunque este término tiene alcance mayores y la actividad puede celebrarse dentro y fuera de nuevas fronteras. Estas operaciones comerciales al realizarlas por medios de comunicación electrónicos suprimen, en la mayoría de los casos, el usos del soporte papel y por supuesto la firma hológrafa"[119]; que dificultaban a los defraudadores su falsificación y uso indebido, aunque dichos casos siempre sucedían a pesar de los obstáculos.

Con respecto al comercio dentro de la Internet, el autor Barrios Osorio describe que: "...las empresas realizan una serie de operaciones administrativas y contables de carácter interno (usuario-usuario), se relacionan con otras empresas como proveedores, crediticias o financieras (usuarios-banco), e inclusive con órganos administrativos del Estado (contribuyentes-Superintendencia de Administración Tributaria). Todos los procedimientos administrativos han pasado de un procedimiento

[119] Barrios Osorio.**Ob. Cit.**, Pág. 290

manual a un procedimiento informatizado; a la digitalización de esos procedimientos se les denomina comúnmente e-business (negocios electrónicos). // A la acción de utilizar procedimientos digitalizados por medio de redes internas o externas (como la Internet) para efectuar compraventa a lo que se le denomina actualmente comercio electrónico (e-commerce); por ello el comercio electrónico es considerado una especie de los negocios electrónicos (e-buiness)".[120]

En el presente estudio las operaciones que interesan son las realizadas en el e-banking, el usuario directamente con la institución bancaria o bien esta como intermediario entre su cliente y un tercero en caso de compraventas u otras transacciones. Asimismo "...en el comercio electrónico se utilizan los medios de pago generalmente aceptados en el comercio tradicional, exceptuándose el pago de contado (efectivo), aunque existe también una equiparación conocida como efectivo digital" [121]. Los medios de pago que actualmente se utilizan, y que pueden ser aplicados al e-banking, mencionados por el autor Barrios Osorio son:

"a) Tarjeta de Pago;

b) Tarjeta de Crédito;

c) Transferencia de cuenta o depósito en cuenta;

d) Pago por correo certificado;

e) Saf-t-pay (pago por medio del Banco del usuario)". Refiriéndose el autor que: "El principal medio de pago actualmente es la tarjeta de crédito"[122].

---

[120] **Ibíd.,** Pág. 29
[121] **Ibíd.,** Pág. 29
[122] **Ibíd.,** Pág. 29

4.1. Banca electrónica

En la actualidad, el comercio ha utilizado otro tipo de plataforma para realizar transacciones comerciales, tomando como elemento de comunicación, la tecnología de la Internet, asimismo el sistema bancario se ha unido al uso de esta herramienta virtual, denominándose banca electrónica, por internet, en línea o e-banking.

La definición de banca electrónica "hace referencia al tipo de banca que se realiza por medios electrónicos como puede ser cajeros electrónicos, teléfono y otras redes de comunicación. // (...) comprende aquellas herramientas que ofrecen una entidad para que sus clientes hagan sus operaciones bancarias a través de la computadora utilizando una conexión a la red Internet. Para otros investigadores la banca por Internet es un nuevo tipo de sistema de información que usa los recursos novedosos de Internet y la World Wide Web (WWW) para permitir a los consumidores efectuar operaciones financieras en el espacio virtual".[123]

También, es considerada la banca virtual o sin presencia física como "...un banco virtual (...) sin oficina y normalmente se asocia el concepto banca virtual al de banca electrónica. En términos generales, este mercado no debería denominarse virtual, siendo más adecuada la denominación de banca electrónica o por Internet, puesto que las organizaciones participantes en el intercambio existen físicamente". [124]

En una definición propia, la e-banking, es un servicio más del sistema bancario que utiliza como plataforma la tecnología informática, provee a los cuentahabientes la

[123] http://es.wikipedia.org/wiki/Banca_electr%C3%B3nica, (29 de junio de 2014)
[124] **Ibíd**

automatización y rapidez en transacciones que en el pasado requerían, más tiempo para su realización.

Las ventajas que da el uso de la banca por internet, son las siguientes:

a) "La entrada en una nueva unidad estratégica de negocio que ofrece un alto potencial de crecimiento aunque también requiere de fuertes inversiones.
b) La reducción de costes de transacción (una transacción realizada vía Internet puede costar a un banco un 1% de lo que vale en la sucursal).
c) El acceso a la información general del banco (marketing directo).
d) La adecuación de los productos y servicios bancarios a las nuevas necesidades de los clientes, lo cual redunda en su fidelización".[125]

A lo anterior puede añadirse la agilización de los servicios, la facilidad en su uso y el control que el usuario tiene sobre las cuentas bancarias, que posee en los bancos del sistema.

En la banca en línea se ha descrito modalidades que agrupan los productos y servicios que ofrecen a los usuarios del servicio, los cuales son:

a) De información:

La información que se transmite o recite depende de la entidad. Regularmente los servicios que se prestan de este tipo son: "...consulta de saldos y movimientos de las cuentas, tarjetas, información sobre préstamos y operaciones bancarias, etc. // Además

[125] http://thales.cica.es/rd/Recursos/rd98/Economia/02/texto2.html, (28 de junio de 2014)

de este tipo de información particular de cada cliente, las entidades ofrecen otras de tipo genérica, como el acceso a los mercados financieros a tiempo real, productos y servicios ofrecidos por el banco, temas de actualidad, como el euro, etc.; completándose todo ello con la posibilidad de realizar consultas directamente a través del correo electrónico".[126]

b) De órdenes:

La modalidad de este servicio se caracteriza por las: "...transferencias y traspasos entre cuentas, solicitud de apertura, domiciliación de recibos, petición de talonarios, suscripción de fondos de inversión, planes de pensiones, petición de tarjetas de crédito, compra - venta de valores, solicitud de moneda extranjera, etc."[127]

La banca en línea ha creado la automatización de muchos servicios que antes eran en forma física, ahora se pueden hacer en cualquier lugar donde tenga acceso la internet, aunque el servicio se agilizo y es más eficiente, aunado a ello se provocaron nuevas formas de hechos ilícitos, con la diferencia que para llevar a cabo la comisión del delito se necesita conocimientos especializados de informática, asimismo, desaparecieron las agresiones físicas o muerte que se producían cuando el cuentahabiente después de realizar una transacción dentro del banco, al momento de su salida sufría de robos que provocaban agresiones y en caso extremos la muerte.

[126] http://thales.cica.es/rd/Recursos/rd98/Economia/02/texto2.html, (28 de junio de 2014)
[127] **Ibíd**

4.2. Estado actual de los servicios de banca electrónica en Guatemala

El estado actual de banca electrónica se da por "...el constante desarrollo y evolución de la tecnología ha dado cauce a la automatización bancaria hoy en día, que permite que el cliente no tenga que acudir a la sucursal bancaria para realizar sus operaciones financieras, por lo que es una banca no presencial o banca a distancia".[128]

Asimismo se ha considerado que "la banca electrónica llamado hoy en día, comprende distintas tecnología y no únicamente los portales web de home banking que son tan popular entre las bancas por internet. Para el caso específico de Guatemala las operaciones descentralizadas por medio de dispositivos electrónicos dieron inicio por medio de cajeros automáticos. Cabe mencionar que, el Comité de Basilea en su documento **Principos de Administración de Riegos para la Banca Electrónica** define a la Banca Electrónica o e-banking como el proceso que incluye la provisión de productos y servicios minoristas y de pequeño valor a través de canales electrónicos, así como pagos electrónicos de gran valor y otros servicios bancario mayoristas proporcionados electrónicamente".[129]

En el caso de Guatemala se describe que: "...se ha visto un crecimiento bastante pronunciado de las ofertas de temas de banca en línea por parte de la entidades bancarias, (...), hacia el pago de servicio y las transferencias entre cuentas. El banco con mayor número de usuarios actualmente es el Banco Industrial, sin embargo, es la entidad que ofrece mayor número de servicios en relación a sus competidores más cercanos. El sistema GuateACH (Sistema de Compensación Automatizado), el cual

[128] http://es.slideshare.net/ltarott/banca-electrnica-en-guatemala, (03 de mayo de 2014)
[129] **Ibíd**

permite realizar transferencias monetarias interbancarias, (...) presupone una infraestructura tecnológica básica entre las entidades financieras involucradas, para poder entrar en esta nueva partida".[130]

Otro de los servicios que se pretenden prestar dentro de la banca electrónica tiene como base la aprobación de un proyecto de ley que permita: "...otorgar validez legal a las imágenes electrónicas de los cheques emitidos."[131] Esta "...se realizará por medio de imágenes digitales, lo que reduce el tiempo para acreditar o pagar los fondos, y los clientes no deban esperar hasta tres días para disponer de ellos."[132]

"En esta forma el tiempo de compensación de un cheque se reduciría a horas y los usuarios podrían disponer del dinero más rápido. Hasta ahora la desmaterialización de los cheques está permitida para la banca **off Shore** (fuera de plaza), pero la tecnología que ha avanzado en los medios de pago tienen que extenderse a las operaciones en Guatemala, iniciativa conocida como Check 21, cuyo propósito es modernizar y reducir los costos para el sistema bancario. Los segmentos populares en el uso de la banca electrónica todavía no están aceptados como a nivel de la banca corporativa, en la que más de la mitad de las transacciones se hacen en forma virtual. Para una entidad bancaria el costo de operar un cheque es cinco veces más alto que el de una operación electrónica; además, la inversión en el mediano plazo le representa una diminución de costo para el banco que adquiere el software para este servicio". [133]

---

[130] **Ibíd**
[131] **Ibíd**
[132] **Ibíd**
[133] **Ibíd**

Entre los diversos servicios de comercio electrónico, que la banca electrónica provee, ya sea como intermediario o bien como proveedor de un servicio bancario virtual pueden realizarse las siguientes transacciones: consultas de cuentas, prestamos, servicios relacionados con tarjeta de crédito, pagos, transferencias, presentación y pago de tributos, revisar las imágenes de cheques girados o pagados, solicitud de chequeras, administración de seguridad y alertas automáticas a e-mail, facebook, entre otros.

Asimismo los métodos de seguridad ofrecidos por uno de los bancos del sistema del servicio en banca en línea son: compromiso de la entidad si existen inconvenientes, brindan seguridad de la información, ofrecen salvaguardar la privacidad, protección contra el robo de identidad y fraude.

Como puede observarse los servicios del e-banking, que ofrecen las entidades bancarias, tienen preparado una serie de ofertas y para ganar la confianza de los cuentahabientes, paralelamente dan a conocer la seguridad que les pueden brindar. Sin embargo, en los casos expuestos de delito informático en Guatemala, el titular principal del bien jurídico tutelado es la entidad bancaria, misma que no tiene ninguna protección de carácter gubernamental; por lo cual existe el peligro latente de que el sistema bancario pueda sufrir déficit comercial a gran escala, si existe una recurrencia en la comisión de estos hechos ilícitos.

Además, los riesgos que conlleva esta nueva actividad comercial a través del uso de la internet y por medio del servicio que prestan el sistema bancario guatemalteco; a pesar de los notables cambios: "...se evidencia en el comercio y los servicio financiero, ya

que, el comercio electrónico a modificado los hábito de las finanzas, y ahora el de los comerciantes y consumidores, a la vez que produce cambios sustanciales en los medios de pago tradicionales. En ese sentido, las entidades financieras se enfrentan a un entorno competitivo radicalmente distinto al que se había conocido hasta ahora".[134]

Aunado a los riesgos mencionados, en este campo es la existencia de robos o fraudes dentro de la banca electrónica, los hechos ilícitos cometidos por el conocimiento especializado, que tienen los autores de los delitos informáticos en ese ámbito; como ya se estableció en apartados anteriores dentro del presente estudio de investigación, donde se demostró la forma de operar en tres formas diferentes, los cuales fueron:

a) Casos de phishing
b) El robo de datos personales
c) aso de los piratas informáticos

Dentro de los anteriores casos la forma de operar más frecuente para poder realizar ilícito dentro de la banca electrónica es el phishing.

Otros hechos ilícito cometidos en el ámbito del e-banking son los siguientes: Defraudaciones a través de publicidad engañosa, fraudes cometidos por medio del acceso y manipulación a sistemas informáticos bancarios o financieros, sabotaje a sistemas informáticos, uso no autorizado de sistemas informáticos ajenos, espionaje informático, falsificación de documentos por medio de la computadora.

[134] http://es.slideshare.net/ltarott/banca-electrnica-en-guatemala, (03 de mayo de 2014)

También existen dificultades que deben superarse dentro del comercio electrónico y que a su vez tiene mucha relación con el e-banking, el autor Barrios Osorio menciona que: "como toda actividad que realiza el hombre, el comercio electrónico tiene una serie de desventajas que pueden ser superadas acorde al interés que muestre cada una de las ciencias involucradas. Muchos inconvenientes técnicos como lo era un protocolo común o sistemas de seguridad en el uso de tarjeta de crédito, han sido salvados por los especialistas en el área técnica de esta actividad. Diversos autores señalan una lista de problemas o inconveniente que se deben considerar; el siguiente es un listado de ellos": [135]

a) La desconfianza creada por el desconocimiento.
b) Sistemas seguros de encriptación para el uso de tarjetas de crédito.
c) Perfeccionamiento de sistemas.
d) No existe facilidad en el manejo del sistema.
e) La limitada interadaptación y compatibilidad de herramientas.
f) Los consumidores no tiene el hábito de uso del sistema.
g) La falta de personal cualificado.
h) Obstáculos legales.
i) La dependencia tecnológica.
j) Falta de conocimiento y adaptación para un uso generalizado.
k) Inversión constante por cambios tecnológicos.

[135] Barrios Osorio. **Ob. Cit.**, Pág. 302

"Está claro que los inconvenientes señalados han de ser superados en un corto o mediano plazo, de no ser así no seguiría el comercio electrónico con el crecimiento vertiginoso que lo impulsa".[136]

Asimismo el Autor Barrios Osorio da conocer que el problema principal está en la falta de: "...creación de la normativa legal que se deberá aplicar para superar cada uno de los problemas e inconvenientes en que el Derecho tenga la solución. La legislación que se emita al respecto no debe provenir de uno solo de los partícipes en la actividad comercial moderna denominada comercio electrónico, debe de ser un trabajo en conjunto y contar con asesores especializados en la materia. Por el momento la interpretación extensiva de las normas legales actuales es una de las soluciones. El problema no se reduce sólo a la creación de normas o interpretación de las actuales, si no los procesos o acciones por medio de la cual se va aplicar esas normas".[137]

El anterior autor manifiesta que: "para que el comercio electrónico se desarrolle en Guatemala y se constituya como un mercado con posibilidades reales de participación tanto nacional como internacional, es necesario que el Derecho al igual que otras ciencias o técnicas, estudie a profundidad el fenómeno que este representa, para poder realizar una efectiva regulación de sus actividades, creando un marco legal que legalice todos aquellos aspectos que lo diferencia del comercio tradicional, pero debiendo considerar todos aquellos factores que puedan tener incidencia en su modificación y actualización especialmente los que tienen que ver con la implementación de tecnología de punta, porque los progresos en el campo de la Informática son

[136] **Ibíd.,** Pág. 302
[137] **Ibíd.,** Pág. 302

constantes".[138] Resalta el autor que lo importante es superar los inconveniente de carácter jurídico, por la falta evidente de leyes sobre la materia y la poca participación de especialistas en la creación de dichos cuerpos normativo.

Aunado a la falta de normativa adecuada, es determinante también la falta de conocimiento de medios informáticos, es importante recordar que en el momento de su implementación del servicio e-banking; un reducido número de la población guatemalteca ha gozado desde el principio de este servicio, porque en sus inicios hasta profesionales de medicina, ciencias sociales o administración de mucha experiencia no tenían el conocimiento del uso de la computadora menos de la Internet, y las personas que podían utilizar el servicio no estaban preparados para los posibles riesgos de fraudes o robos dentro del ciberespacio. Por medio de la experiencia adquirida, es evidente que en el futuro el Estado debe estar involucrado en cualquier actividad que utilice tecnología de punta, tanto en una constante supervisión, planes de prevención, sistema de alarma para la averiguación, persecución y procesamiento de los culpables en caso de hechos delictivos.

4.3. Importancia de la informática forense aplicada al sistema bancario guatemalteco

La banca en línea en Guatemala ha sido objeto de diversos hechos delictivos, que conlleva a una nueva forma de investigación para la averiguación de la verdad, y ésta se logra solamente a través de la informática forense, rama que pertenece a la criminalística.

---

[138] **Ibíd.,** Pág. 302

Con respecto a la informática forense la autora Jeimy Cano explica que existen múltiples definiciones a la fecha sobre el tema forense en informática; sin embargo aplicado al e-banking se establece que: "...una primera revisión (...) sugiere diferentes términos para aproximarse 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".[139]

Finalmente, la autora Cano menciona que: "...digital forensics, forensia digital, trata de conjugar de manera amplia la nueva especialidad. Esta tiene una 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".[140]

---

[139] Cano Martines Jeimy José. **Introducción a la informática forense, una disciplina técnico-legal.** Pág. 3
[140] **Ibíd.**, Pág. 4

Según las anteriores definiciones la aplicable a la averiguación de la verdad en los delitos cometidos dentro de la banca electrónica en Guatemala es la forensia digital, al ser estudios técnicos dirigidos especialmente a coadyuvar en la administración de la justicia.

Por lo tanto una de las ramificaciones de la informática forense aplicables al presente estudio es digital forensics o forensia digital, como ya se menciono con anterioridad y la importancia de que tanto especialistas en la materia, como jurista creen un cuerpo normativo que especifique las practicas de la informática forense a los hechos ilícito cometidos dentro de la banca electrónica.

4.4. Implementación gubernamental de medidas y métodos para la prevención y combate de los delitos cometidos en el e-banking

La participación del Estado tanto en la prevención como en la averiguación de la verdad, mediante las correspondientes entidades (Superintendencia de Bancos, Instituto Nacional de Ciencias Forenses), en los delitos cometidos en la banca electrónica han sido deficientes o nulas; al no contar con una base legal que permite una relación interinstitucional, oficinas técnicas especializadas, que presten el servicio a las entidades bancaria y usuarios del servicio de banca en línea, para promover, prevenir y coadyuvar en la administración de justicia.

4.4.1. Superintendencia de bancos

El tercer párrafo del Artículo 133 de la Constitución Política de la República de Guatemala describe que: "La Superintendencia de Bancos organizada conforme a la

ley, es el órgano que ejercerá la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y las demás que la ley disponga".

Es así que la ley le da la potestad de establecer medidas que permitan la supervisión financiera en todas la actividades que se presenta en esta actividad económica, esto incluye también la banca en línea, sin embargo "...el cliente aún no confía en la seguridad de la banca virtual por lo que el crecimiento en ese punto está siendo lento y legislativamente se están comenzado con leyes", de esta materia, en consecuencia el "...país no cuenta con una legislación específica para la banca electrónica, actualmente los banco se acoplan a las leyes vigentes de la banca convencional. Cabe mencionar que la tercer reforma monetaria se encuentra en enmiendas y se espera que dicha reforma venga a legislar y estandarizar todos las banca electrónica para garantizar los procesos y transacciones que el cliente realiza en línea, así como la seguridad y los métodos de encriptación que los bancos deben de utilizar para prevenir que los datos caigan en manos de personas inescrupulosas".[141]

Existe un vacío legal y reglamentario que permita una supervisión financiera correcta en la actividades de la banca electrónica, al no tener un parámetro normativo, los servicios en línea quedan bajo el arbitrio de los bancos del sistema, la garantía de seguridad y prevención puede no cumplir con requisitos uniformes y de alta tecnología, derivándose una vulnerabilidad del servicio e-banking.

[141] http://es.slideshare.net/ltarott/banca-electrnica-en-guatemala, (03 de mayo de 2014)

El autor Barrios Osorio, describe que la seguridad en el comercio electrónico puede concretarse desde dos puntos de vista:"El primero denominado seguridad tecnológica, y El segundo la seguridad o certeza jurídica o legal. // En determinados fases o momentos del comercio electrónico ha predominado la seguridad tecnológica, desarrollándose ésta primero, pero debe de ser revestida por la seguridad o certeza legal".[142]

"La protección que se debe brindar a quienes ejercen transacciones electrónicas, tomando en cuenta a todos los participes y en cada uno de los momentos de realización de la misma; entre las protecciones mínima se encuentran":[143]

a) Protección de la Red o Sitio: "Realizado con Firewalls (paredes de fuego o cotrafuegos), que son un conjunto de programas que funcionan como alarmas, detectores o guardias de seguridad, para que ningún intruso pueda acceder a su comercio virtual".[144]

b) Programas de encriptación: "La información que viaja entre el comerciante y el usuario debe de revestir ciertas características de resguardo en cuanto a su contenido, lo que se logra a través de la Criptotogía".[145]

c) Los mecanismos o formas de aceptación: "En el momento más importante en la celebración de las transacciones, en que tanto el proveedor de bienes o servicios como el usuario deciden validar sus derechos y obligaciones a través de la aceptación, que

---

[142] Barrios Osorio. **Ob. Cit.**, Pág. 313
[143] **Ibíd.,** Pág. 358
[144] **Ibíd.,** Pág. 358
[145] **Ibíd.,** Pág. 358

puede realizarse desde el simple envío de un correo electrónico, un click, hasta la forma más segura es decir la utilización de la Firma Electrónica o en su caso la Firma Digital".[146] Esto incluye el compromiso de la entidad bancaria con el usuario, los técnico o especialista tecnológicos con la confidencialidad ante la entidad bancaria y el compromiso del usuario a realizar todas y cada uno de los pasos recomendados para evitar hechos delictivos.

La Superintendencia de Banco, a su vez, participa en la prevención de hechos ilícitos cometidos en la banca electrónica, mediante la supervisión e implementación de normas, es como la protección de la privacidad o intimidad, logrando cubrir todos los ámbitos en que los datos personales son utilizados.

Los procedimientos de protección o defensa de los datos personales generales, no cuentan con la participación de la Superintendencia de Bancos en el caso de la banca electrónica, pero de forma general los procedimientos de defensa legales, en Guatemala son: "los mecanismo para hacer valer los derechos cuando no se solucionen por la vía voluntaria o conciliatoria, o bien para aplicar la restricciones cuando no se cumplan las establecidas, se encuentran regulados en las norma jurídicas del Estado. Se caracterizan y diferencian de los voluntarios por que existen participación de órganos con competencia administrativa o judicial y que existe un procedimiento previamente establecido.// En la doctrina y la legislación se encuentran varios procedimientos: el Derecho de Rectificación o de Respuesta; la Procuraduría de los Derechos Humanos; el Habeas Data".[147]

---

[146] **Ibíd.,** Pág. 358
[147] **Ibíd.,** Pág. 358

La actuación de la Superintendencia de Bancos se ve limitada debido a la falta de legislación específica de la banca electrónica, por ende es necesario considerar, la creación de parámetro que permitan una participación estatal dirigida a un mínimo de protección de datos y otras incidencias derivadas de la misma.

Una normativa para la protección de datos en la banca electrónica de conformidad con Lawrence Lessin citado por Barrios Osorio, estipula cuatro formas, siendo estas: a) La ley: creación de normativa adecuada y especializada, (la necesidad de crear una ley que proteja los datos personales). b) Las normas: realizadas a través de contratos que permitan establecer los parámetros de obligaciones y derecho de las partes en un negocio particular, como el caso de actividades comerciales en el e-banking (usurario y banco). c) El mercado en ello se presente en: "...las empresas proveedoras de servicio al cobrar un costo adicional a los usuarios por brindar una mayor seguridad a los datos privados que (...), brindan esa protección como un valor agregado a su servicios". (Caso de G&T Continental que ofrece la encriptación de datos). d) La Arquitectura, (Tecnología) "...el administrador debe de considerar todos los recursos disponibles (hardware y software) para proteger los datos que contiene el sistema informático bajo su responsabilidad" [148]. e) prevención del usuario: esto conlleva a que el usuario debe también proteger su privacidad al no dejar a la vista documento o datos personales en lugares donde fácilmente pueda tener acceso cualquier persona.

Es evidente que la participación en cuanto a medidas de prevención, para evitar hechos delictivos, cometidos dentro de la banca en línea es una atribución especial de la Superintendencia de Bancos, esta participación no es viable en la actualidad por falta

[148] **Ibíd.,** Pág. 358

de normativa, como ya se indico, pero también no existe voluntad por parte de otros sectores como el Congreso de la República de Guatemala, que dentro del proyecto de ley sobre delitos informáticos, (en discusión), no crea una estrategia de coordinación con ninguna entidad estatal o plan nacional para evitar y proceder legalmente con los culpables, la exposición es sobre delitos y no es estratégico; es decir un sistema armonizado de participación de todas las entidades que tenga intima relación con las prestación de servicios bancarios con tecnología de punta. Además, no asigna responsabilidades a entidad estatales financiera en la supervisión y denuncia, para el combate del delito.

4.4.2. Instituto Nacional de Ciencias Forenses de Guatemala

La Ley Orgánica del Instituto Nacional de Ciencias Forenses de Guatemala, establece en el Artículo 2, los fines de la institución al establecer que: "...como finalidad principal la prestación del servicio de investigación científica de forma independiente, emitiendo dictámenes técnicos científicos". Esta entidad agrupa todas las ciencias forenses al aplicar disciplinas científicas en la averiguación de la verdad a un caso concreto. La determinación de la prueba es el fin de una serie de pasos de carácter multidisciplinario que permite coadyuvar en la administración de la justicia.

La prevención y supervisión de las entidades bancarias en cuanto al servicio de e-banking, para evitar hechos ilícitos cometidos en ese ámbito, se determino que debe ser una función que pertenece al campo de la Superintendencia de Bancos, por la naturaleza legal que lo reviste; como entidad estatal encargada de la vigilancia de las actividades bancarias.

Por otro lado, también es necesario el esclarecimiento de hechos ilícitos ya cometidos, esto solamente se puede hacer a través de la informática forense para determinar medios de prueba que sea la base de una acusación eficaz. Asimismo también ya se estableció que la rama o parte de esta ciencia que permite coadyuvar a la administración de justicia es la forensia digital.

De tal manera, es necesaria la implementación de un laboratorio de forencia digital dentro del INACIF, contribuye a la averiguación de la verdad, y en la investigación de hechos ilícitos cometidos en la banca electrónica en conjunto con el Ministerio Público. La parte fundamental de la participación del instituto es lograr determinar medios de prueba.

Respecto al comercio electrónico, aplicable también al e-banking, las pruebas electrónicas según el autor Barrios Osorio, se dividen en: a) El documento electrónico; b) Otras pruebas electrónicas.

Los documentos electrónicos como medio de prueba "...son por su naturaleza documentos pero en formato electrónico. El Tribunal Supremo de España en sentencias de fechas 3 de junio de 1994 y 11 de octubre de 1994 indica" [149]: describe que: // "...Documento es en sentido estricto, y ha de entenderse por tal, el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo puedan asimilarse al mismo -por ejemplo, un disquete, un documento de ordenador, un vídeo, una película, etc.-, con un criterio moderno de interacción de las nuevas realidades tecnológicas, en sentido en que la palabra documento figura en algunos diccionarios como cualquier cosa que sirve

[149] **Ibíd.,** Pág. 247

para ilustrar o comprobar algo, siempre que el llamado documento tenga un soporte material..."[150]

Los documentos electrónicos puede ser varios; el autor Barrios Osorio describe un grupo de ellos, aunque no limitativo, al dar a entender que puede haber más, siempre y cuando llenen los requisito del concepto de documento, entre ellos se encuentran:

"a) Archivos informáticos de carácter general.

b) Las bases de datos.

c) Los formularios electrónicos.

d) Los contratos electrónicos.

e) Las páginas o contenido de los sitios web.

f) Los correos electrónicos".[151]

De forma general se denominan también como medios de prueba electrónicos o evidencia electrónica, los que necesitan de peritos o experto para su diligenciamiento; siendo estos:

a) "Los programas de ordenador.

b) Inspección ocular o peritaje de los programas de ordenador.

c) Peritaje o inspección sobre dispositivos de almacenamiento.

d) Backup o copia de seguridad.

e) Titular de un nombre de dominio, web site o hosting".[152]

---

[150] **Ibíd.,** Pág. 247
[151] **Ibíd.,** Págs. 247, 310
[152] **Ibíd.,** Págs. 247, 310

"Otros medios de prueba derivados del uso de las Tecnología de la Información y Comunicaciones necesitaran de peritos especializados en la materia para su diligenciamiento".[153] Sin embargo el vacío legal continúa y la tecnología sigue avanzando, por lo que el abordaje de este problema por parte del Congreso de la República en la creación de una ley que detalle la prevención, seguridad, aplicación interdisciplinaria tecnológica en la averiguación de la verdad a través de la informática forense, en delitos cometidos en la banca electrónica es de urgencia nacional.

[153] **Ibíd.,** Págs. 247, 310

CONCLUSIÓN DISCURSIVA

Una de los problemas encontrados que tiene mayor importancia, es que actualmente el Instituto Nacional de Ciencias Forenses de Guatemala no cuenta con un laboratorio o servicio de profesionales especializados en materia de informática forense; para la averiguación de hechos ilícitos dentro de la banca electrónica; según el instructivo que tiene como base legal para actuar, solamente realizan a través de sistemas informáticos, examen de documentos físicos en soporte de papel, dentro de la unidad de documentoscopia, siendo necesario la implementación del mismo.

Como deficiencia legal, la falta de regulación especial en materia de protección de datos, permite la comisión de hechos delictivos, realizados en la banca electrónica, al tener acceso a datos dentro del sistema informático que permite la suplantación de identidades eliminando la certeza jurídica de dicho servicio. Siendo necesario que en el Congreso de la República de Guatemala se apruebe la iniciativa 4055 "Ley de Delitos Informáticos" la cual llenaría esta laguna legal.

En virtud de lo anterior, es necesario que para la investigación criminalística de los delitos cometidos en la banca electrónica, el Instituto Nacional de Ciencias Forenses implemente un laboratorio de informática forense, que cuente con técnicos especialistas en alta tecnología, para el examen de indicios que puedan dejar en la comisión de hechos delictivos dentro de la banca en línea.


SECRETARIA

BIBLIOGRAFÍA

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática, aspectos fundamentales**. 3ª. ed. Guatemala: Ed. Mayte, 2006.

BARRIOS OSORIO, Omar Ricardo. **Introducción de las nuevas tecnologías en el derecho.** Instituto de la Defensa Pública Penal. Ed: IDPP, Guatemala, 2010.

CANO Martines Jeimy José. **Introducción a la informática forense, una disciplina técnico-legal. Ed: UA,** Colombia año 2006.

CABRERA FORNEIRO, José, Rocañin Fuentes José Carlos y Plumed Moreno Calixto, **Enfermería legal.** Ed: Ela, Madrid España año 1994.

http://es.slideshare.net/ltarott/banca-electrnica-en-guatemala. (Consultado: 03 de mayo de 2014).

http://especiales.prensalibre.com/revistad/2012/04/22/reportajecentral.shtml. (Consultado: 02 de marzo de 2014).

http://eticauvg.wordpress.com/2012/05/22/analisis-de-casos/. (Consultado: 04 de marzo de 2014).

http://www.elperiodico.com.gt/es/20121104/pais/220128. (Consultado: 22 de enero de 2014).

http://www.gytcontinental.com.gt/portal/portal/productos.asp?idprod=banca_electronica. (Consultado: 08 de mayo de 2014).

http://www.inacif.gob.gt/. (Consultado: 13 de diciembre de 2013).

http://www.inacif.gob.gt/index.php?option=com_content&view=article&id=75&Itemid=85. (Consultado: 12 de mayo de 2014).

http://www.onu.org.gt/. (Consultado: 22 de febrero de 2014).

http://www.prensalibre.com/. (Consultado: 22 de enero 2014).

http://www.rae.es/. (Consultado: 22 de febrero de 2014).

http://www.transdoc.com.gt/assets/images/users/dani/file/. (Consultado: 23 de enero 2014).

http://www.ventanalegal.com/espacio_estudiantil/criminalistica.htm. (Consultado: 14 de septiembre de 2013).

MONTIEL SOSA, Juventino. **Criminalística**. Tomo I. Ed:Limusa, México 4ª. Reimpresión, año 1998.

NORIEGA SALAZAR, Han Aarón. **Delitos informáticos.** Instituto de la Defensa Pública Penal. Ed: IDPP, Guatemala año 2011.

ROCAÑIN FUENTES, José y Plumed Moreno Calixto. **Enfermería legal.** Ed: Ela, Madrid España año 1994.

Legislación:

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

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

Ley Orgánica del Instituto Nacional de Ciencias Forenses. Congreso de la República de Guatemala, Decreto 32-2006, 2006.

Ley de Acceso a la Información Pública. El Congreso de la República de Guatemala, decreto 57-2008, 2008.

Reformas al Decreto 17-73 Código Penal del Congreso de la República. Congreso de la República de Guatemala, Decreto 33-96, 1996.

Ley de Delitos Informáticos, iniciativa 4055. Pleno del Congreso de la República de Guatemala, 2009.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Congreso de los Estados Unidos Mexicanos, Ley 1273-2009, 2009.

Modificación Código Penal Decreto Número 17.613 de 4 de mayo de 1970: Ley de Delitos Informáticos. Asamblea Legislativa de la República de Costa Rica, Ley 9048, 2012.

Ley sobre Delitos de Alta Tecnología. Asamblea Legislativa de la República Dominicana, Ley 53-07, 2007.

Código Penal. Asamblea Legislativa de la República del Perú, 2000.